ESCUELA POLITECNICA DEL EJÉRCITO

DEPARTAMENTO DE ELECTRICA Y ELECTRONICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO EN INGENIERIA

# DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN PARA BRINDAR SERVICIOS Y CAPACIDAD VPN PARA LA EMPRESA INGELSI CIA. LTDA.

ACERO PALACIOS RICARDO VLADIMIR

SANGOLQUI – ECUADOR
2007

# RESUMEN DEL PROYECTO DE GRADO

## DESCRIPCIÓN DEL PROYECTO REALIZADO

Este proyecto tiene por objetivo principal acercar al usuario de la empresa, esto se consigue al compartir información y acceder a esta en cualquier momento requerido sin importar las distancias o medios de comunicación. Por lo tanto se realizaron diferentes redes las cuales tienen diferentes funciones. Se realizó una Red LAN la cual une toda la información y recursos empresariales con los usuarios de la red local con seguridades; una Red WLAN quién es la encargada de unir sin necesidad de cables a los usuarios móviles con los recursos de red, por otro lado se realizó una Red VPN la cual acerca a los recursos de la red con usuarios que se encuentren fuera de la oficina y necesiten revisar información de la misma mediante Internet o Acceso Telefónico y finalmente se configuró una Central Telefónica la cual unirá con el exterior y viceversa mediante una comunicación ágil y sencilla vía telefónica.

Entre las características técnicas y limitaciones, la red LAN trabaja mediante el estándar Fast Ethernet, según la norma 802.11u, topología física en Estrella, cable Cat5e con velocidades de 100Mbps y alcance de 100m y seguridades mediante Firewall. La red WLAN trabaja con el estándar 802.11b y g, en una frecuencia de 2.4Ghz, con velocidades desde los 11Mbps hasta los 54Mbps y seguridades tipo WAP. La red VPN se conecta mediante acceso telefónico a redes y mediante conexión a Internet usando el protocolo PPTP. Finalmente la central telefónica usa como máximo 6 líneas y 16 extensiones, con tarjetas opcionales se puede extender hasta 24 extensiones.

Uva vez implementadas las redes se debe tener como consideración el uso de restricciones y seguridades para las mismas. Se debe actualizar las redes con el paso del tiempo en hardware y software y administrar las redes y chequearlas periódicamente.

## CERTIFICACION

Por medio de la presente, certificamos que el señor estudiante ACERO PALACIOS RICARDO VLADIMIR, ha realizado y concluido en su totalidad la presente tesis de grado, "DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN Y WLAN PARA BRINDAR SERVICIOS Y CAPACIDAD VPN PARA LA EMPRESA INGELSI CIA. LTDA." para la obtención del Título de Ingeniería en Electrónica de Redes y Telecomunicaciones, de acuerdo con el plan aprobado previamente por el Concejo Directivo del Departamento de Eléctrica y Electrónica.

Firman:

| | |
|---|---|
| Ingeniero Fabián Sáenz | Ingeniero Carlos Romero |
| DIRECTOR | CODIRECTOR |

# AGRADECIMIENTO

Esta tesis, si bien ha requerido de esfuerzo y mucha dedicación por parte del autor, no hubiese sido posible su finalización sin la cooperación desinteresada de todas y cada una de las personas que a continuación citaré y muchas de las cuales han sido un soporte muy fuerte en momentos de angustia y desesperación.

Primero y antes que nada, dar gracias a **Dios**, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Agradecer hoy y siempre a mi familia, a mis padres Ricardo Acero y Melba Palacios, mis abuelos, mis hermanas, etc., por haberme dado su apoyo incondicional en todos los momentos difíciles los cuales superé, gracias a ellos. También mi sincero a agradecimiento a la familia Díaz en especial a Belén Díaz por el ánimo, apoyo y alegría que me brindan me dan la fortaleza necesaria para seguir adelante y a mis amigos que me apoyaron siempre en todo momento.

Finalmente agradezco a la Facultad de Ingeniería Electrónica de la Escuela Politécnica del Ejército por haberme acogido en sus aulas y enseñarme todos estos conocimientos con los cuales fueron posibles la elaboración de este proyecto, también agradezco a la empresa INGELSI Cia. Ltda. por haberme permitido llevar estos conocimientos aprendidos y hacerlos realidad en la práctica.

# DEDICATORIA

Esta tesis la dedico en primer lugar a **Dios** por darme la oportunidad de vivir y de regalarme una familia maravillosa.

Con mucho cariño a mis padres que me dieron la vida y que han estado conmigo en todo momento y por darme una carrera para mi futuro y creer en mí, aunque hemos pasado momentos difíciles siempre han pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén conmigo a mi lado, simplemente les estoy devolviendo toda la confianza que han puesto en mi.

# PRÓLOGO

El siguiente proyecto tiene como objetivo general ayudar a la empresa INGELSI Cia. Ltda. a ser más productiva y eficiente en este mundo donde la competencia es inminente.

Para lograr este objetivo se desarrollaron varias redes con los programas más actualizados del mercado en este momento, la primera red que se desarrollo es una Red LAN de voz y datos la cual ayudará a los usuarios a compartir los recursos con mayor facilidad, Internet y para una administración centralizada en esta etapa del proyecto se configuró una central telefónica la cual ayudará en la comunicación más ágil, amigable y segura en todas sus oficinas, a continuación se desarrolló una Red WLAN la cuál ayudará a usuarios móviles como portables, palms, celulares, etc., acceder a la red de la empresa en cualquier lugar de la misma sin necesidad de cables o ataduras y acceder a los beneficios de la misma, finalmente se desarrollo una Red VPN la cuál tiene como finalidad primordial estrechar lazos entre usuario y empresa cuando este se encuentre fuera de la oficina y hacerlo sentir como si estuviera dentro de la misma para que administradores accedan a la base de datos en tiempo real y así verificar cualquier transacción realizada, además para los administradores ayudará verificar el estado de las redes y recursos desde cualquier lugar del mundo con conexión a Internet o mediante una línea telefónica con el Acceso Telefónico a Redes, todos estos beneficios y más son posibles gracias a estas implementaciones las cuales guiarán a esta empresa a un futuro más competitivo en el mercado.

# ÍNDICE

# CAPITULO I

# INTRODUCCIÓN

Actualmente, el manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier organización, sea esta de origen público o privado, por lo que se hace necesario manejarla y emplearla con mucho criterio, ya que de ello podría depender, en gran medida, el éxito o fracaso de las mismas.

Son muchas las herramientas que, en la actualidad, facilitan al hombre el manejo del recurso informativo, así como el acceso a este. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente, rápida y confiable, la constituyen las redes de Computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico que ha caracterizado a las últimas décadas del presente siglo.

La idea de las redes existe desde hace mucho tiempo, y ha tomado muchos significados. Si se consulta el término «red» en el diccionario, se podría encontrar cualquiera de las siguientes definiciones:

- Malla, arte de pesca.
- Un sistema de líneas, caminos o canales entrelazados.
- Cualquier sistema interconectado; por ejemplo, una red de difusión de televisión.
- Un sistema en el que se conectan entre sí varias equipos independientes para compartir datos y periféricos, como discos duros e impresoras.

En la definición, la palabra clave es «compartir». El propósito de las redes de equipos es compartir. La capacidad de compartir información de forma eficiente es lo que le da a las redes de equipos su potencia y atractivo. Y en lo que respecta a compartir información, los seres humanos actúan en cierto modo como los equipos. Así como los equipos son poco más que el conjunto de información que se les ha introducido, en cierto modo, nosotros somos el conjunto de nuestras experiencias y la información que se nos ha dado. Cuando

queremos incrementar nuestros conocimientos, ampliamos nuestra experiencia y recogemos más información. Por ejemplo, para aprender más sobre los equipos, se podría hablar informalmente con amigos de la industria informática, volver a la escuela e ir a clase, o seguir un curso de autoaprendizaje. Independientemente de la opción seleccionada, cuando buscamos compartir el conocimiento y la experiencia de los demás, estamos trabajando en red.

Otra forma de pensar en las redes es imaginarse una red como un equipo. Puede ser un equipo deportivo, como un equipo de fútbol, o un equipo de proyecto. Mediante el esfuerzo conjunto de todos los implicados (compartiendo tiempo, talento y recursos) se alcanza una meta o se termina un proyecto. De forma similar, gestionar una red de equipos no es muy distinto de dirigir un equipo de personas. La comunicación y compartición puede ser fácil y simple (un jugador que pide a otro la pelota) o compleja (un equipo de un proyecto virtual localizado en diferentes zonas horarias del mundo que se comunica mediante tele conferencia, correo electrónico y presentaciones multimedia por Internet para llevar a cabo un proyecto).

En su nivel más elemental, una red de equipos consiste en dos equipos conectados entre sí con un cable que les permite compartir datos. Todas las redes de equipos, independientemente de su nivel de sofisticación, surgen de este sistema tan simple. Aunque puede que la idea de conectar dos equipos con un cable no parezca extraordinaria, al mirar hacia atrás se comprueba que ha sido un gran logro a nivel de comunicaciones.

Las redes de equipos surgen como respuesta a la necesidad de compartir datos de forma rápida. Los equipos personales son herramientas potentes que pueden procesar y manipular rápidamente grandes cantidades de datos, pero no permiten que los usuarios compartan los datos de forma eficiente. Antes de la aparición de las redes, los usuarios necesitaban imprimir sus documentos o copiar los archivos de documentos en un disco para que otras personas pudieran editarlos o utilizarlos. Si otras personas realizaban modificaciones en el documento, no existía un método fácil para combinar los cambios. A este sistema se le llamaba, y se le sigue llamando, «trabajo en un entorno independiente».

En ocasiones, al proceso de copiar archivos en disquetes y dárselos a otras personas para copiarlos en sus equipos se le denomina «red de alpargata» (sneakernet). Esta antigua versión de trabajo en red se la ha usado y puede que se siga usándola actualmente.

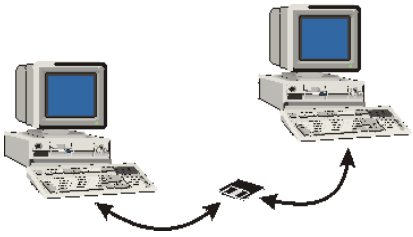


**Figura. 1.1. Red Sneakernet.**

Este sistema funciona bien en ciertas situaciones, y presenta sus ventajas (permite tomar un café o hablar con un amigo mientras intercambiamos y combinamos datos), pero resulta demasiado lento e ineficiente para cubrir las necesidades y expectativas de los usuarios informáticos de hoy en día. La cantidad de datos que se necesitan compartir y las distancias que deben cubrir los datos superan con creces las posibilidades del intercambio de disquetes.

Por otro lado si un equipo estuviera conectado a otros, entonces podría compartir datos con otros equipos, y enviar documentos a otras impresoras. Esta interconexión de equipos y otros dispositivos se llama una red, y el concepto de conectar equipos que comparten recursos es un sistema en red.

Con la disponibilidad y la potencia de los equipos personales actuales, puede que se pregunte por qué son necesarias las redes. Desde las primeras redes hasta los equipos personales actuales de altas prestaciones, la respuesta sigue siendo la misma: las redes aumentan la eficiencia y reducen los costes. Las redes de equipos alcanzan estos objetivos de tres formas principales:

- Compartiendo información (o datos).
- Compartiendo hardware y software.
- Centralizando la administración y el soporte.

De forma más específica, los equipos que forman parte de una red pueden compartir:

- Documentos (informes, hojas de cálculo, facturas, etc.).
- Mensajes de correo electrónico.
- Software de tratamiento de textos.
- Software de seguimiento de proyectos.
- Ilustraciones, fotografías, vídeos y archivos de audio.
- Transmisiones de audio y vídeo en directo.
- Impresoras.
- Faxes.
- Módems.
- Unidades de CD-ROM y otras unidades removibles.
- Discos duros.

Y existen más posibilidades para compartir. Las prestaciones de las redes crecen constantemente, a medida que se encuentran nuevos métodos para compartir y comunicarse mediante los equipos.

La capacidad de compartir información de forma rápida y económica ha demostrado ser uno de los usos más populares de la tecnología de las redes. Hay informes que afirman que el correo electrónico es, con diferencia, la principal actividad de las personas que usan Internet. Muchas empresas han invertido en redes específicamente para aprovechar los programas de correo electrónico y planificación basados en red.

Al hacer que la información esté disponible para compartir, las redes pueden reducir la necesidad de comunicación por escrito, incrementar la eficiencia y hacer que prácticamente cualquier tipo de dato esté disponible simultáneamente para cualquier usuario que lo necesite. Los directivos pueden usar estas utilidades para comunicarse rápidamente de forma eficaz con grandes grupos de personas, y para organizar y planificar reuniones con personas de toda una empresa u organización de un modo mucho más fácil de lo que era posible anteriormente.

Antes de la aparición de las redes, los usuarios informáticos necesitaban sus propias impresoras, trazadores y otros periféricos; el único modo en que los usuarios podían compartir una impresora era hacer turnos para sentarse en el equipo conectado a la impresora.

Las redes hacen posible que varias personas compartan simultáneamente datos y periféricos. Si muchas personas necesitan usar una impresora, todos pueden usar la impresora disponible en la red.

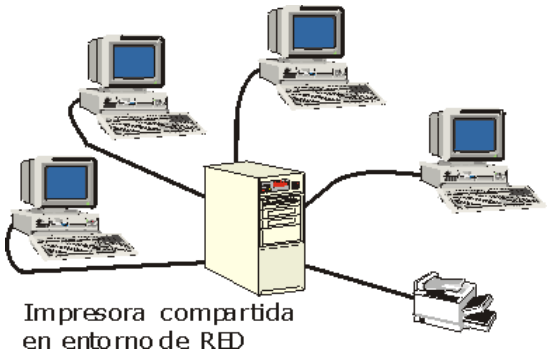



**Figura. 1.2. Impresora compartida en entorno de red.**

Las redes pueden usarse para compartir y estandarizar aplicaciones, como tratamientos de texto, hojas de cálculo, bases de datos de existencias, etc., para asegurarse de que todas las personas de la red utilizan las mismas aplicaciones y las mismas versiones de estas aplicaciones. Esto permite compartir fácilmente los documentos, y hace que la formación sea más eficiente: es más fácil que los usuarios aprendan a usar bien una aplicación de tratamiento de textos que intentar aprender cuatro o cinco aplicaciones distintas de tratamiento de textos.

La conexión en red de los equipos también puede facilitar las tareas de soporte. Para el personal técnico, es mucho más eficiente dar soporte a una versión de un sistema operativo o aplicación y configurar todos los equipos del mismo modo que dar soporte a muchos sistemas y configuraciones individuales y diferentes.

# CAPITULO II

# MARCO TEÓRICO

## REDES DE COMUNICACIÓN

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios es un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros, todo ello desde una computadora personal.

Las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño e implantación de una red mundial de ordenadores es uno de los grandes milagros tecnológicos de las últimas décadas.

En general, todas las redes tienen ciertos componentes, funciones y características comunes. Éstos incluyen:

- Servidores: Equipos que ofrecen recursos compartidos a los usuarios de la red.
- Clientes: Equipos que acceden a los recursos compartidos de la red ofrecidos por los servidores.
- Medio: Los cables que mantienen las conexiones físicas.
- Datos compartidos: Archivos suministrados a los clientes por parte de los servidores a través de la red.
- Impresoras y otros periféricos compartidos: Recursos adicionales ofrecidos por los servidores.
- Recursos: Cualquier servicio o dispositivo, como archivos, impresoras u otros elementos, disponible para su uso por los miembros de la red.

Aun con estas similitudes, las redes se dividen en dos categorías principales.

- Redes trabajo en grupo.
- Redes basadas en servidor (cliente- servidor).

La diferencia entre las redes grupo de trabajo y las redes basadas en servidor es importante, ya que cada tipo presenta distintas capacidades. El tipo de red seleccionado para su instalación dependerá de factores tales como:

- El tamaño de la organización.
- El nivel de seguridad requerido.
- El tipo de negocio.
- El nivel de soporte administrativo disponible.
- La cantidad de tráfico de la red.
- Las necesidades de los usuarios de la red.
- El presupuesto de la red.

**Redes de Trabajo en Grupo.** En una red Trabajo en Grupo, no hay servidores dedicados, y no existe una jerarquía entre los equipos. Todos los equipos son iguales, y por tanto son «pares» (peers). Cada equipo actúa como cliente y servidor, y no hay un administrador responsable de la red completa. El usuario de cada equipo determina los datos de dicho equipo que van a ser compartidos en la red.

- Tamaño: Las redes Trabajo en Grupo (peer-to-peer) se llaman también grupos de trabajo (workgroups). El término "grupo de trabajo" implica un pequeño grupo de personas. Generalmente, una red Trabajo en Grupo abarca un máximo de diez equipos.
- Coste: Las redes Trabajo en Grupo son relativamente simples. Como cada equipo funciona como cliente y servidor, no hay necesidad de un potente servidor central o de los restantes componentes de una red de alta capacidad. Las redes Trabajo en Grupo pueden ser más económicas que las redes basadas en servidor.
- Sistemas operativos: En una red punto a punto, el software de red no requiere el mismo tipo de rendimiento y nivel de seguridad que el software de red diseñado para servidores dedicados. Los servidores dedicados sólo funcionan como servidores, y no como clientes o estaciones.

- Las redes Trabajo en Grupo están incorporadas en muchos sistemas operativos. En estos casos, no es necesario software adicional para configurar una red Trabajo en Grupo.
- Implementación: En entornos típicos de red, una implementación Trabajo en Grupo ofrece las siguientes ventajas:
    - Los equipos están en las mesas de los usuarios.
    - Los usuarios actúan como sus propios administradores, y planifican su propia seguridad.
    - Los equipos de la red están conectados por un sistema de cableado simple, fácilmente visible.

Las redes Trabajo en Grupo resultan una buena elección para entornos en los cuales:

- Hay como máximo 10 usuarios.
- Los usuarios comparten recursos, tales como archivos e impresoras, pero no existen servidores especializados.
- La seguridad no es una cuestión fundamental.
- La organización y la red sólo van a experimentar un crecimiento limitado en un futuro cercano.

Cuando se dan estos factores, puede que una red Trabajo en Grupo sea una mejor opción que una red basada en servidor.

Aunque puede que una red Trabajo en Grupo pueda cubrir las necesidades de pequeñas organizaciones, no resulta adecuada para todos los entornos. A continuación se describen algunas de las consideraciones que un planificador de redes necesita tener en cuenta antes de seleccionar el tipo de red a implementar.

Las tareas de administración de la red incluyen:

- Gestionar los usuarios y la seguridad.
- Asegurar la disponibilidad de los recursos.
- Mantener las aplicaciones y los datos.
- Instalar y actualizar software de aplicación y de sistema operativo.

En una red típica Trabajo en Grupo, no hay un responsable del sistema que supervise la administración de toda la red. En lugar de esto, los usuarios individuales administran sus propios equipos. Todos los usuarios pueden compartir cualquiera de sus recursos de la forma que deseen. Estos recursos incluyen datos en directorios compartidos, impresoras, tarjetas de fax, y demás.

En una red Trabajo en Grupo, cada equipo necesita:

- Utilizar un amplio porcentaje de sus recursos para dar soporte al usuario sentado frente al equipo, denominado usuario local.
- Usar recursos adicionales, como el disco duro y la memoria, para dar soporte a los usuarios que acceden a recursos desde la red, denominados usuarios remotos.

Aunque una red basada en servidor libera al usuario local de estas demandas, necesita, como mínimo, un potente servidor dedicado para cubrir las demandas de todos los clientes de la red.

En una red de equipos, la seguridad (hacer que los equipos y los datos almacenados en ellos estén a salvo de daños o accesos no autorizados) consiste en definir una contraseña sobre un recurso, como un directorio, que es compartido en la red. Todos los usuarios de una red Trabajo en Grupo definen su propia seguridad, y puede haber recursos compartidos en cualquier equipo, en lugar de únicamente en un servidor centralizado; de este modo, es muy difícil mantener un control centralizado. Esta falta de control tiene un gran impacto en la seguridad de la red, ya que puede que algunos usuarios no implementen ninguna medida de seguridad. Si la seguridad es importante, puede que sea mejor usar una red basada en servidor. Como cada equipo de un entorno Trabajo en Grupo puede actuar como servidor y cliente, los usuarios necesitan formación antes de que puedan desenvolverse correctamente como usuarios y administradores de sus equipos.

Redes Basadas en Servidor. En un entorno con más de 10 usuarios, una red Trabajo en Grupo (con equipos que actúen a la vez como servidores y clientes) puede que no resulte adecuada. Por tanto, la mayoría de las redes tienen servidores dedicados. Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación, Los servidores se llaman «dedicados» porque no son a su vez clientes, y porque están

optimizados para dar servicio con rapidez a peticiones de clientes de la red, y garantizar la seguridad de los archivos y directorios. Las redes basadas en servidor se han convertido en el modelo estándar para la definición de redes.

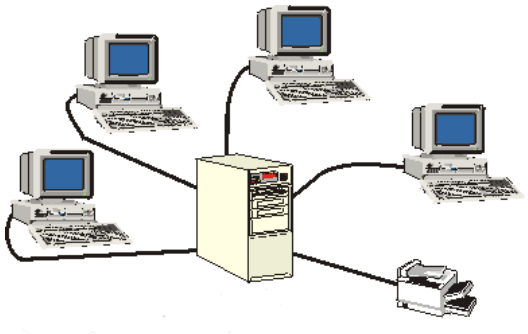


**Figura 2.1: Red Cliente- Servidor.**

A medida que las redes incrementan su tamaño (y el número de equipos conectados y la distancia física y el tráfico entre ellas crece), generalmente se necesita más de un servidor. La división de las tareas de la red entre varios servidores asegura que cada tarea será realizada de la forma más eficiente posible.

Los servidores necesitan realizar tareas complejas y variadas. Los servidores para grandes redes se han especializado para adaptarse a las necesidades de los usuarios. A continuación algunos ejemplos de los diferentes tipos de servidores incluidos en muchas redes de gran tamaño.

Servidores de archivos e impresión: Los servidores de archivos e impresión gestionan el acceso de los usuarios y el uso de recursos de archivos e impresión. Por ejemplo, al ejecutar una aplicación de tratamiento de textos, la aplicación de tratamiento de textos se ejecuta en su equipo. El documento de tratamiento de textos almacenado en el servidor de archivos e impresión se carga en la memoria del equipo, de forma que pueda editarlo o modificarlo de forma local. En otras palabras, los servidores de archivos e impresión se, utilizan para el almacenamiento de archivos y datos.

Servidores de aplicaciones: Los servidores de aplicaciones constituyen el lado servidor de las aplicaciones cliente/servidor, así como los datos, disponibles para los clientes. Por ejemplo, los servidores almacenan grandes cantidades de datos organizados para que resulte fácil su recuperación. Por tanto, un servidor de aplicaciones es distinto de un servidor de archivos e impresión. Con un servidor de archivos e impresión, los datos o el archivo son descargados al equipo que hace la petición. En un servidor de aplicaciones, la base de datos permanece en el servidor y sólo se envían los resultados de la petición al

equipo que realiza la misma. Una aplicación cliente que se ejecuta de forma local accede a los datos del servidor de aplicaciones. Por ejemplo, podría consultar la base de datos de empleados buscando los empleados que han nacido en noviembre. En lugar de tener la base de datos completa, sólo se pasará el resultado de la consulta desde el servidor a su equipo local.

Servidores de correo: Los servidores de correo funcionan como servidores de aplicaciones, en el sentido de que son aplicaciones servidor y cliente por separado, con datos descargados de forma selectiva del servidor al cliente.

Servidores de fax: Los servidores de fax gestionan el tráfico de fax hacia el exterior y el interior de la red, compartiendo una o más tarjetas módem fax.

Servidores de comunicaciones: Los servidores de comunicaciones gestionan el flujo de datos y mensajes de correo electrónico entre las propias redes de los servidores y otras redes, equipos mainframes, o usuarios remotos que se conectan a los servidores utilizando módems y líneas telefónicas.

Servidores de servicios de directorio: Los servidores de servicios de directorio permiten a los usuarios localizar, almacenar y proteger información en la red. Por ejemplo, cierto software servidor combina los equipos en grupos locales (llamados dominios) que permiten que cualquier usuario de la red tenga acceso a cualquier recurso de la misma.

La planificación para el uso de servidores especializados es importante con una red grande. El planificador debe tener en cuenta cualquier crecimiento previsto de la red, para que el uso de ésta no se vea perjudicado si es necesario cambiar el papel de un servidor específico.

Un servidor de red y su sistema operativo trabajan conjuntamente como una unidad. Independientemente de lo potente o avanzado que pueda ser un servidor, resultará inútil sin un sistema operativo que pueda sacar partido de sus recursos físicos. Los sistemas operativos avanzados para servidor, como los de Microsoft y Novell, están diseñados para sacar partido del hardware de los servidores más avanzados.

Aunque resulta más compleja de instalar, gestionar y configurar, una red basada en servidor tiene muchas ventajas sobre una red simple Trabajo en Grupo como por ejemplo:

Compartir recursos: Un servidor está diseñado para ofrecer acceso a muchos archivos e impresoras manteniendo el rendimiento y la seguridad de cara al usuario.

La compartición de datos basada en servidor puede ser administrada y controlada de forma centralizada. Como estos recursos compartidos están localizados de forma central, son más fáciles de localizar y mantener que los recursos situados en equipos individuales.

Seguridad: La seguridad es a menudo la razón primaria para seleccionar un enfoque basado en servidor en las redes. En un entorno basado en servidor, hay un administrador que define la política y la aplica a todos los usuarios de la red, pudiendo gestionar la seguridad.
Copia de seguridad: Las copias de seguridad pueden ser programadas varias veces al día o una vez a la semana, dependiendo de la importancia y el valor de los datos. Las copias de seguridad del servidor pueden programarse para que se produzcan automáticamente, de acuerdo con una programación determinada, incluso si los servidores están localizados en sitios distintos de la red.
Redundancia: Mediante el uso de métodos de copia de seguridad llamados sistemas de redundancia, los datos de cualquier servidor pueden ser duplicados y mantenidos en línea. Aún en el caso de que ocurran daños en el área primaria de almacenamiento de datos, se puede usar una copia de seguridad de los datos para restaurarlos.
Número de usuarios: Una red basada en servidor puede soportar miles de usuarios. Este tipo de red sería, imposible de gestionar como red Trabajo en Grupo, pero las utilidades actuales de monitorización y gestión de la red hacen posible disponer de una red basada en servidor para grandes cifras de usuarios.
Hardware: El hardware de los equipos cliente puede estar limitado a las necesidades del usuario, ya que los clientes no necesitan la memoria adicional (RAM) y el almacenamiento en disco necesarios para los servicios de servidor.

## CLASIFICACIÓN DE LAS REDES

Se denomina red de computadores una serie de host (terminales) autónomos y dispositivos especiales intercomunicados entre sí. Ahora bien, este concepto genérico de red incluye multitud de tipos diferentes de redes y posibles configuraciones de las mismas, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de red concretas.

Las posibles clasificaciones de las redes pueden ser muchas, atendiendo cada una de ellas a diferentes propiedades, siendo las más comunes y aceptadas las siguientes:

### Clasificación de las redes según su tamaño y extensión:

1. Redes LAN. Las redes de área local (Local Area Network) son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas, que generalmente usan la tecnología

de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps (Megabits por segundo).

2. Redes MAN. Las redes de área metropolitana (Metropolitan Area Network) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en un mismo área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.

3. Redes WAN. Las redes de área amplia (Wide Area Network) tienen un tamaño superior a una MAN, y consisten en una colección de host o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de rutear o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un router a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros.

4. Redes Internet. Es una red de redes, vinculadas mediante ruteadores gateways. Un gateway o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10.000 kilómetros en adelante, y su ejemplo más claro es Internet, la red de redes mundial.

5. Redes inalámbricas. Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo, lo que las diferencia de las redes anteriores. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

**Clasificación de las redes según el tipo de transferencia de datos que soportan:**

- Redes de transmisión simple. Son aquellas redes en las que los datos sólo pueden viajar en un sentido.
- Redes Half-Duplex. Aquellas en las que los datos pueden viajar en ambos sentidos, pero sólo en uno de ellos en un momento dado. Es decir, sólo puede haber transferencia en un sentido a la vez.
- Redes Full-Duplex. Aquellas en las que los datos pueden viajar en ambos sentidos a la vez.

## ESTÁNDARES DE IEEE 802.XX

Los estándares de redes de área local definidos por los comités 802 se clasifican en 16 categorías que se pueden identificar por su número acompañado del 802:

Los comités 802 o proyecto 802, del IEEE, poseen el estándares de comunicación de dispositivos en una LAN. Su objetivo principal es asegurar las compatibilidades entre los productos de distintos fabricante, definiendo las normas de las LAN. Muchas de ellas son también normas de ISO. El modelo IEEE, solo estandariza los niveles físico y de enlace.

- Nivel físico: igual que en el modelo OSI, trata lo relacionado con el medio de transmisión, la conexión, señales eléctricas, etc.
- Nivel de enlace: LLC (logical link control). Control de enlace lógico. Su objetivo es manejar distintos tipos de servicios de comunicación que se pueden ofrecer a través del medio. MAC (media access control). Control de acceso al medio. Ofrece la dirección física del equipo conectado a la red y los mecanismos utilizados para el uso del medio.

**IEEE 802.1.** Interfaz de niveles superiores (Higher-layer interface), recomendaciones de interconexión de redes y funciones de gestión y establece los estándares de interconexión relacionados con la gestión de redes.

**IEEE 802.1q.** Redes virtuales (VLAN). Es un grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración) comunicándose entre ellos aunque estén localizados segmentos diferentes de LAN. Esto es porque VLANs están basadas en las conexiones lógicas en lugar de las físicas.

**IEEE 802.2.** Control de enlace lógico (logical Link Control). Relativo al establecimiento, mantenimiento y terminación de enlaces lógicos entre nodos de una comunicación. Define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: los niveles LLC y MAC. El nivel MAC varía en función de los diferentes tipos de red y está definido por el estándar IEEE 802.3.

**IEEE 802.3.** (Ethernet) Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, carrier-sense multiple access with collision detection). Define el nivel MAC para redes de bus que utilizan Acceso múltiple por detección de portadora con

detección de colisiones (CSMA/CD, Carrier-Sense Multiple Access with Collision Detection). Éste es el estándar Ethernet.

**IEEE 802.3u.** Fast Ethernet 100Base-X a velocidad de 100 Mbps. 100-BASEX puede implementarse con las siguientes opciones:

- 100BASE-TX: Utilizando cable STP o UTP (2 pares) a 100 Mbps..
- 100BASE-FX: Utilizando dos cables de fibra óptica, con comunicación dúplex de 100 Mbps.
- IEEE 802.3z: Incluye velocidad de 1000 Mbps.

**IEEE 802.4.** Define el nivel MAC para redes de bus que utilizan un mecanismo de paso de testigo (red de área local Token Bus).

**IEEE 802.5.** Token Ring. Acceso mediante el paso de un testigo en una topología de anillo. Define el nivel MAC para redes Token Ring (red de área local Token Ring).

**IEEE 802.6.** Establece estándares para redes de área metropolitana (MAN, Metropolitan Area Networks), que son redes de datos diseñadas para poblaciones o ciudades. En términos de extensión geográfica, las redes de área metropolitana (MAN) son más grandes que las redes de área local (LAN), pero más pequeñas que las redes de área global (WAN). Las redes de área metropolitana (MAN) se caracterizan, normalmente, por conexiones de muy alta velocidad utilizando cables de fibra óptica u otro medio digital.

**IEEE 802.7.** Utilizada por el grupo asesor técnico de banda ancha (Broadband Technical Advisory Group).

**IEEE 802.8.** Fibra óptica (Optical fiber technoloy). Estándar de la interfaz de datos distribuidos por fibra (FDDI, Fiber Distributed Data Interface. Utilizada por el grupo asesor técnico de fibra óptica (Fiber-Optic Technical Advisory Group).

**IEEE 802.9.** Integración de voz y datos en redes locales. Incluye RDSI. Define las redes integradas de voz y datos.

**IEEE 802.10**. Define la seguridad de las redes.

**IEEE 802.11.** Redes locales inalámbricas. Define los estándares de redes sin cable.

**802.11a:**

- Ancho de banda máximo de hasta 2 Mbps.
- Opera en el espectro de 5 Ghz sin necesidad de licencia.
- Posible interferencia con hornos microondas, dispositivos bluetooth, y teléfonos DECT, puesto que operan en el mismo espectro de frecuencias.

**802.11b:**

- Ancho de banda máximo de hasta 11Mbps.
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Las mismas interferencias que para 802.11.
- Conocido como WIFI.
- Modulación DSSS.
- Compatible con los equipos DSSS del estándar 802.11.

**802.11g:**

- Ancho de banda máximo de hasta 54 Mbps
- Opera en el espectro de 2.4 Ghz sin necesidad de licencia.
- Compatible con 802.11b.
- Modulación DSSS y OFDM

**802.11**:

- Ancho de banda máximo de hasta 54 Mbps.
- Opera en el espectro de 5 Ghz sin necesidad de licencia.
- Menos saturado.
- No es compatible con 802.11b y 802.11g.
- Modulación de OFDM.

**802.11e:**

- Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN.
- Se aplicará a los estándares físicos a, b y g de 802.11.

- La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.

**802.11i:**

- Se refiere al objetivo mas frecuente del estándar 802.11, la seguridad.
- Se aplica a los estándares físicos a, b y g de 802.11.
- Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación.
- IEEE 802.1x constituye una parte clave de 802.11i.

**802.11d.** Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

**802.11f:** Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN mutiproveedor. El estándar define el registro e Puntos de Acceso (AP) dentro de una red y el intercambio de información entre dichos Puntos de Acceso cuando un usuario se traslada desde un punto de acceso a otro.

**802.11h:** El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tendrán control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

**IEEE 802.12:**

- Incluye 100VG-AnyLAN.
- Comité para formar el estándar do 100 base VG quo sustituye CSMA/CD por asignación de prioridades

**IEEE 802.14:**

- Sistemas híbridos de coaxial y fibra. Acceso de los usuarios a banda ancha.

- Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.

**IEEE 802.15.** Define las redes de área personal sin cable (WPAN, Wireless Personal Area Networks).

**IEEE 802.16.** Define los estándares sin cable de banda ancha.

**ESTÁNDARES DE CABLES UTP/STP**

Cat 1: Actualmente no reconocido por TIA/EIA. Previamente usado para comunicaciones telefónicas POTS, ISDN y cableado de timbrado.

Cat 2: Actualmente no reconocido por TIA/EIA. Previamente fue usado con frecuencia en redes token ring de 4 Mbit/s.

Cat 3: Actualmente definido en TIA/EIA-568-B, usado para redes de datos usando frecuencias de hasta 16 MHz. Históricamente popular (y todavía usado) para redes ethernet de 10 Mbit/s.

Cat 4: Actualmente no reconocido por TIA/EIA. Posee performance de hasta 20 MHz, y fue frecuentemente usado en redes token ring de 16 Mbit/s.

Cat 5: Actualmente no reconocido por TIA/EIA. Posee performance de hasta 100 MHz, y es frecuentemente usado en redes ethernet de 100 Mbit/s ethernet networks. Es posible usarlo para ethernet de gigabit 1000BASE-T.

Cat 5e: Actualmente definido en TIA/EIA-568-B. Posee performance de hasta 100 MHz, y es frecuentemente usado tanto para ethernet 100 Mbit/s como para ethernet 1000 Mbit/s (gigabit).

Cat 6: Actualmente definido en TIA/EIA-568-B. Posee performance de hasta 250 MHz, más del doble que las categorías 5 y 5e. Usado principalmente para Gigabit

Cat 6a: Especificación futura para aplicaciones de 10 Gbit/s.

Cat 7: Nombre informal aplicado a cableado de clase F de ISO/IEC 11801. Este estándar especifica 4 pares blindados individualmente dentro de otro blindaje. Diseñado para transmisión a frecuencias de hasta 600 MHz.

## PROTOCOLOS DE REDES

Un protocolo de red es como un lenguaje para la comunicación de información. Son las reglas y procedimientos que se utilizan en una red para comunicarse entre los nodos que tienen acceso al sistema de cable. Los protocolos gobiernan dos niveles de comunicaciones:

- Los protocolos de alto nivel: Estos definen la forma en que se comunican las aplicaciones.
- Los protocolos de bajo nivel: Estos definen la forma en que se transmiten las señales por cable.

Los protocolos de red son una o más normas estándar que especifican el método para enviar y recibir datos entre varios ordenadores. Su instalación esta en correspondencia con el tipo de red y el sistema operativo que la computadora tenga instalado.

No existe un único protocolo de red, y es posible que en un mismo ordenador coexistan instalados varios de ellos, pues cabe la posibilidad que un mismo ordenador pertenezca a redes distintas. La variedad de protocolos puede suponer un riesgo de seguridad: cada protocolo de red que se instala en un sistema queda disponible para todos los adaptadores de red existentes en dicho sistema, físicos (tarjetas de red o módem) o lógicos (adaptadores VPN). Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no deseado a los recursos de la red. En estos casos, la regla de seguridad más sencilla es tener instalados el número de protocolos indispensable; en la actualidad y en la mayoría de los casos debería bastar con sólo TCP/IP.

Dentro de la familia de protocolos se pueden distinguir:

**Protocolos de transporte:**

- ATP (Apple Talk Transaction Protocol).
- NetBios/ NetBEUI.
- TCP (Transmission Control Protocol).

**Protocolos de red:**

- DDP (Delivery Datagram Protocol).

- IP (Internet Protocol).
- IPX (Internet Packed Exchange).
- NetBEUI Desarrollado por IBM y Microsoft.

**Protocolos de aplicación:**

- AFP (Appletalk File Protocol).
- FTP (File Transfer Protocol).
- Http (Hyper Text transfer Protocol).

Dentro de los protocolos antes mencionados, los más utilizados son:

IPX/SPX, protocolos desarrollados por Novell a principios de los años 80 los cuales sirven de interfaz entre el sistema operativo de red Netware y las distintas arquitecturas de red. El protocolo IPX es similar a IP, SPX es similar a TCP por lo tanto juntos proporcionan servicios de conexión similares a TCP/IP.

NETBEUI/NETBIOS (Network Basic Extended User Interface / Network Basic Input/Output System) NETBIOS es un protocolo de comunicación entre ordenadores que comprende tres servicios (servicio de nombres, servicio de paquetes y servicio de sesión, inicialmente trabajaba sobre el protocolo NETBEUI, responsable del transporte de datos. Actualmente con la difusión de Internet, los sistemas operativos de Microsoft más recientes permiten ejecutar NETBIOS sobre el protocolo TCP/IP, prescindiendo entonces de NETBEUI.

APPLE TALK es un protocolo propietario que se utiliza para conectar computadoras Macintosh de Apple en redes locales.

TCP/IP (Transmission Control Protocol/Internet Protocol) este protocolo fue diseñado a finales de los años 60, permite enlazar computadoras con diferentes sistemas operativos. Es el protocolo que utiliza la red de redes Internet.

Como es frecuente en el caso de las computadoras el constante cambio, también los protocolos están en continuo cambio. Actualmente, los protocolos más comúnmente utilizados en las redes son Ethernet, Token Ring y ARCNET. Cada uno de estos esta diseñado para cierta clase de topología de red y tienen ciertas características estándar.

**Ethernet**

El sistema de texto Ethernet fue originalmente creado por Xerox, pero desarrollado conjuntamente como una norma en 1.980 por Digital, Intel y Xerox. La norma 802.3 de IEEE define una red similar, aunque ligeramente diferente que usa un formato alternativo de trama. Ethernet presenta un rendimiento de 10 Mbits/seg. y utiliza un método sensible a la señal portadora mediante el cual las estaciones de trabajo comparten un cable de red, pero sólo una de ellas puede utilizarlo en un momento dado. El método de acceso múltiple con detección de portadora y detección de colisiones se utiliza para arbitrar el acceso al cable.

Las redes Ethernet pueden ser cableadas con diferentes tipos de cable. Cada uno con sus ventajas e inconvenientes. Las tres especificaciones más populares para Ethernet son las siguientes:

**Ethernet 10 Base-T.** Ofrece la mayoría de las ventajas de Ethernet sin las restricciones que impone el cable coaxial. Parte de esta especificación es compatible con otras normas 802.3 del IEEE de modo que es sencillo realizar una transición de un medio a otro. Es posible mantener las mismas tarjetas Ethernet al pasar de un cable coaxial a cable de par trenzado. Además pueden añadirse líneas troncales de par trenzado a las ya existentes gracias a repetidores que admiten la conexión de líneas troncales de cable coaxial, fibra óptica y par trenzado. Muchos fabricantes presentan este tipo de dispositivos en su línea de productos Ethernet. La especificación 10 Base-T incluye una utilidad de verificación de cableado denominada Verificación de integridad del enlace.

**Ethernet 10 Base-2.** Se utiliza cable coaxial fino que se manipula más fácilmente que el grueso y no requiere transceptores en las estaciones. Este cable es más barato, aunque la longitud máxima de la línea troncal es menor.

**Ethernet 100 Base-X**. Con el crecimiento del uso de la multimedia y el vídeo de alta definición en tiempo real, además del correo electrónico que incorpora estos formatos, existe una necesidad creciente de obtención de mayores anchos de banda en los equipos. Los usuarios de aplicaciones de diseño asistidos por ordenador requieren siempre un alto ancho de banda. 100 BASE-X mantiene el método de acceso CSMA/CD sobre cable de par trenzado sin blindar de categoría 5 o superior. El comité 802.3.del IEEE es el responsable de este desarrollo.

**Token Ring.** El anillo con testigo es la norma 802.5 del IEEE. Una red en anillo con paso de testigo se puede configurar en una topología en estrella. IBM hizo posible la norma con la comercialización de la primera red Token Ring a 4 Mbit/seg. a mediados de los 80. Aunque la red físicamente aparece como una configuración en estrella, internamente, las señales viajan alrededor de la red de una estación a la siguiente. Por tanto, la configuración del cableado y la adición o supresión de un equipo debe asegurar que se mantiene el anillo lógico. Las estaciones de trabajo se conectan a los concentradores centrales llamados unidades de acceso multiestación (MAU). Para crear redes grandes se conectan múltiples concentradores juntos. Las tarjetas de Token Ring de IBM están disponibles en una versión a 4 Mbit/seg. y en otra a 16 Mbit/seg. Son comunes el cable de par trenzado no apantallado y las MAUS con 16 puertos.

**Arcnet.** La red de computación de recursos conectados ARCNET es un sistema de red banda base con paso de testigo que ofrece topologías flexibles de estrella y bus a un precio bajo. Las velocidades de transmisión son de 2,5 Mbit/seg. y en ARCNET Plus de 20 Mbit/seg.

ARCNET proporciona una red robusta que no es tan susceptible a fallos como la Ethernet de cable coaxial si el cable se suelta o se desconecta. Esto se debe particularmente a su topología y a su baja velocidad de transferencia. Si el cable que une una estación de trabajo a un concentrador se desconecta o se suelta, sólo dicha estación de trabajo se va abajo, no la red entera. El protocolo de paso de testigo requiere que cada transacción sea reconocida, de este modo no hay cambios virtuales de errores aunque el rendimiento es mucho más bajo que en otros esquemas de conexión de red.

## TOPOLOGÍA DE UNA RED

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores.

A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades, teniendo en cuenta factores como la distribución de los equipos a interconectar, tipo de aplicaciones que se van a ejecutar, inversión que se quiere hacer, coste que se quiere dedicar al mantenimiento y actualización de la red, tráfico que debe soportar la red, capacidad de expansión, entre otros.

Las topologías puras son tres: topología en bus, en estrella y en anillo. A partir de estas tres se generan otras como son: anillo - estrella, bus - estrella, etc.

**Topología de bus.** La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

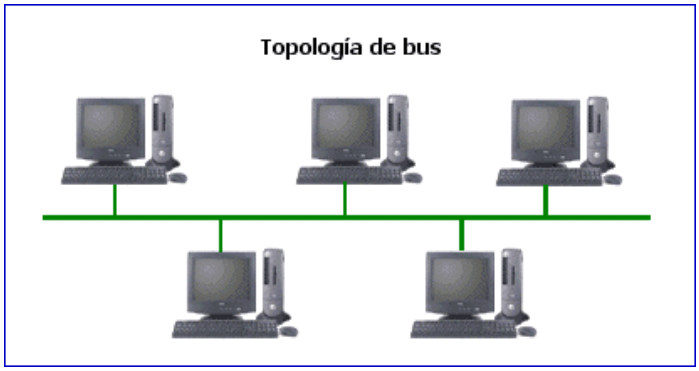



**Figura 2.2: Topología de Bus.**

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

**Topología de anillo.** Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes.


**Figura 2.3: Topología en Anillo.**

Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

*Topología De Anillo Doble.-* Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, para incrementar la confiabilidad y flexibilidad de la red, hay un segundo anillo redundante que conecta los mismos dispositivos. La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

**Topología en estrella.** La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub o Switch, pasa toda la información que circula por la red.

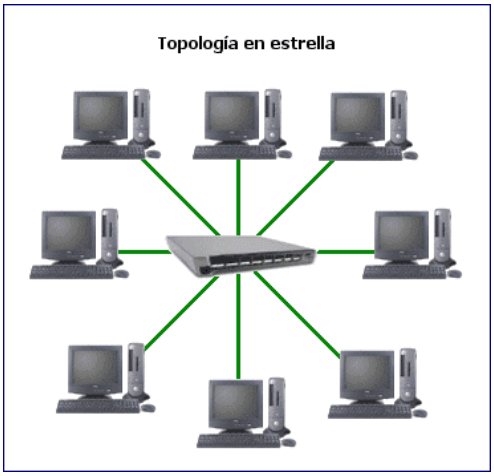



**Figura 2.4: Topología en Estrella.**

La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

**Topología En Estrella Extendida.** La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

**Topología en árbol.** La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

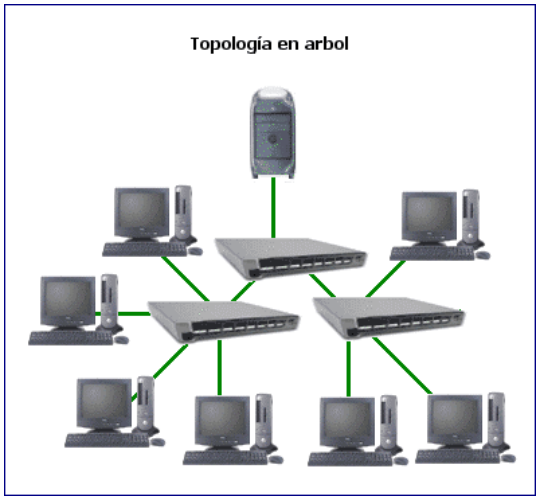



**Figura 2.5: Topología en Árbol.**

El enlace troncal es un cable con varias capas de ramificaciones, y el flujo de información es jerárquico. Conectado en el otro extremo al enlace troncal generalmente se encuentra un host servidor.

**Topología en malla completa.** En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

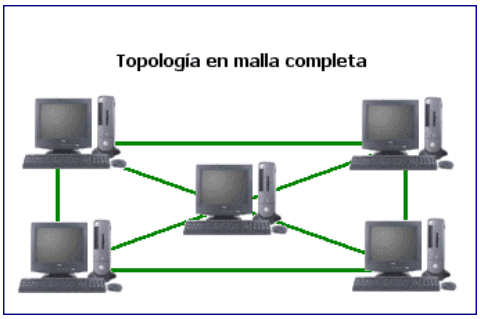



**Figura 2.6: Topología en Malla Completa.**

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

## REDES WLAN (WIRELESS LAN)

Las redes de área local inalámbricas (WLANs) constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación como UMTS y LMDS, pues éstas requieren de un importante desembolso económico previo por parte de los operadores del servicio. Ahora bien, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

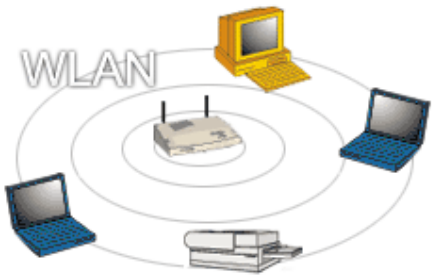



**Figura 2.7: Red Wireless Lan (WLAN).**

Originalmente las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno residencial y del hogar, grandes redes corporativas, PYMES, zonas industriales, campus universitarios, entornos hospitalarios, ciber-cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet.

Básicamente, una red WLAN permite reemplazar por conexiones inalámbricas los cables que conectan a la red los PCs, portátiles u otro tipo de dispositivos, dotando a los usuarios de movilidad en las zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes: terminales de usuario o Clientes (dotados de una tarjeta interfaz de red que integra un transceptor de radiofrecuencia y una antena), puntos de acceso y

controladores de puntos de acceso, que incorporan funciones de seguridad, como autorización y autenticación de usuarios, firewall, etc.

El futuro de la tecnología WLAN pasa necesariamente por la resolución de cuestiones muy importantes sobre seguridad e interoperabilidad, en donde se centran actualmente la mayor parte de los esfuerzos. Sin embargo, desde el punto de vista de los usuarios, también es importante reducir la actual confusión motivada por la gran variedad de estándares existentes.

**ESTÁNDARES DE WLAN**

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (Institute of Electrical and Electronics Engineers) y la ETSI (European Telecommunications Standards Institute). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

Entre los principales estándares se encuentran:

- IEEE 802.11: El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.
- IEEE 802.11a: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- IEEE 802.11b: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.
- HiperLAN2: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.
- HomeRF: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

| Estándar | Velocidad máxima | Interfase de aire | Ancho de banda de canal | Frecuencia |
|---|---|---|---|---|
| 802.11b | 11 Mbps | DSSS | 25 MHz | 2.4 GHz |
| 802.11a | 54 Mbps | OFDM | 25 MHz | 5.0 GHz |
| 802.11g | 54 Mbps | OFDM/DSSS | 25 MHz | 2.4 GHz |
| HomeRF2 | 10 Mbps | FHSS | 5 MHz | 2.4 GHz |
| HiperLAN2 | 54 Mbps | OFDM | 25 MHz | 5.0 GHz |
| 5-UP | 108 Mbps | OFDM | 50 MHz | 5.0 GHz |

**Tabla 2.1: Principales estándares WLAN.**

DSSS: Direct Sequence Spread Spectrum.
OFDM: Orthogonal Frequency Division Multiplexing.
FHSS: Frequency Hopping Spread Spectrum.
5-UP: 5-GHz Unified Protocol (5-UP), Protocolo Unificado de 5 GHz propuesto por Atheros Communications.

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varía de país a país. La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión. Estos errores ocasionan que sean reenviados una y otra vez los paquetes de información. Una razón de error del 50% ocasiona que se reduzca el caudal eficaz real (throughput) dos terceras partes aproximadamente. Por eso la velocidad máxima especificada teóricamente no es tal en la realidad. Si la especificación IEEE 802.11b nos dice que la velocidad máxima es 11 Mbps, entonces el máximo caudal eficaz será aproximadamente 6 Mbps y menos.

Para reducir errores, el 802.11a y el 802.11b automáticamente reducen la velocidad de información de la capa física. Así por ejemplo, el 802.11b tiene tres velocidades de información (5.5, 2 y 1 Mbps) y el 802.11a tiene 7 (48, 36, 24, 18, 12, 9 y 6 Mbps). La velocidad máxima permisible sólo es disponible en un ambiente libre de interferencia y a muy corta distancia.

La transmisión a mayor velocidad del 802.11a no es la única ventaja con respecto al 802.11b. También utiliza un intervalo de frecuencia más alto de 5 GHz. Esta banda es más ancha y menos atestada que la banda de 2.4 GHz que el 802.11b comparte con teléfonos

inalámbricos, hornos de microondas, dispositivos Bluetooth, etc. Una banda más ancha significa que más canales de radio pueden coexistir sin interferencia.

Sin bien, la banda de 5 GHz tiene muchas ventajas, también tiene sus problemas. Las diferentes frecuencias que utilizan ambos sistemas significan que los productos basados en 802.11a no son interoperables con los 802.11b. Esto significa que aunque no se interfieran entre sí, por estar en diferentes bandas de frecuencias, los dispositivos no pueden comunicarse entre ellos. Para evitar esto, la IEEE desarrolló un nuevo estándar conocido como 802.11g, el cual extenderá la velocidad y el intervalo de frecuencias del 802.11b para así hacerlo totalmente compatible con los sistemas anteriores. Sin embargo, no será más rápido que el estándar 802.11a y según políticas de los fabricantes han retardado el estándar 801.11g. La demora en la ratificación del 802.11g ha obligado a muchos fabricantes irse directamente por el 802.11a donde existe una gran variedad de fabricantes de chips [circuitos integrados] tales como Atheros, National Semiconductor, Resonext, Envara, inclusive Cisco Systems quien adquirió a Radiata, la primer compañía en desarrollar un prototipo en 802.11a en el 2000.

Como otro intento de permitir la interoperatibilidad entre los dispositivos de bajas y altas velocidades, la compañía Atheros Comunications, Inc. (http://www.atheros.com/) propuso unas mejoras a los estándares de WLANs de la IEEE y la ETSI. Este nuevo estándar conocido como 5-UP (5 GHz Unified Protocol) permite la comunicación entre dispositivos mediante un protocolo unificado a velocidades de hasta 108 Mbps.

Ambas especificaciones, la 802.11a (IEEE) y la HiperLAN2 (ETSI) son para WLANs de alta velocidad que operan en el intervalo de frecuencias de 5.15 a 5.35 GHz. La propuesta de Atheros es para mejorar esos protocolos y proveer compatibilidad hacia atrás para productos que cumplan con las especificaciones existentes, además de permitir nuevas capacidades. El radio espectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos; dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20 MHz para un segmento de red soporta 54 Mbps de caudal eficaz compartido entre los dispositivos en el segmento en un tiempo dado.

**HARDWARE PARA WLAN**

- *Cliente:* cada ordenador que acceda a la red como cliente debe estar equipado con una tarjeta WiFi. Las más comunes son de tipo PC Card (para portátiles) aunque pueden conectarse a una ranura PCI estándar mediante una tarjeta adaptadora.
- *Punto de Acceso:* hace las veces del hub o switch tradicional. Envía cada paquete de información directamente al ordenador indicado con lo que mejora sustancialmente la velocidad y eficiencia de la red. Es normalmente una solución hardware.
- *Antena:* se utilizan solamente para amplificar la señal, así que no siempre son necesarias. Las antenas direccionales emiten en una sola dirección y es preciso orientarlas "a mano". Dentro de este grupo están las de Rejilla, las Yagi, las parabólicas, las "Pringles" y las de Pane. Las antenas omnidireccionales emiten y reciben señal en 360º.
- *Pigtail:* es simplemente el cable que conecta la antena con la tarjeta de red. Es el único cable necesario en una WLAN y hay que vigilar posibles pérdidas de señal.

**TOPOLOGÍA DE LAS REDES WLAN**

Depende de la funcionalidad con la que se desee montar este tipo de redes, se puede hacer de 2 modos distintos: Ad-Hoc o lo que es lo mismo, redes punto a punto o bien por infraestructura.

**Redes Ad-Hoc (punto a punto).** El estándar denomina a este modo como un servicio básico independiente (IBSS) con un coste bajo y flexible. Las comunicaciones entre los múltiples nodos se establecen sin el uso de ningún servidor u otro medio como pueden ser los puntos de acceso o Access Point (AP).

Uno de los métodos básicos para encaminar paquetes en este modo, seria tratando a cada uno de los nodos que forman la red como un router y utilizando entre ellos un protocolo convencional (como puede ser los basados en el vector de distancia) para encaminarlos hacia su destino.

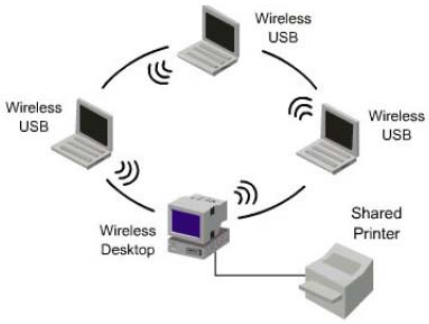



**Figura 2.8: Redes Punto a Punto.**

**Redes de infraestructura.** En este modo, cada cliente de la red envía todas sus comunicaciones a una central o punto de acceso (AP, Access Point). Para efectuar el intercambio de datos, previamente los clientes y los puntos de acceso establecen una relación de confianza.

Los APs, pueden emplearse dentro de la Wireless Lan como:

- Gateway: para redes externas (Internet, intranet, etc.).
- Bridge: hacia otros Access Points para extender los servicios de acceso.
- Router: de datos entre el área de cobertura, abarcando los 100-150mts en un entorno cerrado (dependiendo de la disposición y objetos que bloqueen las ondas de radio) o los 300mts en espacios abiertos.

Estos puntos de acceso tienen un límite de 64 NICs (Network Interface Cards) dentro de su área de actuación. Para paliar este problema se opta por poner en funcionamiento varios APs al mismo tiempo, ampliando así las posibilidades de roaming de un equipo móvil sin perder la conexión.

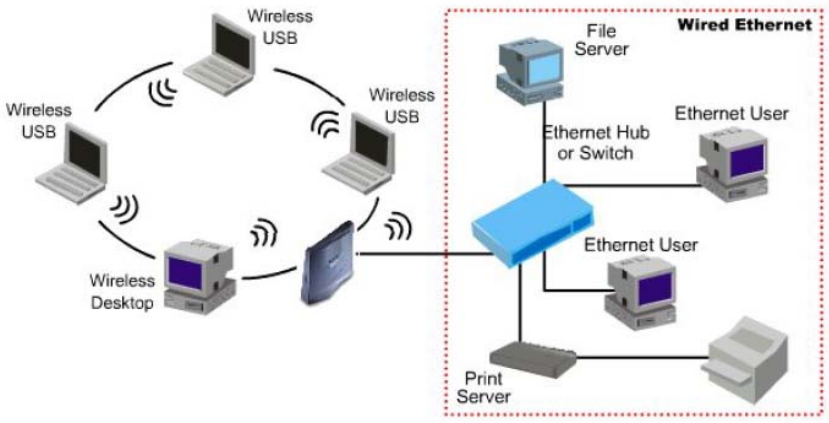



**Figura 2.9: Redes WLAN y LAN.**

## SEGURIDADES DE WLANS

**WEP (Protocolo de equivalencia con red cableada).** La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.

Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 13 dígitos alfanuméricos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

**WPA (Wi-Fi Protected Access).** WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos

alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

**Para el uso personal doméstico.** El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

**Para el uso en empresarial/de negocios.** El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

*WPA2* es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 es compatible tanto con la versión para la empresa como con la doméstica.

La tecnología SecureEasySetup™ (SES) de Linksys o AirStation OneTouch Secure System™ (AOSS) de Buffalo permite al usuario configurar una red y activar la seguridad de Acceso protegido Wi-Fi (WPA) simplemente pulsando un botón. Una vez activado, SES o AOSS crea una conexión segura entre sus dispositivos inalámbricos, configura automáticamente su red con un Identificador de red inalámbrica (SSID) personalizado y habilita los ajustes de cifrado de la clave dinámico de WPA. No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña ni clave asociada con una configuración de seguridad tradicional inalámbrica.

**RED PRIVADA VIRTUAL (VPN).**

Hace unos años no era tan importante conectarse a Internet por motivos laborables, pero a medida que ha pasado el tiempo las corporaciones han requerido que las redes de área local (Local Area Network, LAN) trasciendan más allá del ámbito local para incluir personal y centros de información de otros edificios, ciudades, estados e incluso otros países. En contrapartida, era necesario invertir en hardware, software y en servicios de telecomunicaciones costosos para crear redes amplias de servicio (Wide Area Network, WAN). Sin embargo, con Internet, las corporaciones tienen la posibilidad de crear una red privada virtual (VPN) que demanda una inversión relativamente baja utilizando Internet para la conexión entre diferentes localidades o puntos.

Las VPNs utilizan protocolos especiales de seguridad que permiten, únicamente al personal autorizado, obtener acceso a servicios privados de una organización: cuando un empleado se conecta a Internet, la configuración VPN le permite conectarse a la red privada de la Compañía y navegar en la red como si estuvieran localmente en la oficina.

Una de las necesidades vitales de la empresa moderna es la posibilidad de compartir información, particularmente para aquellas empresas que se encuentran dispersas, con sedes en diferentes zonas y unidades de negocio que no se encuentran en el mismo entorno físico. Hasta el momento, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de empresas de menor tamaño y con recursos económicos y técnicos más escasos.

Sin embargo, desde hace ya un tiempo, aparece un nuevo término: VPN – Virtual Private Network (red privada virtual), el cual no es en realidad, ninguna novedad tecnológica, sino una nueva fórmula de interconexión con tecnologías de menor costo.

Una VPN (Virtual Private Network) es una estructura de red corporativa implantada sobre una red de recursos de transmisión y conmutación públicas, que utiliza la misma gestión y políticas de acceso que se utilizan en las redes privadas. En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay. Adicionalmente, puede definirse como una red privada que se extiende, mediante procesos de encapsulación y cifrado, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte, como la Internet.

Las funcionalidades de una VPN están definidas más que por el protocolo de transporte WAN, por los dispositivos instalados en sus extremos, encargados de realizar la conexión con los elementos de la red de área local, en los puntos remotos a través de la WAN. Las VPN pueden enlazar las oficinas corporativas con aliados comerciales o asociados de negocio, usuarios móviles y sucursales remotas, mediante canales de comunicación seguros utilizando protocolos como IPSec (IP Secure), como se muestra en la Figura 2.10.

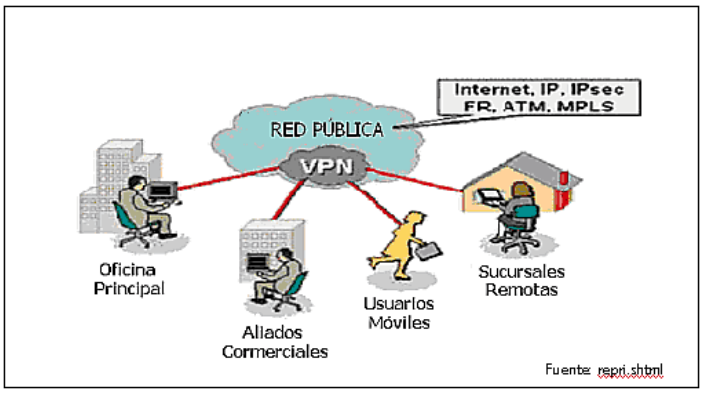



**Figura. 2.10: Conexión de la Red Corporativa a través de una VPN.**

**SEGURIDAD EN UN "TÚNEL" PRIVADO.**

Los paquetes de datos de una VPN viajan por medio de un "túnel" definido en la red pública. El túnel es la conexión definida entre dos puntos en modo similar a como lo hacen los circuitos en una topología WAN basada en paquetes. A diferencia de los protocolos orientados a paquetes, capaces de enviar los datos a través de una variedad de rutas antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel, tal como se muestra en la Figura 2.11.

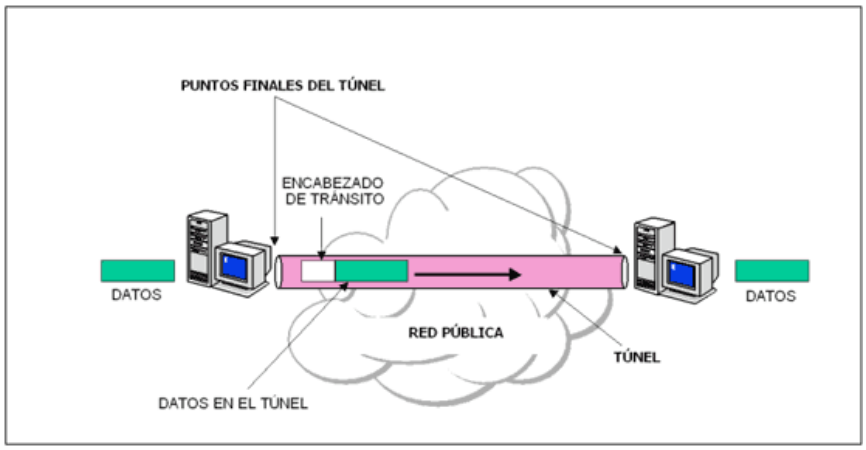



**Figura. 2.11: Túnel en una VPN.**

Adicionalmente las VPNs emplean el túnel con propósitos de seguridad. Los paquetes utilizan inicialmente funciones de cifrado, autenticación o integridad de datos, y después se encapsulan en paquetes IP (Internet Protocol). Posteriormente los paquetes son descifrados en su destino. Entre los principales protocolos utilizados para el proceso de "tunneling" se pueden mencionar:

**PPTP (Point-To-Point Tunneling Protocol).** PPTP es un protocolo de red que permite la realización de transferencias desde clientes remotos a servidores localizados en redes privadas. Para ello emplea tanto líneas telefónicas conmutadas como Internet. PPTP es una extensión de PPP que soporta control de flujos y túnel multiprotocolo sobre IP.

**L2f (Layer 2 Forwarding).** El protocolo L2F tiene como objetivo proporcionar un mecanismo de "tunneling" para el transporte de tramas a nivel de enlace: HDLC, PPP, SLIP, etc. El proceso de "tunneling" involucra tres protocolos diferentes: el protocolo pasajero representa el protocolo de nivel superior que debe encapsularse; el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación (el protocolo encapsulador es L2F); y el protocolo portador será el encargado de realizar el transporte de todo el conjunto.

**L2tp (Layer 2 Tunneling Protocol).** Encapsula características PPTP y L2F como un todo, resolviendo los problemas de interoperatividad entre ambos protocolos. Permite el túnel del nivel de enlace de PPP, de forma que los paquetes IP, IPX y AppleTalk enviados de forma privada, puedan ser transportados por Internet. Para seguridad de los datos se apoya en IPSec.

**IPSec (IP Secure).** Protocolo de seguridad que opera sobre la capa de red que proporciona un canal seguro para los datos. Ofrece integridad, autenticación, control de acceso y confidencialidad para el envío de paquetes IP por Internet.

**CATEGORÍAS DE VPN.**

Las VPN pueden dividirse en tres categorías, a saber:

**VPN de Acceso Remoto**. Conectan usuarios móviles con mínimo tráfico a la red corporativa. Proporcionan acceso desde una red pública, con las mismas políticas de la red privada. Los accesos pueden ser tanto sobre líneas analógicas, digitales, RDSI o DSL.

**VPN de Intranet.** Permite conectar localidades fijas a la red corporativa usando conexiones dedicadas.

**VPN de Extranet.** Proporciona acceso limitado a los recursos de la corporación a sus aliados comerciales externos como proveedores y clientes, facilitando el acceso a la información de uso común para todos a través de una estructura de comunicación pública.

**FIREWALL**

Un firewall es un dispositivo de seguridad, a continuación se detalla exactamente lo que hace y en que se basa su funcionamiento.

Un firewall es un dispositivo que funciona como un muro entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de Web, correo y Ftp, pero no a IRC que puede ser innecesario para el trabajo. También se

puede configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la Web, (si es que se posee un servidor Web y si se quiere que sea accesible desde Internet). Dependiendo del firewall que se tenga también se podrá permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparato que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el módem que conecta con Internet. Incluso se puede encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes.


**Figura. 2.12. Firewall.**

También es frecuente conectar al cortafuego una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

## TIPOS DE CORTAFUEGOS

**Cortafuegos de capa de red o de filtrado de paquetes.** Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

**Cortafuegos de capa de aplicación.** Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuego a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a Internet de una forma controlada.

**Cortafuegos Personales.** Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

## VENTAJAS DE UN CORTAFUEGO

- **Protege de intrusiones.** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- **Protección de información privada.** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- **Optimización de acceso.-** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

## LIMITACIONES DE UN CORTAFUEGO

- Un cortafuego no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- El cortafuegos no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes.
- El cortafuego no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.
- El cortafuego no puede proteger contra los ataques de Ingeniería social.
- El cortafuego no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

## POLÍTICAS DEL CORTAFUEGO

Hay dos políticas básicas en la configuración de un cortafuego y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva.** Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- **Política permisiva.** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

## CENTRAL TELEFÓNICA

La central telefónica es el punto donde se reúnen las conexiones de todos los aparatos telefónicos de una determinada área, que se denomina “área local” o “área central”; en este punto central se conectan todas las extensiones disponibles, líneas las cuales se configuran para que sean líneas de salida y otras de entrada, impresoras, computadores, alimentación alternativa tales como baterías, etc.

Para escoger una central telefónica se debe tener en cuenta las necesidades del usuario de acuerdo a esto se compara con las funciones de las diferentes centrales y así se puede escoger la misma, otro punto importante para escoger la central telefónica son las funciones que desempeñará, a continuación se detallan diferentes funciones de centrales telefónicas existentes en el mercado y de acuerdo a las mismas se escoge la central telefónica a implementar en la red de voz:

· Acceso a Funciones Externas.
· Bloqueo Interno.
· Búsqueda Interna.
· Capacidad de Mensajes de Ausencia.
· Captura de Llamada.
· Conexión de Teléfono en Paralelo.
· Conferencia (3 personas/5 personas).
· Consola DSS (Selección Directa Interna).
· Contraseña de Extensiones / Contraseña del Sistema.
· Conversión de Pulso a Tono.
· Desvío de llamada.
    - Todas ocupadas/Sin respuesta.
    - Sígueme.
    - Hacia fuera.
· Detección de Señal de Control de Llamada.
· DISA (Acceso Directo al Anexo) sin mensaje.
· DISA (Acceso Directo al Anexo) con mensaje.
· Discado de un toque.
· Discado Rápido.
    - Mediante el Sistema.

- Interno.

· Duración de llamadas limitada (1-32 minutos).

· Grupo de Extensiones.

· Integración con el Correo de Voz (DTMF).

· Interfase de Respaldo de Batería (Incorporado).

· Introducción de Código de Cuenta (Opcional/Forzado/Verificado).

· Línea de Entrada Directa.

· Línea de Entrada / Línea de Salida.

· Llamada de Emergencia.

· Llamada al Operador.

· Llamada de Regreso cuando esta Ocupado (Camp-on).

· Llamada en Espera.

· Mensaje de Bienvenida (OGM).

· Música para la Retención de Llamada (BGM).

· Rediscado.

- Automática.
- Último Número.
- Número Memorizado.

· Restricción de Llamada.

· Retención de Llamada.

· Seguridad en Línea de Datos.

· Selección de Patrón de Timbrado.

· Señalización de Extensión Ocupada (BSS).

· Servicios de Horario (Diurno/Nocturno/Almuerzo).

- Automático.
- Manual.

· Tono Distintivo de Llamada.

· Transferencia Automática de Fax.

· Transferencias de Llamadas (hacia extensiones o líneas externas).

- Transferencia hacia una Extensión.
- Transferencia hacia una línea CO.

· Transferencia en caso de falla eléctrica.

En el ámbito de las redes, las centrales telefónicas son útiles para el desarrollo e implementación de una red telefónica interna, la cual necesita de: el uso de extensiones para todos los usuarios quienes podrán comunicarse con el exterior mediante una tecla de salida o con usuarios de la misma red interna marcando la extensión correspondiente, líneas de salida a las cuales tendrán acceso todos los usuarios que deseen comunicarse con el exterior, líneas de entrada las cuales tomará todas las llamadas la central telefónica anunciando un mensaje previo explicando la extensión a la cual desee comunicarse el usuario externo o comunicando a este usuario a la operadora en caso de que no se reciba respuesta del usuario con la extensión deseada, establecer una línea específica para el fax el cual necesita estar disponible a todo momento y finalmente una comunicación con el servidor por donde se podrá establecer una comunicación VPN mediante acceso telefónico a redes.

En el campo de las telecomunicaciones, en un sentido amplio, una central telefónica se define como el lugar (puede ser un edificio, un local o un contenedor), utilizado por una empresa operadora de telefonía, donde se albergan el equipo de conmutación y los demás equipos necesarios, para la operación de llamadas telefónicas en el sentido de hacer conexiones y retransmisiones de información de voz. En este lugar terminan las líneas de abonado, los enlaces con otras centrales o los circuitos interurbanos necesarios para la conexión con otras poblaciones.

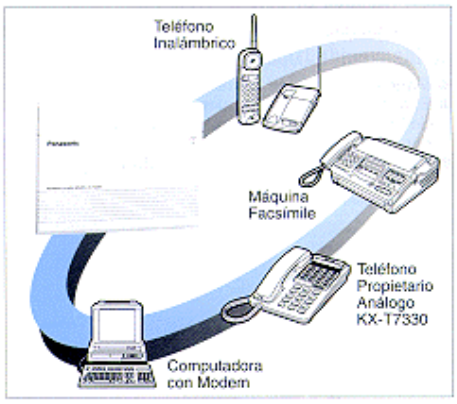



**Figura. 2.13: Conexión a Central Telefónica.**

# CAPITULO III

# INFRAESTRUCTURA ACTUAL Y REQUERIMIENTOS

## 3.1. INFRAESTRUCTURA DEL SITIO A IMPLEMENTAR LAS REDES.

Las instalaciones de la empresa INGELSI Cia. Ltda. tiene 2 plantas, donde funcionan varias dependencias de carácter administrativo y departamento de ventas. En la planta baja están localizadas las oficinas del departamento de ventas, almacén, recepción y sala de reuniones, por otro lado, en la Planta Alta de estas instalaciones están ubicados el Departamento de Contabilidad, Administración y Gerencia.

Durante el levantamiento de información se pudo constatar que en el interior de las instalaciones de esta empresa no existe ningún punto de Red igualmente se realizó un previo reconocimiento sobre las líneas telefónicas en la que solo existía un punto de acceso para toda la empresa, por ende es imperativo crear toda la red interna de voz y datos empezando en cero, añadiendo además las redes externas las cuales serán muy útiles para el desarrollo de la empresa, las configuraciones del servidor y de la central telefónica.

Para que toda la empresa pueda compartir su información este diseño debe abarcar cada rincón de la misma donde existan oficinas y puntos de acceso, a continuación se detalla las áreas que involucrarán el diseño:

Planta Baja:

- Cubículos (Ventas, Administración, Contabilidad, Ventas1).
- Almacén.
- Recepción.
- Sala de Reuniones.
- Cuarto de Servidores.

Planta Alta:

- Presidencia.
- Soporte.

- Gerencia.

La infraestructura de la empresa INGELSI Cia. Ltda. anteriormente descrita se la puede visualizar en los Anexos al final de este proyecto (Anexo 1 y Anexo 2).

La empresa INGELSI Cia. Ltda. posee actualmente los siguientes equipos y software para la implementación de este proyecto:

- 1 Servidor Compaq ML330 con Licencia Windows Server 2003 R2, Isa Server 2006 y Exchange Server 2003.
- 7 Computadores de Escritorio tipo clones 800Mhz, 1GB RAM, 80GB con licencias de Windows XP Pro. y Microsoft Office 2007.
- 2 Computadores Portables Toshiba Tecra A3 con licencias de Windows XP Pro. y Microsoft Office 2007.
- 1 Computador Portable Toshiba Satellite con licencia de Windows XP Pro. y Microsoft Office 2007.
- 2 Switch de 24 Puertos marca D-Link.
- 1 Central Telefónica Panasonic KX-TA308.

Con la realización de este proyecto, se pretende aportar soluciones a las carencias de infraestructura de redes que existe en las instalaciones de la empresa INGELSI Cia. Ltda.

## 3.2. FACTIBILIDAD

El estudio de factibilidad requerido para efectos del diseño de red, se basa en 3 aspectos o niveles: técnico, económico y operativo. A continuación, se evaluará cada una de estas factibilidades por separado:

**Factibilidad Técnica.** El proyecto es, desde el punto de vista técnico realizable, ya que están a la disposición en el mercado los diferentes equipos y dispositivos de comunicación que darán soporte a la implementación del diseño de la red. Además se cuenta con el personal capacitado para manejar los equipos que requerirá la red; este personal se ubica, específicamente en el área de Tecnologías de la Información (I.T.). El hecho de contar con este personal implica que no se hará necesario la contratación de personal externo, lo que evitaría un gasto adicional.

**Factibilidad Económica.** El costo que genera el diseño de red que se propone es bajo, ya que la tecnología que emplea el estándar de red que se utilizará será Fast Ethernet, se considera, al ser comparada con otras tecnologías, económica. En función de ello, y de los beneficios que aportaría esta red a la empresa (costo- beneficio), se considera que el proyecto es, económicamente factible.

**Factibilidad Operacional.** El levantamiento de información realizado determinó que, en las instalaciones de la empresa, una red de comunicaciones solucionaría múltiples inconvenientes que en la actualidad se presentan con el manejo de la información de las dependencias que allí funcionan como por ejemplo limitaciones en las comunicaciones, por lo que se garantiza que el personal que labora en éstas, está de acuerdo con el diseño de la Red y harán uso permanente de esta una vez que sea implementada.

## 3.3. CARACTERÍSTICAS DE LAS NECESIDADES.

Las necesidades de esta empresa son varias y muy importantes debido a esto se tiene que realizarlas bien y sin perder mucho tiempo para que los usuarios puedan trabajar lo más pronto posible ya que de esta manera la economía de la empresa no se verá afectada por la falta de trabajo.

Las necesidades de la empresa fueron proporcionadas por los usuarios y administradores de la empresa, posteriormente analizadas para verificar su factibilidad, a continuación se detallan las necesidades más importantes y servicios a implementar:

- Implementación de una red LAN, de esta manera los usuarios pueden comunicarse con el servidor, obtener Internet y comunicación con el resto de máquinas a quienes compartir información.

- Red de voz para que exista comunicación con la central telefónica interna, con sus respectivas extensiones y comunicación externa desde cualquier lugar de trabajo.

- Implementación de una red wireless la cual servirá para la comunicación con usuarios móviles y ofrecer comunicación en cualquier lugar de la empresa.

- Implementación de una red VPN para la comunicación con usuarios externos con quienes compartir información mediante http y modem.

- Configurar el servidor de la empresa para que funcione correctamente dentro del dominio y centralizar toda la información posible.

- Clasificar a los usuarios de la empresa y restringirlos a ciertos recursos de la red y de las máquinas.

- Configurar el firewall para crear las redes, seguridades a las redes expuestas y permitir acceso a los servicios de la red.

### 3.4. RAZONES PARA IMPLEMENTAR ESTAS REDES.

El motivo fundamental que lleva a realizar este proyecto, radica en no contar con el acceso a los recursos mediante redes de comunicación en ninguna punto, lo que dificulta ostensiblemente al personal administrativo y ventas compartir y aprovechar los recursos informativos que podrían proveerle la implementación de estas redes, limitando de esta manera los ingresos de la empresa, así como la comunicación directa de éstas con el exterior, lo antes mencionado representará un aporte fundamental al desarrollo de la empresa y a un reconocimiento en el mercado.

Las conexiones por red permiten a los empleados de una empresa colaborar entre sí y con empleados de otros lugares u otras empresas; posibilitan el contacto de nuevas maneras, a la vez que lo estrechan al usuario y a la empresa más de lo que jamás habría cabido imaginar, entre personas de la oficina o de cualquier punto del globo. Si la empresa está conectada por una red, nadie está lejos de nadie.

La empresa INGELSI Cia. Ltda. ha decidido implementar las redes de su empresa robustas y con todos los dispositivos necesarios para que estas redes tengan mínimos fallos y que tengan una vida útil larga. Con la infraestructura correcta se puede lograr redes con estas características y así obtener mínimos costos en mantenimiento y operación de las mismas.

Ya que la red también se utiliza para voz, es necesario configurar una central telefónica interna existente en la empresa y adecuarla, para que los usuarios puedan comunicarse hacia la empresa o dentro de la misma con la mayor facilidad.

Otro punto, es la importancia de que cualquier usuario con permisos pueda comunicarse con la red local y acceder o sincronizarse con sus datos personales o de la empresa para que estos puedan trabajar fuera de la oficina, tener toda información actualizada deseada y

así aprovechar el tiempo al máximo cuando se requiera una información imperativa a tiempo, esto se lo puede realizar mediante una Red Privada Virtual la cual es un objetivo alcanzar sin importar costes.

Además para usuarios que no dispongan de una conexión a Internet por cualquier motivo, se proporcionará un acceso a la empresa y a los servicios de la misma mediante una conexión mediante línea telefónica, con este método cualquier usuario autentificado podrá acceder a la información.

Los recursos de la red pueden estar en peligro de algún intruso, debido a esto se necesita configurar un firewall ya sea en hardware o en software para que este sea el muro que proteja a las redes y restringir ciertos recursos de las mismas a los usuarios que podrían poner en peligro el desempeño de estas y el abuso de la información.

Una vez realizadas estas implementaciones los empleados podrán trabajar sin problema alguno y poder culminar sus deberes en la empresa a tiempo. Por otra parte el Departamento de Tecnología de la Información (IT) tendrá una garantía y confianza en la red desarrollada; se tendrá una mayor organización en el cableado y por ende poder realizar un mantenimiento y control más eficiente.

En resumen, la empresa podrá tener la seguridad de que no existan intrusos que roben la información vital, el gerente o cualquier administrador podrá comunicarse con la red para sincronizar información y poder manejar la empresa desde fuera de la oficina aún si este no tiene acceso a Internet, por último, los clientes que se comuniquen a la empresa lo puedan hacer y comunicarse con la persona deseada con más facilidad y rapidez mediante la configuración de la central telefónica; con todo los descrito anteriormente la empresa tendrá la garantía de que su información se encuentra segura y su desempeño será el máximo.

## 3.5. SEGURIDADES EXISTENTES PARA LAS REDES A IMPLEMENTAR.

Por seguridad se puede entender como el comportamiento deseado por administradores, programadores y usuarios del sistema para así utilizar todos los recursos disponibles sin verse estos afectados ni en riesgo debido a intrusos o software malintencionados tanto para una red como para una máquina ya que cualquier camino expuesto puede afectar a toda la infraestructura.

El activo más importante en las organizaciones publicas, privadas y de cualquier índole, es la información que tienen. Entre más grande es la organización mas grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia el asegurar la seguridad de la información.

La seguridad no es solamente el implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información.

Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

Dentro de las redes inalámbricas el sentido de seguridad es más sentido debido a la naturaleza de las mismas. En sus inicios la seguridad en este tipo de redes era muy deficiente y algunas personas daban la tarea de encontrar redes inalámbricas para acceder a ellas desde las calles.

Para una red segura es necesario considerar los siguientes aspectos:

- Accesos no autorizados.
- Daño intencionado y no intencionado.
- Uso indebido de información (robo de información).

Posteriormente se definen las políticas referentes a los usuarios y contraseñas, los métodos de acceso a los servidores y a los sistemas. Se definen la complejidad que debe reunir las contraseñas y su validación dentro de la red, el tiempo de trabajo de las estaciones de trabajo, áreas de acceso por cada usuario, etc.

La seguridad basada en autentificación de usuario es la más usada, permite administrar y asignar derechos a los usuarios de la red. Permitiendo o denegando los accesos a los recursos a través de una base de datos en el servidor.

El trabajo del administrador deberá incluir la administración de usuarios. Otra manera de administrar usuarios es mediante el uso de grupos de usuarios, el cual nos da la facilidad de aplicar las políticas de seguridad a grupos específicos los cuales heredaran estas a los miembros de dicho grupo.

Debido a esto se implementará una nueva Unidad Organizativa (UO) en Active Directory de Windows Server 2003 el cual contendrá otras UO las cuales contendrán a su vez a los usuarios quienes serán divididos por categorías o grupos de usuraos tales como Administradores, Usuarios Avanzados, Usuarios y Usuarios Restringidos. Todas las unidades organizativas tendrán directivas de grupo para que cumplan con las siguientes accesos y restricciones:

Administradores……Tendrán acceso a todos los recursos de la red.
Fondo de pantalla con logotipo de la empresa.
Permiso para cambiar el fondo de pantalla.

Usuarios Avanzados……..No podrán eliminar impresoras agregadas.
No podrán instalar ni desinstalar ningún programa.
Fondo de pantalla con logotipo de la empresa.

Usuarios…….No podrán instalar ni desinstalar ningún programa.
No podrán modificar ni ingresar al panel de control.
No podrán eliminar impresoras agregadas.
Fondo de pantalla con logotipo de la empresa.

Usuarios Restringidos……No podrán instalar ni desinstalar ningún programa.
No podrán modificar ni ingresar a panel de control.
No podrán eliminar impresoras agregadas.
Fondo de pantalla con logotipo de la empresa.
Restricciones para el uso del Messenger de Windows.

Se debe tomar en cuenta el uso de cortafuegos que permita administrar el acceso de usuarios de otras redes así como el monitorear las actividades de los usuarios de la red, permitiendo tener una bitácora de sucesos de red.

Las bitácoras son de gran utilidad para aplicar auditorias a la red. La revisión de los registros de eventos dentro de la red permite ver las actividades de los usuarios dentro de la red, esto permite al administrador darse cuenta de los accesos no autorizados por parte de los usuarios y tomar las medidas que faciliten incrementar la seguridad. La auditoria permite monitorear algunas de las siguientes actividades o funciones

- Intentos de acceso.
- Conexiones y desconexiones de los recursos designados.
- Terminación de la conexión.
- Desactivación de cuentas.
- Apertura y cierre de archivos.
- Modificaciones realizadas en los archivos.
- Creación o borrado de directorios.
- Modificación de directorios.
- Eventos y modificaciones del servidor.
- Modificaciones de las contraseñas.
- Modificaciones de los parámetros de entrada.

Se puede implementar algoritmos de encriptación de datos para la información relevante. Hay algunos organismos que certifican este tipo de software y garantizan la confidencialidad de los datos a través de la red, en especial en Internet, donde la seguridad de nuestra información es delicada.

El funcionamiento de estos sistemas de encriptación funcionan de la siguiente manera: el emisor aplica el algoritmo de encriptación a los datos, estos viajaran a través de la red de tal forma que si algún intruso quiera verla no le será posible. Al llegar al destino se aplicara un algoritmo inverso que permita traducir los datos a su forma original.

Debido a que la información que se maneja en las redes y empresas es confidencial, se deberá implementar para este proyecto certificados los cuales ayudarán en la encriptación de los datos, en los cuales viajan información sobre estados de cuenta, números de cédula, números de tarjetas de crédito, etc.

El servidor creará su propio Certificado Digital para la implementación de las redes bajo HTTPS lo que garantiza que toda la información viaje encriptada y sin peligro.

También existen medidas de identificación biométrica como lectores de huella digital, escaneo de palma de mano, entre otros, esta tecnología es más segura que la simple identificación de nombre de usuario y contraseña ya que el usuario no tendrá que recordar contraseñas que en algunos casos son complejas y difíciles de recordar además que a diferencia de las contraseñas la huella digital no se puede transferir a otros usuarios y no

puede ser robada, los cuales no se van a implementar en este caso debido a costos muy elevados.

**La Seguridad en Redes Inalámbricas (WLAN).** Por la misma naturaleza de las redes inalámbricas que utilizan como medio físico de transmisión el aire el factor de seguridad es critico.

La seguridad de este tipo de redes se ha basado en la implantación de la autenticación del punto de acceso y los clientes con tarjetas inalámbricas permitiendo o denegando los accesos a los recursos de la red.

**Mecanismos de Seguridad para Redes WLAN.** La especificación del estándar 802.11 originalmente utiliza tres métodos para la protección de la red.

SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Cada uno de los clientes debe tener configurado el SSID correcto para acceder a la red inalámbrica.

Filtrado de direcciones MAC. Se definen tablas que contienen las direcciones MAC de los clientes que accederán a la red.

WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11.

El IEEE creo el estándar 802.X diseñado para dar controlar los accesos a los dispositivos inalámbricos clientes, Access Point y servidores. Este método emplea llaves dinámicas y requiere de autentificación por ambas partes. Requiere de un servidor que administre los servicios de autentificación de usuarios entrantes.

WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y

minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP (ver arriba). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

La tecnología SecureEasySetup™ (SES) de Linksys o AirStation OneTouch Secure System™ (AOSS) de Buffalo permite al usuario configurar una red y activar la seguridad de Acceso protegido Wi-Fi (WPA) simplemente pulsando un botón. Una vez activado, SES o AOSS crea una conexión segura entre sus dispositivos inalámbricos, configura automáticamente su red con un Identificador de red inalámbrica (SSID) personalizado y habilita los ajustes de cifrado de la clave dinámico de WPA. No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña ni clave asociada con una configuración de seguridad tradicional inalámbrica.

## OTRAS AMENAZAS

**Virus Informáticos.** Los virus informáticos son pequeños programas de computadora que al igual que un virus biológico, infecta equipos de computo y se propaga a través de la red o utilizando otros medios de transmisión como memorias, disquetes, discos ópticos, etc.

El crecimiento de las redes y en especial de la Internet ha facilitado la propagación de virus de forma acelerada. Un método de propagación de virus común es el uso de correo electrónico. Al abrir un correo infectado por virus puede infectar el equipo y puede ser capaza de reenviarse a otros usuarios de correo utilizando la libreta de direcciones del usuario. Tener en consideración de que cualquier medio de intercambio de datos puede ser un medio potencial de propagación de virus.

Los medios más comunes pueden ser:

- Disquetes, DVD, Conexiones LAN, Via MODEM, CD, Unidades portables (memorias Flash), cintas magnéticas, conexiones a Internet.

Un virus puede causar muchos daños como perdida de datos, evitar que el equipo arranque normalmente (daños en el sector de arranque), formateo de las unidades lógicas. Un síntoma de infección dentro de la red es que el desempeño de esta baja considerablemente a causa de trafico excesivo provocado por virus.

**Prevención.** Se debe tener políticas de prevención contra estas amenazas que ponen en riesgo la integridad de la red. Esto se puede evitando abrir correos sospechosos, entrar en páginas de Internet con contenidos pornográficos, de juegos y paginas sospechosas.

**Instalar programas antivirus**. Actualmente hay una gran variedad de proveedores de estos servicios, hay que elegir el que más se adapte a nuestras necesidades. Algunos cuentan con detectores de spyware, robots, antispam, entre tras amenazas potenciales.

En este proyecto se va a contar con Symantec Corporate Edition 10.1, es un antivirus fuerte para redes ya que desde el servidor se puede controlar actualizaciones, infecciones, instalaciones remotas, etc. de todos los usuarios de la red. Por otro lado para evitar el spam se configurará el filtro inteligente que trae Exchange Server 2003 en su service pack 1 y finalmente contra el spyware se usará Windows Defender de Microsoft.

## 3.6. DESCRIPCIÓN DE LA CENTRAL TELEFÓNICA A CONFIGURAR.

Los teléfonos son unas de las principales fuentes de comunicación ya que con ellos se puede tener contacto con distribuidores, clientes, amigos, miembros de la oficina y sobre todo familiares. El sistema Híbrido Avanzado KX-TA616 es un sistema telefónico que puede manejar negocios y necesidades personales, se la utiliza en este proyecto ya que es un equipo que pertenece a la empresa desde hace un período de tiempo, la cual necesita ser adaptada a las necesidades de los usuarios.

**Figura. 3.1. Central Telefónica.**

La KX-TA616 acepta 6 líneas CO y 16 extensiones análogas. Con Tarjetas opcionales, se podrá fácilmente incrementar la capacidad del sistema hasta 6 líneas CO y 24 extensiones dependiendo como las necesidades aumenten. Este sistema provee las funciones que satisfacen la demanda de los usuarios más sofisticados y conscientes de los costos. Se podrá conectar con una variedad de equipos de comunicación tales como teléfonos inalámbricos, maquinas contestadoras, módems verificadores de tarjetas de crédito, máquinas de fax y cualquier otro equipo que trabaje con líneas de teléfonos convencionales.

La central Panasonic KX-TA616 es ideal para negocios pequeños u oficinas en casa que requieren de un sistema flexible con un alto grado de sofisticación.

Las características más sobresalientes de este sistema son las siguientes:

1. Expansión Simple y Flexible.
2. Sistema Híbrido.
3. Administración Inteligente de Llamadas (DISA, UCD) Identificador de Llamadas y Desvío de Llamadas.

4. Administración Eficiente de Costos Económicos (Registro Detallado de Llamadas en el Sistema, Código de Entrada, Restricción de Costos de Llamadas).
5. Fácil Mantenimiento (Interfase de Respaldo de Batería Incorporado).

A continuación se detallará las diferentes ventajas de esta central telefónica:

Las centrales telefónicas híbridas permiten integrarse a una amplia gama de equipos de comunicación y teléfonos propietarios.

Cada puerto de extensión “Híbrido” permite acomodar teléfonos propietarios análogos así como cualquier dispositivo de línea sencilla (tales como el sistema Telefónico Integrado (ITS), máquinas de fax, maquinas contestadoras, teléfonos inalámbricos, módems de computadoras, etc.). Tarjetas o cables adicionales no son requeridos.

El manejo eficiente de llamadas permite que las personas que llaman desde afuera accedan cualquier extensión sin pasar a través de un operador. Las personas que llaman desde afuera pueden marcar el destino deseado como por ejemplo una extensión o un grupo deseado, o también líneas externas. Si una tarjeta opcional de mensaje de bienvenida es instalada, la persona que llama escuchará un mensaje de saludo. Dos mensajes diferentes de DISA (saludo) pueden ser grabados por el operador o el administrador. Un mensaje puede ser usado en el modo diurno y otro en el modo nocturno, o ambos pueden ser usados por diferentes líneas CO.

Cuando el sistema recibe una señal de transmisión de fax a través de DISA este automáticamente lo conecta a la extensión prefijada de fax. Las llamadas de fax pueden ser recibidas de día o de noche sin un operador y con esto no es necesaria una línea de teléfono dedicada al fax.

Identificador de llamadas que le permite al usuario ver la información de la persona que llama en un Teléfono Propietario análogo (APTS). El exhibidor de teléfonos propietarios puede ser utilizado para acceder a la bitácora de las identificaciones de llamadas para las 5 llamadas más recientes (Bitácora de Llamadas).

Las llamadas entrantes que hayan sido registradas en la bitácora, pueden ser contestadas fácilmente.

Adicionalmente con este sistema se podrá abrir puertas y tener audio de porteros, esto se usa si un visitante presiona el botón del portero, el usuario de la extensión pre-asignada podrá responder la llamada y hablar con el visitante. Cualquier extensión puede llamar al Audio portero. Los Audio porteros son usados también como monitores de habitación. Un portero eléctrico opcional/ y la tarjeta para abrir puertas deben ser instalados al sistema.

La Puerta de Tarifación (SMDR) automáticamente imprime la información detallada de llamada para las llamadas externas. Una impresora conectada al puerto de Interfase Serial (RS-232C) puede ser usada para imprimir llamadas internas y externas, así como también imprimir una copia de la programación del sistema.

Puede imprimir la siguiente información:

1. Fecha - Llamada saliente.
2. Hora - Llamada recibida.
3. Numero de la Extensión - Llamada en Espera.
4. Numero de teléfono de la oficina publica - (Distribución Uniforme de Llamadas UCD).
5. Numero marcado/recibido.
6. Duración.
7. Código de cuenta.

La información del Registro Detallado de llamadas en el sistema (SMDR) ayuda a controlar los costos de las llamadas de larga distancia, la productividad del personal y el uso del sistema del teléfono.

Códigos de cuenta: pueden ser utilizados para identificar llamadas externas para fines contables y de facturación. Si una persona marca un número de larga distancia debe introducir un código de cuenta valido para rechazar temporalmente la restricción de cargos (Introducción de código de cuenta verificada). Las actividades de llamadas hechas con un código de identificación pueden ser impresas (SMDR). Los códigos de cuenta y SMDR para manejar sus costos de teléfono de manera más efectiva.

**Alarma Recordatoria.** Esta característica le permite al usuario generar una alarma la cual funcionará como alarma-despertador o alarma-recordatoria. El usuario puede configurar esta función para ser activada solo un día o todos los días.

**Asignación de Líneas de Preferencia.** Líneas de Entrada, el usuario de un teléfono propietario puede seleccionar el método para responder llamadas entrantes desde el exterior utilizando alguna de las siguientes opciones:

1. Línea sin preferencia o indicación: cuando una llamada entrante es recibida, el usuario de la extensión debe cerrar su teléfono utilizando la horquilla y después presionar la tecla de “Flashing” CO.

2. Línea de primera preferencia: Cuando se reciben varias llamadas al mismo tiempo, el usuario puede recibir dicha llamada en el modo registrado como preferencia externa (CO) mediante el cierre de la horquilla en el teléfono.

3. Timbrado de las líneas de preferencia: Al recibir una llamada entrante, el usuario puede recibir dicha llamada con solo cerrar su teléfono y dejar que este timbre en su extensión.

**Conferencia, desatendida (3 personas).** Cuando el usuario de un teléfono se encuentra en conferencia de 3 personas con 2 personas externas, el usuario puede abandonar la conferencia para permitirles a las otras 2 personas continuar la conversación. El usuario puede regresar a la conferencia si así lo desea.

**Consola de selección de estación directa (DSS).** La consola de selección directa (DSS) provee acceso directo a las extensiones, una luz que indica que la línea esta ocupada, así como también los botones de 16 características programables (16 PF). La consola DSS debe ser programada para trabajar con teléfono propietario (PT). Hasta 2 consolas por sistema pueden ser instaladas.

**Respuesta de llamadas.**

- Respuesta directa de llamadas: Le permite al usuario de una extensión responder una llamada en una extensión diferente a la suya.
- Respuesta a un Grupo de llamadas: Le permite al usuario de la extensión responder una llamada de otra extensión, si las llamadas suenan dentro del grupo de extensiones del usuario.

- Respuesta de llamada Negada: le permite al usuario de la extensión impedir que otras extensiones respondan una llamada en la extensión del usuario mediante la característica de respuesta de llamadas.
- Rehabilitar una llamada desde la maquina contestadora de llamadas (telephone Answering Machine): Permite al usuario de la extensión contestar una llamada interna recibida por la extensión de TAM.

**Duración limite de llamada.** El sistema desconecta 2 tipos de llamadas externas cuando el tiempo preprogramado expira. La primera, es una llamada de una persona externa. La otra es una llamada externa hacia fuera (Coa CO) utilizando Desvío de llamadas hacia línea (CO) externa, Transferencia de llamada hacia línea (CO) externa, característica DISA. Un tono de alarma a ambos usuarios 15 minutos antes la señal asignada del tiempo limite. Limitar el tiempo de la llamada puede ser asignada a través de un sistema de programación (1 –32 minutos).

**Llamada de emergencia.** Le permite al usuario de la extensión acceder a un número presagiando de emergencia el cual puede ser marcado sin ninguna restricción. Pueden almacenarse 5 números de emergencia.

**Llamada en espera.** Durante una conversación, el tono de llamada en espera informa al usuario de la extensión que hay una llamada en espera. El usuario puede responder la segunda llamada desconectando la primera o poniéndola en espera.

**Mensaje en espera.** Le permite al usuario de la extensión notificar a la extensión llamada de un mensaje en espera cuando esta ocupada o no contesta la llamada. Solo los usuarios de teléfonos propietarios con botón de mensaje pueden saber que hay un mensaje en espera si la lámpara de mensaje se pone roja. Presionando el botón de mensaje encendido puede volver a llamar a la persona llamada. Los mensajes que han sido almacenados en el correo del sistema de procesamiento de Voz pueden ser escuchados por los mensajes hablados en el correo de Voz después de presionar el botón Mensaje encendido (integración de correo de voz). El sistema soporta un máximo de 8 mensajes simultáneos.

**Transferencia de llamadas – hacia extensión.** Le permite al usuario de la extensión transferir una llamada recibida, una llamada interna o externa hacia otra extensión.

Dos tipos están disponibles:

- Transferencia de llamada por Pantalla: Anuncia la llamada de la otra extensión antes de completar la conferencia.
- Transferencia de llamada sin pantalla: Inmediatamente transfiera a la persona que llama sin anunciar.

## Diagrama de Conexión.

### KX – TA616

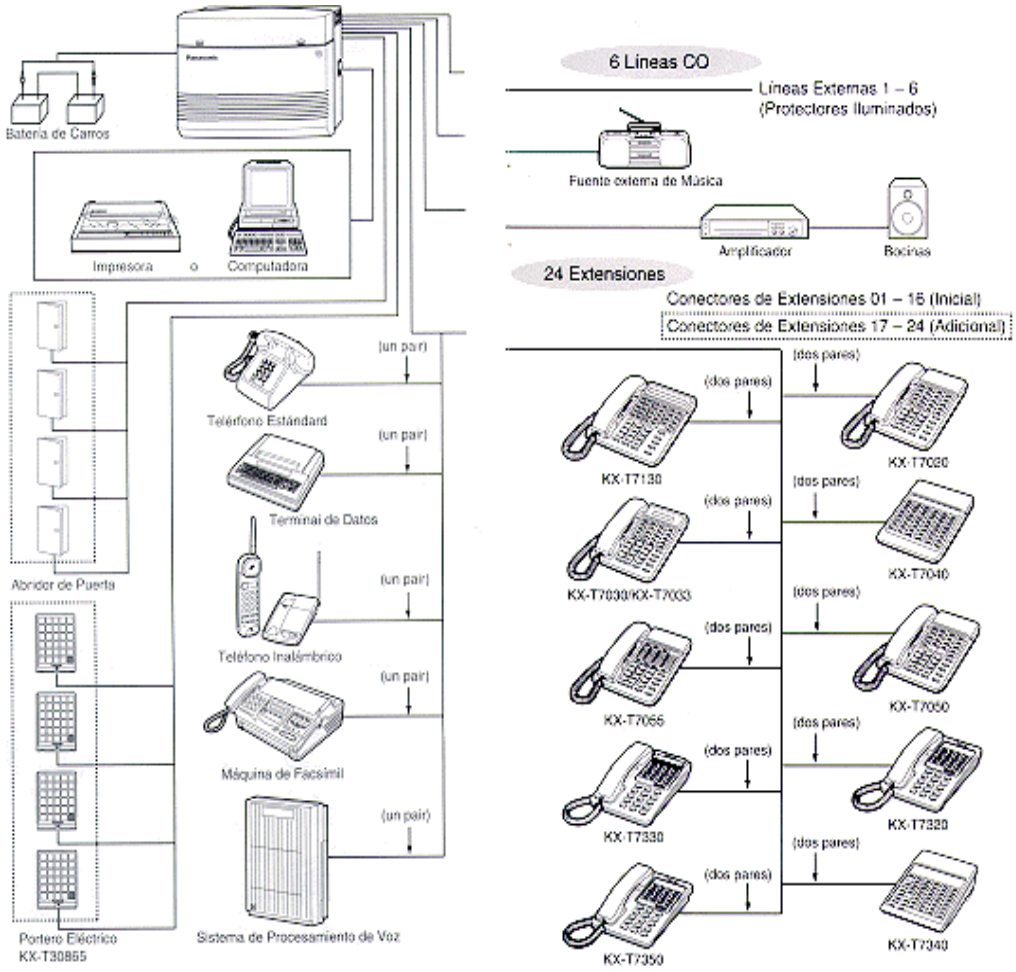



**Figura. 3.2. Conexión de Central Telefónica.**

# CAPÍTULO IV

# DISEÑO DE LAS REDES

## 4.1. ÁREA DE COBERTURA.

El área de cobertura es la región o campo en la que los usuarios fijos o móviles tendrán acceso a los recursos de la red.

Para el diseño de una red es importante tener en cuenta aspectos como el área de cobertura de esta manera se dimensionará los elementos a utilizar en la implementación de esta red.

Analizando previamente la ubicación de los diferentes departamentos los cuales necesitarán el acceso a los recursos de la red y los requerimientos manifestados por el gerente de la empresa se concluyó en los siguientes puntos:

- La red que incluye voz y datos deberá cubrir las dos plantas de la infraestructura perteneciente a la empresa INGELSI Cia. Ltda., los puestos de trabajo que contarán con el acceso a los recursos de la red serán los siguientes:

  Planta Baja:

  a. Servidor
  b. Recepción.
  c. Fax.
  d. Almacén
  e. Ventas.
  f. Contabilidad.
  g. Ventas1.
  h. Sala de Reuniones.
  i. Contabilidad.

  Planta Alta:

  j. Gerencia General.

k. Presidencia.
l. Soporte.

- Los nombres de las oficinas, son los definidos por la Empresa y deberá tener especial cuidado en la cobertura de la primera planta ya que es donde se encuentra la sala de reuniones y es donde más cantidad de usuarios móviles se encontrarán y la segunda planta se cubrirá parcialmente como prioridad secundaria.

## 4.2. SISTEMA DEL CABLEADO ESTRUCTURADO

Por definición significa que todos los servicios en el edificio para las transmisiones de voz y datos se hacen conducir a través de un sistema de cableado en común. En un sistema bien diseñado, todas las tomas de piso y los patch panel terminan en conectores del tipo RJ45 que se alambran internamente a EIA/TIA 568a o 568b.

El método más confiable es el de considerar un arreglo sencillo de cuatro pares de cables, que corren entre el dorso del “patch panel” y el conector. El único método de interconexión es entonces, muy sencillo, un patch cordon RJ45 a RJ45.

Todos los servicios se presentan como RJ45 vía patch panel de sistema y la extensión telefónica y los puertos del conmutador se implementan con cables multilínea hacia el sistema telefónico y otros servicios entrantes. Adicionalmente se pueden integrar también servicios de fibra óptica para proporcionar soporte a varios edificios cuando se requiera una espina dorsal de alta velocidad.

Estas soluciones montadas en rack incorporan normalmente los medios para la administración de cable horizontal empleando patch cordon de colores para indicar el tipo de servicio que se conecta a cada conector. Esta práctica permite el orden y facilita las operaciones además de permitir el diagnóstico de fallas.

En los puestos de trabajo se proporcionan condiciones confiables y seguras empleando cables a la medida para optimizar los cables sueltos. La mejora en la confiabilidad es enorme. Un sistema diseñado correctamente no requiere mantenimiento.

Ventajas Principales de los cables UTP: movilidad, facilidad de crecimiento y expansión, integración a altas velocidades de transmisión de data compatibles con todas las Lan que

soporten velocidades superiores a 100 mbps, flexibilidad para el mantenimiento de las instalaciones dispositivos y accesorios para cableado estructurado.

El Cableado Estructurado permite voz-datos, dotando a locales y oficinas de la infraestructura necesaria para soportar la convivencia de redes locales, centrales telefónicas, fax, videoconferencia, intranet, Internet, etc.

Durante el levantamiento de la información se pudo constatar que en todo el edificio de esta empresa no existe conexión de Red para las dependencias que allí funcionan. Debido a esto las actividades normales de una empresa que depende bastante de la comunicación se ven notablemente limitadas debido a la imposibilidad de poder aprovechar los recursos que podrían ofrecer la implementación de las redes Lan, WLan y VPN.

En función de integrar a todos las distintas dependencias de esta empresa que carecen de conexión de redes, se plantea diseñar el sistema de cableado estructurado para el area de cobertura descrita anteriormente el cual consta de dos plantas la Planta Baja y la Planta Alta.

Para definir el sistema de cableado por el cual se regirá el proyecto, se considerarán las normas que establece el sistema de cableado estructurado, específicamente se adoptará la norma 568-A debido a que todos los puntos necesitan tener la misma norma para que exista comunicación entre ellos. Como medio físico se utilizará el cable UTP CAT5E, ya que éste permite mayor rapidez para el manejo de información y es el más utilizado y recomendado en el mercado. Este medio físico tendrá una longitud máxima de 100 mts, tal y como lo establecen las normas del Cableado Estructurado.

**DESCRIPCIÓN**

**Cableado.** El cableado está formado por los cables que se extienden a través del techo de la empresa, desde el cuarto de servidores hasta cada cuarto de equipos de la empresa. Este cableado consta de cables par trenzado UTP categoría 5 CAT5E con topología en estrella. Las canaletas son utilizadas para distribuir y soportar el cableado horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de servidores. Cada punto terminal de conexión está conectado al Patch Panel que se encuentra en el cuarto de servidores siguiendo un orden específico. El cableado horizontal del edificio cumple con la máxima distancia horizontal permitida entre el Patch Panel y el terminal de conexión; en este

proyecto la mayor distancia recorrida por el cable es de 60 metros; y con la longitud máxima del punto terminal hasta la estación de trabajo que es de 3 metros.

**Cuarto De Servidores.** Debido a que la infraestructura de la empresa es un solo edificio de dos plantas se optará por convertir el cuarto de telecomunicaciones y el de equipos en uno solo al cual llamaremos cuarto de servidores. El área donde funcionará el cuarto de servidores es estratégico debido a la facilidad con la que se llega a cada uno de los puestos de trabajo que conforma la empresa; además, en esa dependencia labora personal capacitado que solventará algún tipo de problema que pueda presentarse con éstos; se consideró también esta ubicación, debido a que en este lugar existe un punto de acceso que permite conectar nuestra red a Internet asignado por la empresa contratada, finalmente el cuarto de servidores es un sitio central desde donde se extenderá todo el cableado uniformemente. Este cuarto administrará y controlará toda la red de la empresa.

Desde el cuarto de servidores se proporcionan dos cables independientes a cada puesto de trabajo de la red: uno para uso regular y otro de respaldo o voz. Debido al número de puntos requeridos por la empresa el cuarto de servidores deberá ser provisto del siguiente material:

- Dos switch con 24 puertos de salidas UTP a 10 o 100 Mbps.
- Módem por el cual ingresa el Internet.
- Dos UPS.
- Central Telefónica.
- Un Rack de pared LAN.
- Un Patch Panel LAN-PRO de 24 puertos.
- Un Patch Panel LAN-PRO de 12 puertos.
- Una bandeja para rack.

## 4.3. ESTÁNDARES A UTILIZAR EN LAS DIFERENTES REDES

**Estándar de red LAN a utilizar.** El estándar que se utilizará en el diseño de la red será Fast Ethernet según la norma IEEE 802.3u. Esta tecnología presenta como ventajas principales el bajo costo de su implementación y la capacidad proteger las estaciones conectadas a la red del riesgo que implica la posibilidad de que un usuario desconecte intencionalmente o no, una estación o cable; debido a que el tipo de topología física que se emplea es en estrella. Adicional este estándar define el uso del cable UTP categoría 5, el

cual permite velocidades de hasta 100 Mbps, lo cual se adapta a los requerimientos de velocidad de la red; por otro lado el método de acceso al medio que específica la norma es el CSMA/CD(acceso múltiple por detección de portadora con detección de colisiones). Este método consiste en comprobar si la línea esta libre antes de comenzar la transmisión, verificando si se ha producido una colisión durante la transmisión, de haberse producido una colisión se detiene la transmisión y se vuelve a transmitir el bloque de dato después de un tiempo de espera aleatorio. Asimismo, el tipo de conector que específica este estándar es el RJ-45.

**Estándar de red WLAN a utilizar.** El estándar que se utilizará para la implementación de la red WLAN será IEEE 802.11b el cuál es un estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz con una interfase de aire DSSS y un ancho de banda de canal de 25 Mhz, además se optará por implementar el estándar IEEE 802.11g que soporta velocidades 54 Mbps en la banda de los 2.4 Ghz, utiliza codificación OFDM/DSSS con un ancho de banda de canal de 25Mhz. Para poder implementar estos dos estándares se contará con un Linksys Wireless router WRT54G el cual tiene la capacidad para que clientes tanto del estándar 802.11b, 802.11g o los dos a la vez puedan trabajara simultáneamente o por separado.

## 4.4. UBICACIÓN DE LOS PUNTOS DE ACCESO A LAS REDES

Para establecer la ubicación de los puntos de acceso de las redes se tomará como referencia el área de cobertura descrita en el tema 4.1, los puntos serán ubicados según el número de puestos de trabajo existentes y en otros casos pensando en el uso de esos puntos a futuro. Por consiguiente cada estación de trabajo necesitará de dos puntos los cuales serán repartidos como sigue: el primer punto para voz y el segundo para datos o cualquier combinación que necesite la red, en casos especiales como el servidor, recepción y fax se añadirán dos puntos adicionales para su uso a futuro y serán usados de acuerdo a las necesidades de la red, debido a que el número de puntos que se usarán en la sala de reuniones varía de acuerdo al número de personas que ingresen se añadirá un switch en cascada con el cuál se podrá hacer uso de los puntos del mismo hasta un máximo de veinte y cuatro, finalmente los puntos de la red LAN serán ubicados lo más cerca posible de los equipos para su fácil manejo.

Por lo manifestado anteriormente la red LAN de la empresa INGELSI Cia. Ltda. constará de treinta puntos los cuales serán repartidos por cada una de las estaciones de trabajo requeridas. A continuación se detalla la ubicación y el número de puntos por estación de trabajo:

| UBICACIÓN | NÚMERO DE PUNTOS |
|---|---|
| Servidor | 4 Puntos |
| Recepción | 4 Puntos |
| Fax | 4 Puntos |
| Almacén | 2 Puntos |
| Ventas (Cubículo 1) | 2 Puntos |
| Contabilidad (Cubículo 2) | 2 Puntos |
| Administración (Cubículo 3) | 2 Puntos |
| Ventas1 (Cubículo 4) | 2 Puntos |
| Sala de Reuniones | 2 Puntos |
| Gerencia | 2 Puntos |
| Presidencia | 2 Puntos |
| Soporte | 2 Puntos |

**Tabla. 4.1. Número y Ubicación de puntos en la Red LAN.**

Las redes WLAN no tienen puntos de acceso definidos, estos se los define mediante el área de cobertura por consiguiente se tratará a continuación la ubicación del concentrador principal el cual es el punto de acceso principal de la red WLAN.

Debido a la importancia de tener una red WLAN en la primera planta como prioridad principal se deberá ubicar al concentrador inalámbrico en esa planta y en un sitio central por lo que el área para encontrar el sitio del concentrador inalámbrico se reduce a una planta, a continuación mediante pruebas se encontrará el sitio ideal en esta planta para que la señal del concentrador alcance toda el área de cobertura señalada anteriormente. Por consiguiente se realizan varias pruebas, la primera de ellas será detectar la menor cantidad de señales en un sitio específico, para esto se instala un software el cual ayude a detectar otras señales en el area de cobertura, en este caso se instalará el software llamado NetStumbler, con el cual se podrá ver las señales que pueden interferir a la red WLAN a implementar y los canales de las señales existentes, en esta prueba se comprobó que el sitio

ideal se encuentra cerca del cuarto de servidores por lo que se tratará de realizar las pruebas faltantes desde esta ubicación para una mejor administración del mismo además se comprobó que el canal sin utilizar es el nueve por lo que usará este canal, a continuación se realiza un recorrido por el área de cobertura con una portátil y haciendo un ping continuo al concentrador el cuál ya está ubicado en el cuarto de servidores, la prueba da como resultado que la señal llega al area de cobertura deseada con una respuesta menor a 1ms en la planta baja y menor a 8ms en el area deseada de la planta alta, finalmente se realiza la prueba para verificar la potencia de la señal lo que dará la información sobre la velocidad de la misma, mediante la ayuda del software utilizado anteriormente se recorrerá el area de cobertura para verificar velocidad de la misma, con esto se determinó que la velocidad en la planta baja oscila de 48Mbps hasta 54Mbps y la velocidad en el area de la planta alta oscila de 32Mbps hasta los 54Mbps, por lo que se concluye que el sitio ideal para ubicar el concentrador inalámbrico es el cuarto de servidores por ser un sitio central y cumple con los requerimientos de la red WLAN como son: comunicación, poca interferencia y velocidades aceptables.

## 4.5. PLANOS DE LOS PUNTOS DE ACCESO DE LAS DIFERENTES REDES

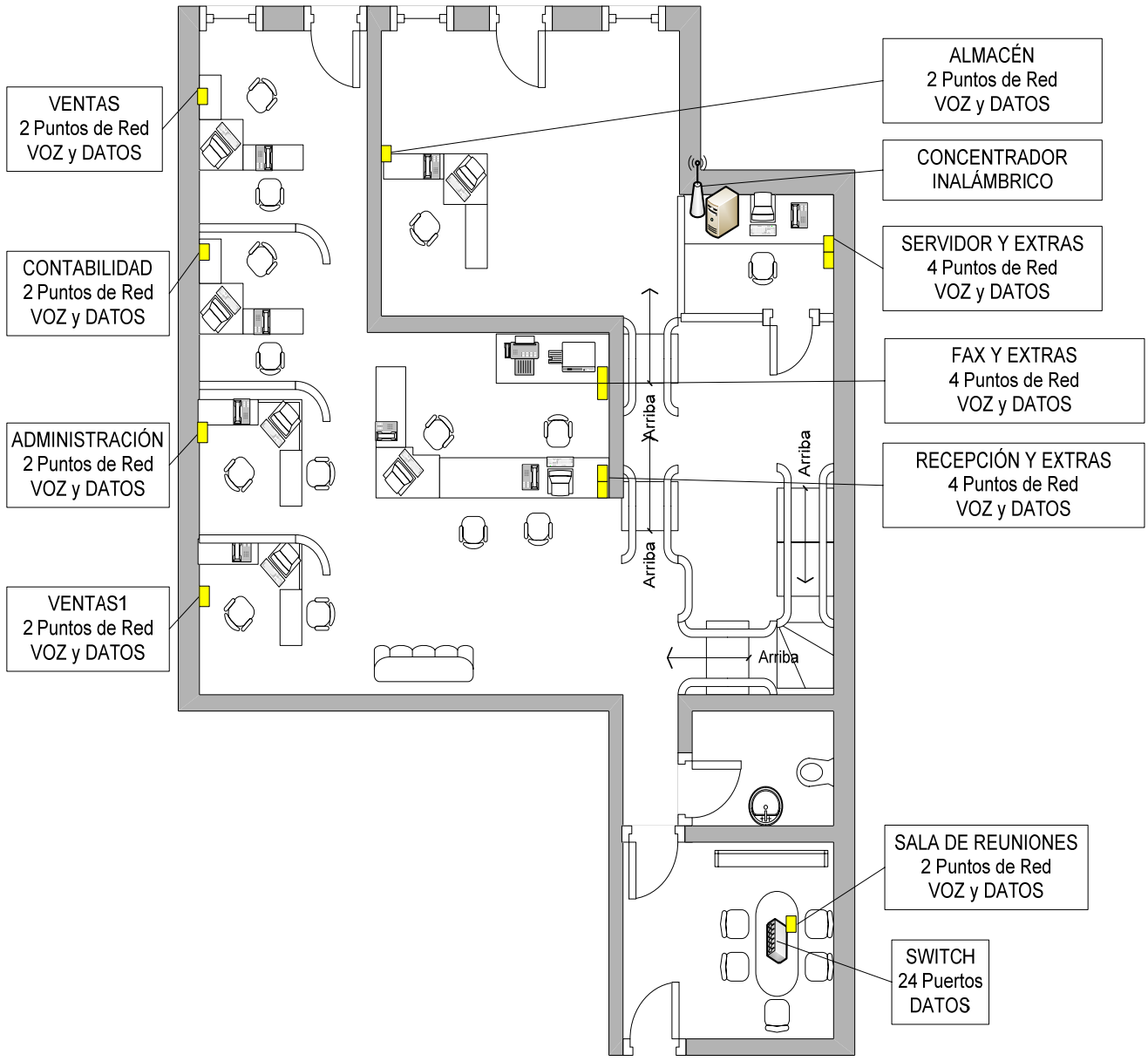



**Figura. 4.1. Plano Puntos de Acceso Planta Baja.**

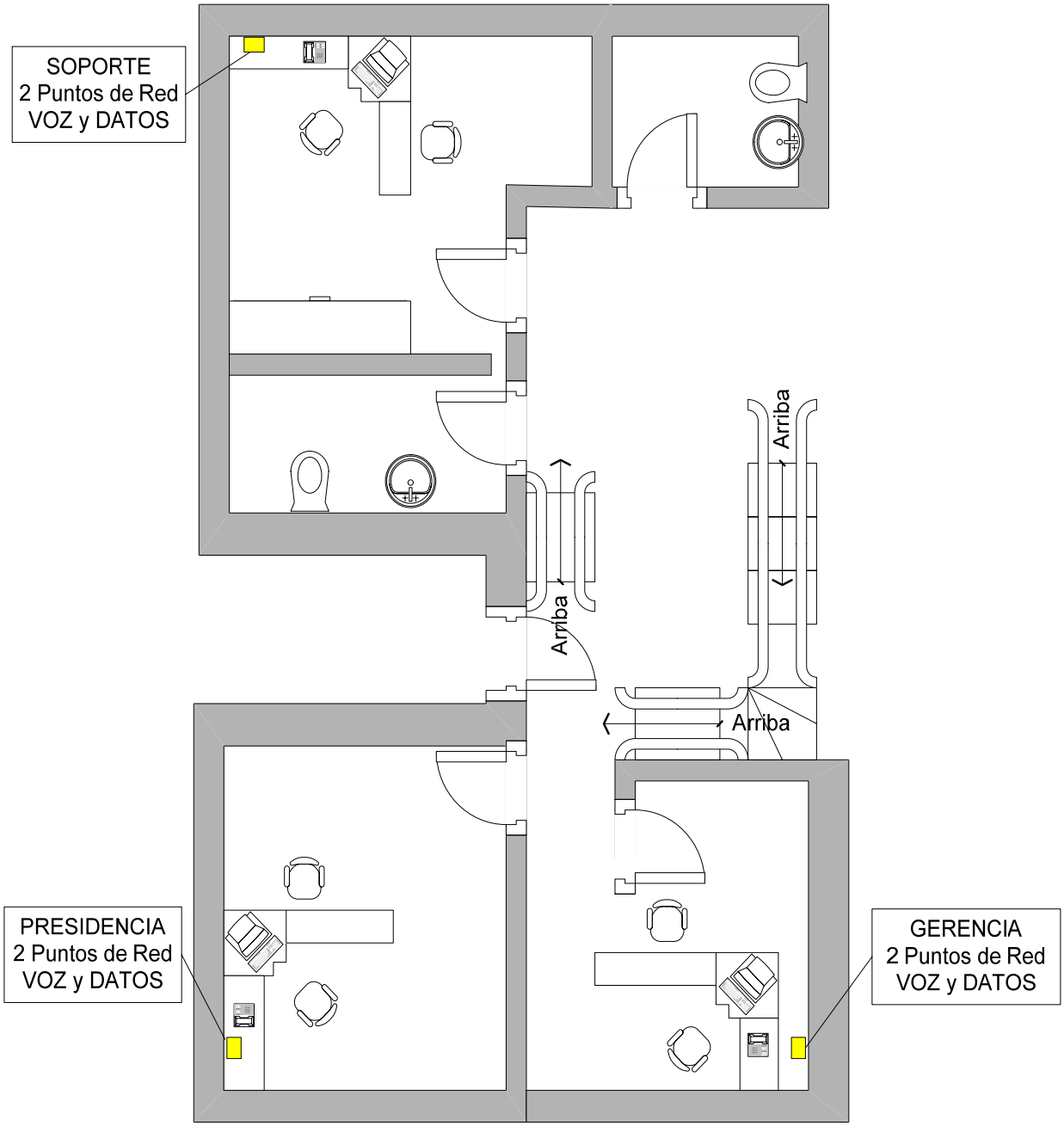



**Figura. 4.2. Plano Puntos de Acceso Planta Alta.**

## 4.6. PROTOCOLOS DE COMUNICACIÓN

Los protocolos definen las normas que posibilitan que se establezca una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre sí.

Los protocolos a utilizar para este proyecto son los siguientes:

**FTP (File Transfer Protocol).** FTP (File Transfer Protocol) es un protocolo de transferencia de ficheros entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar ficheros desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier fichero, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante lo tiene muy fácil para capturar este tráfico, acceder al servidor, o apropiarse de los ficheros transferidos.

**HTTP (Hyper Text transfer Protocol).** El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas Web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido. También sirve el protocolo para enviar 'información adicional en ambos sentidos, como formularios con campos de texto. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden. Por esto se popularizaron las cookies, que son pequeños ficheros guardados en el propio ordenador que puede leer un sitio Web al establecer conexión con él, y de esta forma reconocer a un visitante que ya estuvo en ese sitio anteriormente. Gracias a esta identificación, el sitio Web puede almacenar gran número de información sobre cada visitante, ofreciéndole así un mejor servicio.

**HTTPS.** El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es aquí, cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS). Los protocolos https son utilizados por navegadores como: Safari (navegador), Internet Explorer, Mozilla Firefox, Opera,... entre otros. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El puerto estándar para este protocolo es el 443. Para conocer si una página Web que estamos visitando, utiliza el protocolo https y es, por tanto, segura en cuanto a la trasmisión de los datos que estamos transcribiendo, debemos observar si en la barra de direcciones de nuestro navegador, aparece https al comienzo, en lugar de http.

Algunos navegadores utilizan un icono en la barra de estado (parte inferior de la ventana), indicando la existencia de un protocolo de comunicaciones seguro.

**SSL (Secure Sockets Layer).** Secure Sockets Layer (SSL) y Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente (phising) y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación

- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

**TCP (Transmission Control Protocol) / IP (Internet Protocol).** TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware. TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmisión Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto

**Fast Ethernet.** Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps. En su momento el prefijo fast se le agregó para diferenciarlas de la Ethernet regular de 10 Mbps. Fast Ethernet no es hoy por hoy la más rápida de las versiones de Ethernet, siendo actualmente Gigabit Ethernet y 10 Gigabit Ethernet las más veloces. En su momento dos estándares de IEEE compitieron por el mercado de las redes de área local de 100 Mbps. El primero fue el IEEE 802.3 100BaseT, denominado comercialmente Fast Ethernet, que utiliza el método de acceso CSMA/CD con algún grado de modificación, cuyos estándares se anunciaron para finales de 1994 o comienzos de 1995. El segundo fue el IEEE 802.12 100BaseVG, adaptado de

100VG-AnyLAN de HP, que utiliza un método de prioridad de demandas en lugar del CSMA/CD. Por ejemplo, a la voz y vídeo de tiempo real podrían dárseles mayor prioridad que a otros datos. Esta última tecnología no se impuso, quedándose Fast Ethernet con casi la totalidad del mercado.

## 4.7. DESCRIPCIÓN DEL FIREWALL A IMPLEMENTAR

El Firewall a implementar es un Firewall tipo software desarrollado por Microsoft desde hace mucho tiempo atrás, se ha escogido para este proyecto el Firewall Internet Security and Accelerator (ISA) debido a las siguientes características de este poderoso Firewall además se contará con la posibilidad de trabajar con la última versión de este Firewall el ISA Server 2006.

### INTERNET SECURITY AND ACCELERATION SERVER 2006 (ISA SERVER 2006)

ISA Server 2006 es un gateway integrado de seguridad perimetral que le ayuda a proteger su entorno de TI frente a amenazas procedentes de Internet y además proporciona a sus usuarios un acceso remoto rápido y seguro a las aplicaciones y datos corporativos. ISA Server 2006 está disponible en dos versiones: la edición estándar y la enterprise. En esta página mostramos información sobre las funcionalidades y características que serán comunes a ambas versiones, salvo en los casos en que se indique otra cosa.

ISA Server 2006 proporciona seguridad integrada, gestión eficiente y acceso seguro y rápido para todo tipo de redes.

ISA Server 2006 ofrece valor a los responsables de TI, los administradores de red y los profesionales de la seguridad en la información: todos ellos se preocupan de los aspectos de seguridad, capacidad de gestión y reducción de costes de las operaciones de red. ISA Server 2006 puede ayudarles a todos en distintas áreas:

- *Publicación segura de contenidos, para acceso remoto*. ISA Server 2006 permite optimizar la solución adoptada al mantener un elevado nivel de seguridad para aquellas aplicaciones corporativas a las que se accede desde Internet.
- *Conectividad y seguridad para redes de oficinas*. ISA Server 2006 supone una solución potente para expandir de forma segura las redes corporativas y reducir sus costes, al aprovechar al máximo todos los recursos existentes de conectividad.

- *Defensa frente a amenazas internas y externas basadas en Web*. ISA Server 2006 se ha sido diseñado para mantener los niveles de seguridad más elevados y proteger y gestionar de forma adecuada sus redes.

Las empresas necesitan ofrecer a sus empleados y colaboradores un acceso remoto en buenas condiciones y seguro a sus aplicaciones, documentos y datos desde cualquier PC o dispositivo.

Publicación segura de aplicaciones con ISA Server 2006 ya se pueden exponer los servidores Exchange, SharePoint, y de otras aplicaciones Web para su acceso desde fuera de la red corporativa de forma segura. Mediante la pre-autenticación de usuarios antes de que accedan a ningún servidor publicado, la inspección de paquetes a nivel de capa de aplicación -incluso si los datos están cifrados- manteniendo sus características previas ("stateful") y por medio de las herramientas de publicación automática que incorpora, ISA Server 2006 facilita la tarea de crear un entorno seguro para aquellas aplicaciones corporativas a las que se debe dotar de acceso a través de Internet.

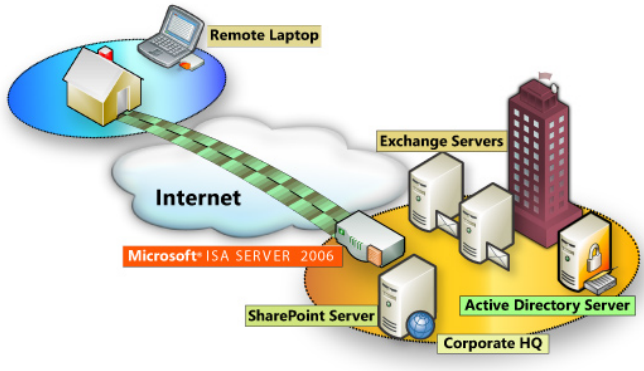



**Figura 4.3. Conectividad Y Seguridad Para Las Redes De Oficinas.**

Las empresas necesitan conectar sus oficinas remotas con sus sedes centrales, disponer de un acceso a Internet con las máximas garantías de seguridad desde esas oficinas y aprovechar al máximo el ancho de banda disponible, haciendo un uso eficiente del mismo.

Las organizaciones pueden utilizar ISA Server 2006 como un gateway para redes de sucursales que permite conectar y proteger los enlaces de sus redes de oficinas, utilizando el ancho de banda disponible con la máxima eficiencia. Dispone de funcionalidades como la compresión HTTP, el cache de contenidos (incluyendo las actualizaciones de software y funciones de VPN (Virtual Private Networks) entre sitios remotos, todo ello integrado

junto con un potente filtrado de paquetes a nivel de aplicación. ISA Server 2006 es una forma efectiva de ampliar su red corporativa manteniendo los máximos estándares de seguridad y capacidad de gestión de los recursos.

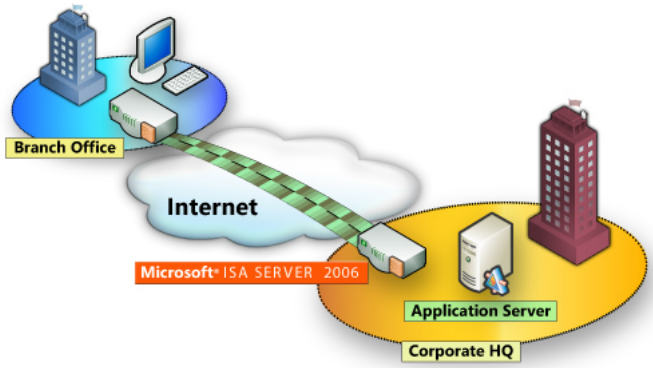



**Figura 4.4. Defensa Frente A Amenazas Basadas En Web, Internas Y Externas.**

Las empresas necesitan eliminar los nocivos efectos del malware y ataques externos por medio de un conjunto completo de herramientas de análisis y bloqueo de contenidos dañinos, archivos potencialmente peligrosos y sitios Web sospechosos.

Protección del acceso a Internet: con ISA Server 2006 las organizaciones pueden proteger sus entornos de TI frente a ataques y amenazas basadas en tecnologías de Internet, tanto de origen interno como externo. Su arquitectura híbrida proxy-firewall, su potente inspección interna de paquetes, su capacidad para aplicar políticas con una alta granularidad y funcionalidades completas de alerta y monitorización hacen posible una protección real para la red y una mayor facilidad de gestión de los recursos de conectividad.

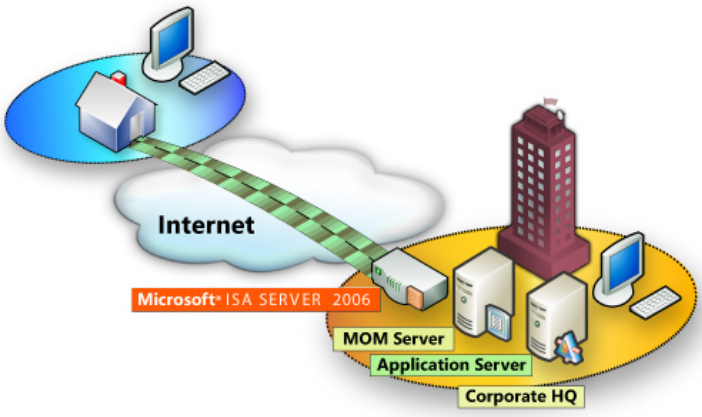



**Figura 4.5. Protección del Acceso a Internet.**

## 4.8. DESCRIPCIÓN DE LAS FUNCIONES A CONFIGURAR EN LA CENTRAL TELEFÓNICA

Para escoger una central telefónica se debe tener en cuenta las necesidades del usuario de acuerdo a esto se compara con las funciones de las diferentes centrales y así se escoge la misma. En este proyecto ya se cuenta con una central telefónica el cual se lo va a configurar para su uso, se trata del sistema híbrido avanzado Panasonic KX-TA616.


**Figura. 4.6. Comunicación de Central telefónica.**

El sistema le permite integrarse a una amplia gama de equipos de comunicación y teléfonos propietarios. Cada puerto de extensión “Híbrido” permite acomodar teléfonos propietarios análogos así como cualquier dispositivo de línea sencilla (tales como el sistema Telefónico Integrado (ITS), máquinas de fax, maquinas contestadoras, teléfonos inalámbricos, módems de computadoras, etc.). Tarjetas o cables adicionales no son requeridos.

Se ha escogido esta central telefónica debido a sus funciones, su rendimiento y a los beneficios que esta trae. A continuación se detallan algunas funciones importantes:

· Acceso a líneas Externas.
· Captura de Llamada.
· Conversión de Pulso a Tono.
· DISA (Acceso Directo al Anexo) con mensaje.
· Grupo de Extensiones.
· Línea de Entrada Directa.
· Línea de Entrada / Línea de Salida.
· Llamada de Operador.

· Llamada de Regreso cuando esta Ocupado.

· Llamada en Espera.

· Llamada Interna.

· Mensaje de Bienvenida (OGM).

· Música para la Retención de Llamada (BGM).

· Tono Distintivo de Llamada.

· Transferencias de Llamadas hacia extensiones.

## 4.9. COSTOS

Para determinar los materiales a utilizar en las diferentes redes, se debe analizar las necesidades del usuario y otros aspectos los cuales se detallan en el Capítulo V, Tema 5.1 Descripción y Selección de Materiales a Utilizar, en este tema se detallarán los materiales con sus respectivos precios encontrados departamentos técnicos. A continuación se detallan precios de los materiales a utilizar en la implementación de las diferentes redes para este proyecto.

| CANT. | DESCRIPCIÓN | PRECIO UNITARIO | PRECIO TOTAL |
|---|---|---|---|
| 1 | Rack 19" de 4U marca Nexxt. (*) | 29,00 | 29,00 |
| 1 | Patch Panel 24 entradas marca Nexxt. (*) | 45,00 | 45,00 |
| 1 | Patch Panel 12 entradas marca Nexxt. (*) | 31,00 | 31,00 |
| 1 | Bandeja para rack marca Nexxt. (*) | 15,00 | 15,00 |
| 1 | Organizadores de cable con tapa. | 10,14 | 10,14 |
| 2 | Switch de 24 entradas marca D- Link modelo DES- 1024D. (*) | 90,00 | 180,00 |
| 1 | Wireless Router marca Linksys modelo WRT54G. (*) | 90,00 | 90,00 |
| 2 | Cajas de rollos de cable UTP Categoría 5 (60 Metros). | 25,00 | 50,00 |
| 24 | Patch Cables CAT5E 2m | 1,95 | 46,80 |
| 24 | Cables Telefónicos RJ45. | 1,50 | 36,00 |
| 24 | Cajetines dobles de voz y datos marca Nexxt. (*) | 5,00 | 120,00 |
| 49 | Canaletas de 32x18 | 1,96 | 96,04 |
| 10 | Canaletas de 40x25 | 4,55 | 45,50 |
| 49 | Accesorios para Canaletas. | 0,40 | 19,60 |
| | | **Subtotal** | 814,08 |
| | | **12% IVA** | 97,69 |
| | | **TOTAL** | 911,77 |

(*) La selección de equipos se detalla en el Capítulo V

Tabla 4.2. Costos de materiales a utilizar.

# CAPÍTULO V

# IMPLEMENTACIÓN

## 5.1. DESCRIPCIÓN Y SELECCIÓN DE MATERIALES A UTILIZAR EN LA CONSTRUCCIÓN DE LAS REDES

Para seleccionar el material a utilizar en la implementación de las redes primeramente se debe tomar en consideración algunos puntos importantes en este caso algunos temas descritos en capítulos anteriores como infraestructura del sitio a implementar, características de las necesidades, area de cobertura, ubicación de los puntos de acceso, etc., posteriormente se verifica en el mercado la existencia de los materiales necesarios para implementar estas redes. Tomando en cuenta estos dos puntos se escogieron diferentes tipos de materiales necesarios para esta implementación los cuales se detallan a continuación:

| | |
|---|---|
| 1 | Rack 19” de 4U marca Nexxt. |
| 1 | Patch Panel 24 entradas marca Nexxt. |
| 1 | Patch Panel 12 entradas marca Nexxt. |
| 1 | Bandeja para rack marca Nexxt. |
| 1 | Organizadores de cable con tapa Nexxt. |
| 2 | Switch de 24 entradas marca D- Link modelo DES- 1024D. |
| 1 | Wireless Router marca Linksys modelo WRT54G. |
| 2 | Cajas de rollos de cable UTP CAT5E Nexxt. |
| 24 | Patch Cables CAT5E. |
| 24 | Cables Telefónicos RJ45. |
| 24 | Cajetines dobles de voz y datos marca Nexxt. |
| 49 | Canaletas de 32x18 |
| 10 | Canaletas de 40x25 |
| 49 | Accesorios para Canaletas. |

**Tabla. 5.1. Materiales para el diseño.**

**Organizadores con Tapa.** Los organizadores con tapa proporcionan un medio ordenado y eficiente para dirigir y proteger los cables, además de dar una solución de instalación más elegante. Estos accesorios pueden ser usados en cualquier rack o gabinete de 19” y ayudan a mantener el radio de tensión apropiado de los cables. Dimensiones: Alto: 1.75” x Ancho: 19” x Profundidad: 1.76” Este organizador se seleccionó por su facilidad en conseguirlo en el mercado y a que cumple con las dimensiones y requerimientos para ubicarlo en el rack seleccionado.

**Figura. 5.1. Organizador con tapa.**

**Bandejas para Racks y Gabinetes.** Nexxt ofrece una gran variedad de bandejas para cubrir todas las necesidades como son: Bandejas sólidas de uso general: La solución perfecta para equipos pesados. Estas bandejas pueden soportar hasta más del 50% del peso que soportan las bandejas ventiladas. Disponibles en dos tamaños: sencilla y doble. Profundidad 14.95 in. La bandeja para rack detallada anteriormente se seleccionó por su facilidad en conseguirlo en el mercado y a que cumple con las dimensiones y requerimientos para ubicarlo en el rack seleccionado.

**Figura. 5.2. Bandejas Sencilla para Rack.**

**Rack de Pared.** Los racks pueden ser montados directamente sobre la pared, comúnmente utilizados para cualquier instalación estándar pequeña de 19”, que no requiera de altos niveles de seguridad. Estos equipos brindan una instalación organizada con apariencia profesional. Dimensiones: (H5.25” x W19”x D5.8”). 4U. Este material se seleccionó

debido a su calidad, resistencia y por experiencia en el uso del mismo debido a su gran utilidad en la construcción de redes.

**Figura. 5.3. Rack de Pared. 4U.**

**Patch Panels CAT5E.** Los Patch Panels Cat5e de Nexxt están diseñados excediendo los requisitos de la norma ANSI/TIA/EIA 568-A. Estos Patch Panels están hechos para su instalación directa en estantes de 19” y se ofrecen en configuraciones de 12, 24, y 48 puertos; todos con las configuraciones T568A y T568B. Viene con terminales de conexión en bronce fosforoso estañado, según el estándar 110 IDC (conductores de 22 a 26 AWG), esto proporciona una conexión con un desempeño más seguro y confiable. Los patch panels anteriormente mencionado fueron seleccionados ya que se adaptan perfectamente al rack seleccionado, brindan facilidades al seleccionar el protocolo y de ubicar los cables además de cumplir con los requerimientos necesarios para la construcción de la red.


**Figura. 5.4. Par Protocolo 568-A ó 568-B.**

**Figura. 5.5. Patch Panel 12 Puertos**.

**Figura. 5.6. Patch Panel 24 Puertos.**

**D-Link Switch 24 puertos 10/100Mbps DES-1024D.** El Switch no administrable DES-1024D 10/100Mbps está diseñado para aumentar el rendimiento en una red LAN y proporcionar un alto nivel de flexibilidad. Fácil de usar, este dispositivo permite a los usuarios conectarse en forma muy simple a cualquier puerto a 10Mbps ó 100Mbps en una red, multiplicar el ancho de banda, tiempo de respuesta y satisfacer sus requerimientos de acceso a los servicios de red. Adicionalmente provee soporte para la detección Auto MDI/MDIX Crossover en todas las puertas, eliminando la necesidad de cables crossover o puertas Up-Link.

Características:

- Control de Flujo para transmisión segura
- Auto-negociación MDI/MDIX
- Tamaño desktop.
- Plug & Play
- Con Kit de montaje para instalación en Rack de 19 pulgadas.
- Soporte Full/Half duplex por puerto.

Para seleccionar el switch antes mencionado se realizó una tabla comparativa de las características de los mismos.

| REQUISITOS BÁSICOS | DLINK 1024D | 3COM SUPERSTACK 3 SWITCH 3870 |
|---|---|---|
| 24 PUERTOS | CUMPLE | CUMPLE |
| MONTAJE EN RACKS DE 17" Y ESPECIAL DE 19" | 17" Y 19" | 17" |
| VELOCIDAD 10/100 MBPS | CUMPLE | CUMPLE |
| PESO | 2,6 KG | 5 KG. |
| PRECIO | $80 | $150 |

**Tabla. 5.2. Comparación Switches.**

En base a las características básicas requeridas y el precio, se selecciono el equipo Switch D-Link 1024D.

**Figura. 5.7. D-Link 1024D Switch 24 puertos.**

**Linksys WRT54G Ruteador de banda ancha Wireless-G.** Wireless-G es el novedoso estándar de red inalámbrica de 54 Mbps que proporciona una velocidad casi 5 veces superior que los populares productos Wireless-B (802.11b) para el hogar, la oficina y establecimientos públicos con conexiones inalámbricas en cualquier lugar. Los dispositivos Wireless-G comparten una banda de radio común de 2,4 GHz, por lo que también funcionan con equipos Wireless-B de 11 Mbps existentes. Ya que ambos estándares son incorporados, puede aprovechar la inversión realizada en infraestructura 802.11b y migrar al novedoso y velocísimo estándar Wireless-G a medida que aumentan todas las necesidades de una red.

El ruteador de banda ancha Wireless-G de Linksys supone, en realidad, tres dispositivos en uno. En primer lugar, el punto de acceso inalámbrico, que permite conectar dispositivos Wireless-G o Wireless-B a la red. También incorpora un conmutador 10/100 de cuatro puertos de dúplex completo para conectar dispositivos Ethernet con cables. Tiene los puertos para conectar cuatro PC directamente o encadenar en margarita varios concentradores y conmutadores para crear una red que satisfaga varios requisitos. Por último, la función de ruteador une todos los elementos y permite compartir una conexión a Internet DSL o por cable de alta velocidad en toda la red.

Características:

- Ruteador para compartir Internet, conmutador de 4 puertos y punto de acceso Wireless-G (borrador 802.11g) "todo en uno".
- Velocidades de transferencia de datos de hasta 54 Mbps: 5 veces más rápido que Wireless-B (802.11b).

- Compartir una única conexión a Internet y otros recursos con clientes con cables Ethernet y Wireless-G.
- Funciona con dispositivos Wireless-B
- Seguridad inalámbrica avanzada con encriptación WEP de 128 bits y filtrado de direcciones MAC o IP.

**Figura. 5.8. Ruteador Wireless.**

Para seleccionar el router wireless de Linksys se realizó una tabla comparativa de varios equipos existentes en el mercado.

| REQUISITOS BÁSICOS | LINKSYS WRT54G | D-LINK DWL-2100AP |
|---|---|---|
| ESTÁNDAR 802.11 B Y G | CUMPLE | CUMPLE |
| ACCESS POINT Y RUTEADOR | CUMPLE | SOLO ACCESS POINT |
| SEGURIDAD WEP, WAP Y WAP2. | CUMPLE | SOLO WEP |
| SERVIDOR DHCP | CUMPLE | CUMPLE |
| PRECIO | $90 | $110 |

**Tabla. 5.3. Comparación Concentradores Wireless.**

En base a las características básicas requeridas y el precio, se selecciono el equipo Linksys WRT54G.

**Cable UTP CAT5E Nexxt.** Cable UTP Cat5e está diseñado para transmisión de datos a altas velocidades en soluciones LAN (Red de área local) bajo el estándar ANSI/TIA/EIA-568. 2 Categoría 5e e ISO/IEC 11801.

**Características:**

• Número de Pares: 4

• Conductores: 8

• AWG: 24

• Tipo: Sólido CM

• Alambre de Cobre

Por experiencia, se selecciono el cable marca Nexxt, debido a que cumple los requisitos básicos y posee normas de Calidad Internacional


**Figura. 5.9. Caja de Cable UTP CAT5E.**

**Cajetines Superficiales CAT5E Nexxt.** Los cajetines Superficiales Cat5e tienen un diseño compacto y están diseñadas para ser instaladas en superficies planas. Vienen con el Conector Hembra RJ-45 Integrado, autoadhesivo y tornillos de instalación. Disponible en 1 y 2 puertos para voz y datos. Dimensiones: L60.00 x A54.40 x Alt.26.60 mm.

Este material se seleccionó debido a su calidad, resistencia y por experiencia en el uso del mismo.

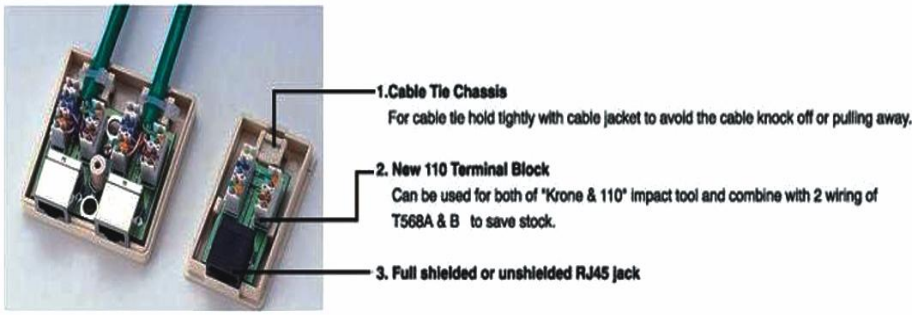



**Figura. 5.10. Cajetines CAT5E.**

**Figura. 5.11. Cajetín Superficial**.

**Patch Cordons CAT5E y RJ45.** Los Patch Cables Cat5e UTP, de par trenzado, cumplen la función de transportar datos, voz e imágenes bajo los estándares de la industria. Características Eléctricas (ISO/IEC 11801, TIA/EIA 568, En 50173), Impedancia: 100 Ohmios El +/- 15%, Máx. D.C. Resistencia: 14,8 Ohm/100m (26 AWG), Máx. Resistencia Desequilibra: el 3% (el 5% para TIA/EIA), Min. Velocidad de propagación: 0.65C. Contactos: placa de níquel con baño de oro de 50um. Longitudes disponibles: 3, 7, 10, 14, 25 y 50 pies de largo. Colores disponibles: gris, azul, rojo, amarillo, verde, negro y blanco.

**Figura. 5.12. Patch Cables y Cable RJ45.**

**Canaletas y Accesorios.** Canaleta de PVC rígido antiflama, con adhesivo de alta calidad, de 2 m de largo, diseñada para proteger cableado o alambrado en instalaciones eléctricas, de voz o datos, en color gris. Se utiliza para cables de hasta 8 hilos o de 1 x 2 cm.

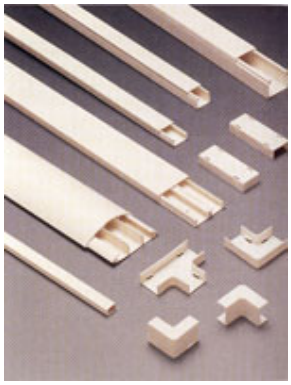


**Figura. 5.13. Canaletas.**

## 5.2. CONSTRUCCIÓN DE LA RED LAN

En la construcción de este tipo de redes se procede primeramente a ubicar un sitio central para que sea el cuarto de equipos donde se ubicarán los equipos y a donde llegarán todos los cables provenientes de los puntos, este cuarto se lo ubicará en la planta baja ya que ahí es donde se encuentra la mayor cantidad de puntos.

A continuación se procede a ver el camino por donde irán los cables y las canaletas teniendo siempre en consideración los caminos por donde irán pocos cables para ubicar canaletas medianas y caminos donde irán bastantes cables para ubicar canaletas que soporten mayor capacidad de los mismos.

Una red LAN siempre será bien construida cuando se respeten normas y estándares, para definir el sistema de cableado por el cual se regirá el proyecto, se considerarán las normas que establece el sistema de cableado estructurado, específicamente se adoptará la norma 568-A debido a que todos los puntos necesitan tener la misma norma para que exista comunicación entre ellos. Como medio físico se utilizará el cable UTP CAT5e, ya que éste permite mayor rapidez para el manejo de información y es el más utilizado y recomendado en el mercado. Este medio físico tendrá una longitud máxima de 100 mts, tal y como lo establecen las normas del Cableado Estructurado.

Como siguiente paso se procede a ponchar todos los cables provenientes de los diferentes puntos al correspondiente Patch Panel ubicados en el Rack previamente instalado en el cuarto de equipos, respetando un orden específico para ubicar el punto con facilidad en caso de algún daño, seguido de una prueba de continuidad mediante un LAN Tester desde el punto del cajetín al Patch Panel, si la prueba resulta satisfactoria se procede al paso final

el cual es conectar los puntos del Patch Panel a su correspondiente Switch y de este a las respectivas tarjetas de red de las máquinas de los usuarios, servidores, teléfonos, etc., siguiendo siempre un orden específico para facilidad de ubicación de los puntos.

Una vez creados los caminos por donde se transmitirá toda la información, se deberá configurar el o los servidores para su uso, en este proyecto se configurará un solo servidor el cual desempeñará todas las funciones requeridas. Para esto se utilizará de la función Administre su Servidor para crear todas la funciones necesarias, primeramente se configura el servidor como Controlador de Dominio utilizando el wizard lo que creará conjuntamente el Servidor DNS, Servidor DHCP y Active Directory; una vez implementados estas funciones se procede a crear los usuarios del dominio y las máquinas que se usarán en la red en la función de Usuarios y Equipos de Active Directory, posteriormente se une al dominio todas las máquinas creadas anteriormente para que el servidor las reconozca y pueda trabajar con ellas; posteriormente se configura el Servidor DHCP para que entregue direcciones privadas dinámicas a equipos conectados a la red activados previamente la opción Obtener una Dirección IP Automática para esto se asigna un grupo de direcciones que pueda hacer uso el Servidor DHCP y un grupo de Direcciones Restringidas las cuales el servidor no podrá entregar a ningún usuario de la red, finalmente y por requerimientos de la empresa las máquinas de la red se configuran con direcciones IP estáticas las cuales fueron concedidas en el grupo de Direcciones Restringidas en el Servidor DHCP y los equipos visitantes o clientes VPN se les concede direcciones IP dinámicas, debido a este procedimiento no es necesario configurar la función de Servidor DNS ya que los registros A y PTR se crean automáticamente en direcciones IP estáticas por el Servidor DNS.

Para terminar la creación de la red LAN se realizan pruebas de comunicación enviando una petición con respuesta mediante un ping de dirección IP y mediante el nombre DNS de la máquina desde el servidor a las máquinas y viceversa para comprobar conectividad y resolución de nombres en el Dominio, posteriormente se comprueba las direcciones dinámicas activando en varias máquinas la opción Obtener una Dirección IP Automáticamente, a continuación se compraba que no existan errores mediante el visor de sucesos de Windows en el servidor y en los clientes, si las pruebas resultan exitosas se procede a compartir documentos necesarios e ingresar al grupo, finalmente se procede a ingresar a la red creada mediante conexiones de red y verificar que todas las máquinas de la red se puedan ver y acceder ellos para concluir con la implementación de la red LAN.

## 5.3. IMPLEMENTACIÓN DE LA RED WLAN

El funcionamiento básico de una red WLAN es utilizar ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) se conecta la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero se puede colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena. La naturaleza de la conexión sin cable es transparente al sistema del cliente.

Para este proyecto se procederá como primer paso encontrar un sitio central donde se ubicará el concentrador inalámbrico en este caso el Wireless Router WMP54G el cual enviará la señal que tiene que llegar a todos los sitios propuestos en el tema 4.1 Area de Cobertura, por lo que se procede a tener en consideración ciertas recomendaciones como no ubicar el concentrador cerca de estantes metálicos de gran tamaño, hornos microondas, artefactos inalámbricos para evitar cualquier obstáculo, instalar el concentrador cerca de piso falso o tumbado, a continuación se procede a detectar la menor cantidad de señales en un sitio específico, para esto se instala un software el cual ayude a detectar otras señales en el area de cobertura, en este caso se instalará el software llamado NetStumbler, con el cual se podrá ver las señales que pueden interferir a la red WLAN a implementar y los canales

de las señales existentes, en esta prueba se comprobó que el sitio ideal se encuentra cerca del cuarto de servidores por lo que se tratará de realizar las pruebas faltantes desde esta ubicación para una mejor administración del mismo además se comprobó que el canal sin utilizar es el nueve por lo que usará este canal, a continuación se realiza un recorrido por el área de cobertura con una portátil haciendo un ping continuo al concentrador el cuál ya está ubicado en el cuarto de servidores, la prueba da como resultado que la señal llega al area de cobertura deseada con una respuesta menor a 1ms en la planta baja y menor a 8ms en el area deseada de la planta alta, finalmente se realiza la prueba para verificar la potencia de la señal lo que dará la información sobre la velocidad de la misma, mediante la ayuda del software utilizado anteriormente se recorrerá el area de cobertura para verificar velocidad de la misma, con esto se determinó que la velocidad en la planta baja oscila de 48Mbps hasta 54Mbps y la velocidad en el area de la planta alta oscila de 32Mbps hasta los 54Mbps, por lo que se concluye que el sitio ideal para ubicar el concentrador inalámbrico es el cuarto de servidores por ser un sitio central y cumple con los requerimientos de la red WLAN como son: comunicación, poca interferencia y velocidades aceptables.

El estándar a utilizar en esta red es el 802.11b y 802.11g por lo que se configura el Router Wireless mediante la página principal del equipo para que sea compatible con ambos estándares, una vez realizadas las pruebas se comprobó que el equipo llegará con su señal hasta una distancia máxima de 85 metros en interiores con esto se verifica el alcance permitido por el fabricante que dice que el alcance de una red WLAN del estándar 802.11 es de 100 metros en interiores y de hasta 300 metros en espacios abiertos, se trabajará además con una velocidad de 54Mbps debido a que se utiliza el estándar 802.11b y 802.11g. Debido a que cada Punto de Acceso puede dar servicio a 20 equipos o más se administrará la red WLAN para evitar incremento de usuarios móviles en la red ya que la cantidad está limitada por el uso que se haga del ancho de banda, es decir, cuantos más equipos estén funcionando simultáneamente, más lenta será la transmisión, se configura el equipo para que utilice una seguridad para establecer conexión al concentrador o a la Red WLAN en este caso se utilizará WPA con algoritmo TKPI para conexión con dispositivos móviles en la cual solo los usuarios que conozcan la contraseña podrán ingresar a la red y podrán obtener los beneficios de la misma, finalmente al concentrador se le asignará una dirección IP fija en el rango de la red interna y los usuarios que se conecten a este se les proporcionará una IP otorgada por el Servidor DHCP de la red.

Esta red se implementó para el uso de cualquier usuario sin importar el equipo tales como: Computadores Portátiles, Pocket PC, Computadores de Escritorio, entre otros, con el requerimiento de adaptadores inalámbricos en los equipos como tarjetas PCI o PCMCIA los cuales cumplan con la norma 802.11b o 802.11g para poder ingresar a la red WLAN.

## 5.4. IMPLEMENTACIÓN DE LAS REDES VIRTUALES (VPN Y MODEM)

VPN son las siglas de Red Privada Virtual (Virtual Private Network). Este servicio consiste en la extensión de la Red Informática Cableada de la Empresa INGELSI Cia. Ltda. a ordenadores que no estén ubicados físicamente en esta. De esta forma se permite a los usuarios de la Empresa conectarse desde un ordenador externo a la red empresarial de forma sencilla y transparente, formando parte de la red interna aunque el equipo no se encuentre físicamente en las dependencias de la empresa. La velocidad de acceso dependerá del tipo de conexión a Internet que utilice el usuario.

El esquema de este tipo de conexión es el siguiente:

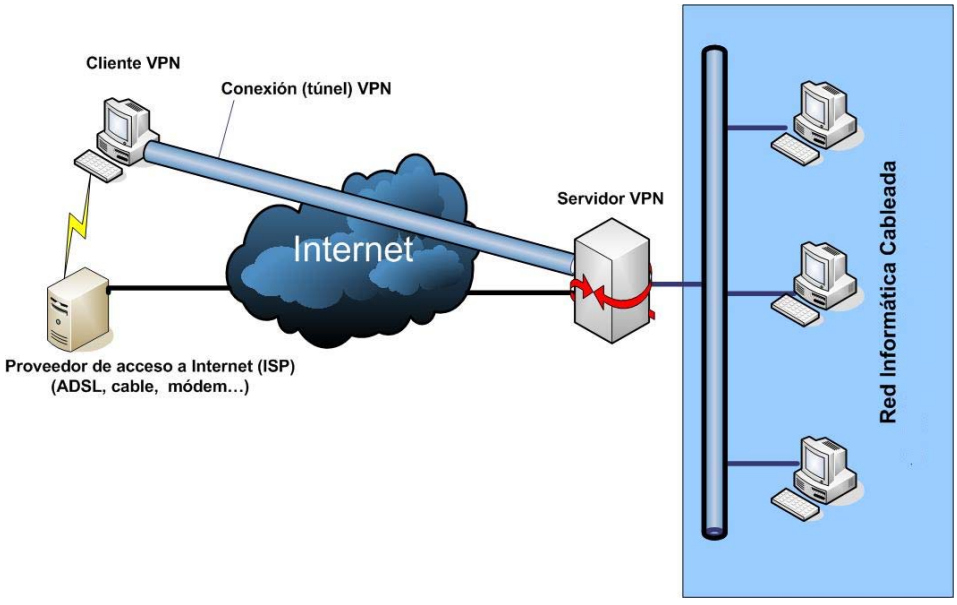



**Figura. 5.14. Conexión VPN.**

El sistema establece una conexión segura específica (túnel virtual) entre un ordenador y un servidor situado en la Red Informática Cableada de la Empresa INGELSI Cia. Ltda. Desde el momento de la conexión, todas las conexiones de red irán encaminadas a través de ese túnel seguro. Antes de establecer el túnel se requiere la autenticación del usuario, mediante usuario y contraseña, siendo por tanto un medio de conexión bastante seguro.

Para realizar una Red Privada Virtual (VPN) se puede utilizar una conexión desde el exterior hacia el equipo de la red mediante Internet (Red Privada Virtual) o realizar un Acceso Telefónica a Redes mediante Dial- UP. Para ambos casos se necesita configurar el servicio que viene incluido en Windows Server 2003 llamado Enrutamiento y Acceso Remoto, el cual permitirá la comunicación desde el exterior hacia el equipo. Para configurar este servicio se ingresará por medio de Herramientas Administrativas de Windows Server, primeramente se deshabilita el servicio haciendo click derecho sobre el mismo y seleccionar deshabilitar, a continuación se realizan los mismo pasos anteriores pero se escoge la opción habilitar y se continúa con el asistente seleccionando la opción predeterminada, Acceso Remoto (acceso telefónico o red privada virtual), seguido de Acceso Telefónico (Dial-UP), a continuación se comprueba que esté seleccionado Conexión área local y se aceptan los demás valores predeterminados hasta finalizar el asistente, finalmente aparece un mensaje indicando que debe configurar las propiedades del Agente de retransmisión DHCP para lo que se hará click en aceptar, una vez realizado estos pasos se culmina con la instalación verificando que en la consola Enrutamiento y Acceso Remoto se muestra una nueva configuración bajo el icono del servidor.

Para la Empresa INGELSI Cia. Ltda. es de mucha importancia esta comunicación ya que el Departamento de Contabilidad, Gerente o Administradores podrán ingresar a la red de la Empresa desde cualquier lugar y sincronizar su base de datos para obtener información importante de la Empresa como ingresos, egresos, etc., y así saber todo lo que pasa en la Empresa aunque se encuentren fuera de ella, además que los usuarios podrán aprovechar el Internet de la empresa el cual no se usa en horas fuera de oficina.

En este proyecto se ha utilizado un Firewall el ISA Server 2006 el cual es capaz de controlar al servicio antes mencionado mediante opciones que vienen incluidas en este Firewall, mediante este servicio podemos habilitar la conexión ya sea Internet o Módem en este caso utilizaremos un Módem externo debido a su mejor desempeño que un módem interno, otras opciones que vienen incluidas son las de conceder permisos a ciertos usuarios o a los usuarios del Dominio, además de permitir el acceso a determinadas horas y finalmente el poder controlar los protocolos a utilizar cuando se realice esta conexión para una mayor seguridad al equipo, a la información y a la red.

Una vez realizada la configuración del Firewall los usuarios podrán ingresar a la VPN de la siguiente manera:

Los usuarios que deseen realizar una conexión a la Red Privada Virtual mediante una conexión previa de Internet tendrán que crear una conexión VPN ingresando a Conexiones de Red/ Crear Nueva Conexión/ Conectarse a la red de mi lugar de trabajo/ Conexión de red privada virtual/ Ingresar el nombre/ Ingresar IP del Servidor VPN/ Finalizar.

Al contrario para usuarios que deseen realizar un Acceso Telefónico a Redes deberán ingresar a Conexiones de Red/ Crear Nueva Conexión/ Conectarse a la red de mi lugar de trabajo/ Acceso telefónico a redes/ Ingresar el nombre/ Ingresar número de teléfono/ Finalizar.

## 5.5. CONFIGURACIÓN DEL FIREWALL

Antes de comenzar la instalación de ISA Server 2006, es recomendable recopilar información acerca del entorno. Es útil disponer de esta información previamente, ya que es necesaria cuando se ejecuta el asistente para la instalación. Se describe la información que se debe recopilar para instalar o configurar ISA Server 2006. Se debe recopilar información de redes acerca del equipo servidor ISA, tal como se describe a continuación.

**Información general.** Actualizar la siguiente tabla con información acerca del nombre de dominio completo.

Para este proyecto se utilizará:

| Propiedad | Valor |
|---|---|
| Nombre de dominio completo | INGELSI.COM.EC |

**Tabla. 5.4. Dominio.**

**Nota:** Se puede instalar ISA Server 2006 en equipos con un solo adaptador de red.
Normalmente, se llevará a cabo esta tarea cuando otro firewall se encuentre en los límites de la red, conectando los recursos de la empresa a Internet. En este entorno de adaptador de red único, el servidor ISA funciona normalmente como un servidor proxy Web, que almacena en caché el contenido de Internet para que los clientes lo utilicen en la red corporativa. Si instala un adaptador de red único, sólo deberá actualizar la tabla del adaptador de red interno, que se muestra en la siguiente sección.

**Adaptador de Red Interna.** Actualizar la siguiente tabla con información acerca de un adaptador de red interno.

Para este proyecto se tienen los siguientes datos:

| Propiedad | Valor | Propiedad | Valor |
|---|---|---|---|
| Dirección IP | 10.0.0.2 | Máscara de subred | 255.0.0.0 |
| Puerta de enlace predeterminada | 10.0.0.2 | No aplicable | No aplicable |
| Servidor DNS preferido | 10.0.0.2 | Servidor DNS alternativo | ___.___.___.___ |

**Tabla. 5.5. Información IP Red Interna..**

**Adaptador de Red Externa.** Actualizar la siguiente tabla con información acerca de un adaptador de red externo.

A continuación se detalla la siguiente información proporcionada por el ISP contratado para suministrar servicios a la empresa en cuestión.

| Propiedad | Valor | Propiedad | Valor |
|---|---|---|---|
| Dirección IP | 157.100.111.2 | Máscara de subred | 255.255.255.248 |
| Puerta de enlace predeterminada | 157.100.111.4 | No aplicable | No aplicable |
| Servidor DNS preferido | 157.100.45.2 | Servidor DNS alternativo | 157.100.45.11 |

**Tabla. 5.6. Información IP red externa**.

**Adaptador de Red Perimetral.** Actualizar la siguiente tabla con información acerca de un adaptador de red perimetral. Para este proyecto no aplica esta tabla debido a que no se dispone de una red perimetral ya que existe un único servidor en la red.

| Propiedad | Valor | Propiedad | Valor |
|---|---|---|---|
| Dirección IP | ___.___.___.___ | Máscara de subred | ___.___.___.___ |
| Puerta de enlace predeterminada | ___.___.___.___ | No aplicable | No aplicable |
| Servidor DNS preferido | ___.___.___.___ | Servidor DNS alternativo | ___.___.___.___ |

**Tabla. 5.7. Información IP red perimetral.**

Se tomará en consideración algunas recomendaciones para la configurar este tipo de Firewall:

- Si se tiene un servidor con más de un adaptador de red, normalmente se especificará una puerta de enlace predeterminada. Con el servidor ISA, la puerta de enlace predeterminada suele configurarse en el adaptador de red externo.
- Si hay redes internas adicionales conectadas mediante un enrutador, se debe agregar las rutas que sea necesario al servidor ISA antes de empezar la instalación.
- Asegurarse de que el enrutamiento esté debidamente configurado antes de instalar ISA Server 2006.
- En la mayoría de los casos, los servidores de sistema de nombres de dominio (DNS) deben configurarse en el adaptador de red interno y apuntar a un servidor DNS interno, además confirmar que la resolución de nombres funciona correctamente.
- Según la configuración, quizá se deba crear una regla de acceso para permitir consultas DNS desde la red interna.

ISA Server 2006 incluye plantillas de red que corresponden a topologías de red comunes. Se puede seleccionar una plantilla de red que permita configurar rápidamente la topología de red del servidor ISA junto con directivas de Firewall configuradas previamente. Se tiene la posibilidad de seleccionar una plantilla de red para configurar una directiva de Firewall predeterminada para el tráfico entre redes.

Para este proyecto se escogerá la función Firewall Perimetral, debido a que disponemos de dos tarjetas de red la una para la red externa y la otra para la interna, además de que se implementará la red bajo un único servidor.

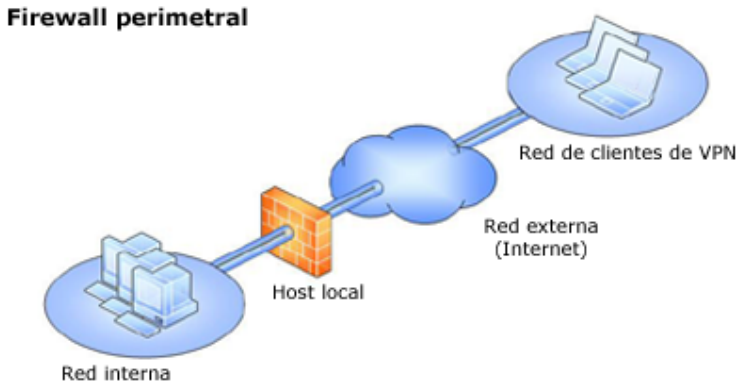



**Figura. 5.15. Firewall perimetral.**

ISA Server 2006 determina si se permite que un paquete pase o se deniegue en función de los siguientes conjuntos de reglas en el orden que se indica a continuación:

- Reglas de red. Se puede utilizar ISA Server 2006 para configurar reglas de red, que permiten definir y describir una topología de red. Las reglas de red determinan si existe una relación entre dos entidades de red y qué tipo de relación se define. Las relaciones de redes se pueden configurar de la forma siguiente:
  - Ruta. Las peticiones de clientes de la red de origen se retransmiten directamente a la red de destino. La dirección del cliente de origen se incluye en la petición.
  - Traducción de direcciones de red (NAT). El servidor ISA sustituye la dirección IP (protocolo de Internet) del cliente en la red de origen por su propia dirección IP.
- Directivas de sistema. ISA Server 2006 incluye una configuración predeterminada de directivas de sistema, que permite el uso de servicios que suelen ser necesarios para que la infraestructura de red funcione correctamente.
- Directivas de firewall. Con ISA Server 2006 se puede crear una directiva de firewall que incluya un conjunto de reglas de publicación y acceso. Estas reglas, junto con las reglas de red y las directivas de sistema, determinan la forma en que los clientes tienen acceso a los recursos a través de las redes.

Para este proyecto se crearon las siguientes Reglas de red:

- Acceso a host local mediante Ruta como la Red de origen Host local y la Red de destino Todas las redes (y host local).
- De clientes de VPN a la red interna mediante Ruta como la Red de origen Clientes de VPN en cuarentena y Clientes VPN y la Red de destino Interna.
- Acceso a Internet mediante NAT como la Red de origen Clientes de VPN en cuarentena, Clientes VPN, Interna y la Red de destino Externa.

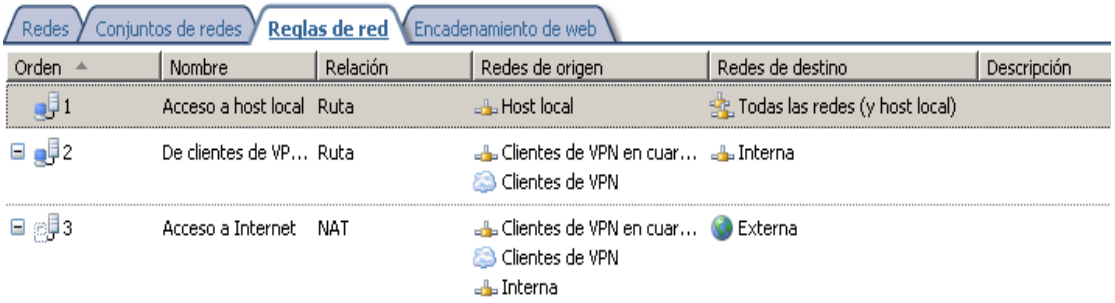



**Figura. 5.16. Reglas de Red.**

Dado que el acceso a la Red es imprescindible debido a que lleva a cabo una gran diversidad de tareas, ISA Server 2006 permite ofrecer a los usuarios un acceso seguro a Internet, esto se lo realiza creando una regla de acceso que permita el tráfico HTTP, HTTPS y FTP desde la red interna a Internet.

Para este proyecto se crearon las reglas de acceso seguro a Internet:

- Cuando se publica una aplicación Web a través del servidor ISA, este protege el servidor Web de un acceso externo directo porque el usuario no puede tener acceso al nombre y la dirección IP del servidor Web. El usuario obtiene acceso al equipo servidor ISA, que reenvía a continuación la petición al servidor Web en función de las condiciones de la regla de publicación del servidor Web.
- Dos aplicaciones a las que los usuarios necesitan habitualmente tener acceso cuando no se encuentran en la oficina son Outlook Web Access y Microsoft SharePoint® Portal Server (sitios Web de intranet). ISA Server 2006 protege los recursos internos a la vez que proporciona un acceso seguro a la información que precisan los usuarios autorizados.
- Antes de ejecutar el asistente de publicación que corresponda, se necesita llenar la siguiente tabla con información relativa a la publicación segura de aplicaciones.

| Descripción | Valor |
|---|---|
| Especificar el nombre de dominio completo del sitio Web que utilizarán los usuarios para obtener acceso al sitio desde Internet. | Nombre de dominio completo: ingelsi.com.ec<br>Por ejemplo: owa.contoso.com. |
| Solicitar e instalar un certificado de servidor Web a través de una entidad emisora de certificados (CA) en el firewall del servidor ISA. Se puede utilizar una entidad emisora de certificados interna, pero es necesario instalar el certificado de entidad emisora de certificados (CA) raíz en todos los equipos que vayan a tener acceso a este servidor Web publicado. | Realizado: Sí (Entidad Emisora de Certificados Interna) |
| Registrar una entrada DNS para el número de dominio completo de su servidor DNS público. Si no administra sus propios servidores DNS públicos, lo normal es que deba dirigir la solicitud al proveedor de servicios Internet (ISP) o a la organización que administra el DNS público de la empresa.<br>**Nota** La dirección IP de la entrada DNS debe ser una dirección IP en el firewall del servidor ISA. | Realizado: Sí |
| Instalar una dirección IP pública válida independiente para cada sitio Web que publique para el que se utilice un certificado de servidor Web distinto. La dirección IP debe instalarse en el adaptador de red externo como dirección IP secundaria. | Dirección IP para servidor Web publicado: 157.100.111.2<br>Máscara de subred: 255.255.255.248 |
| Especificar el nombre de dominio completo del servidor Web interno. | Nombre de dominio completo: ingelsi.com.ec |
| Proporcionar una dirección URL completa para el acceso al servidor Web interno de la red interna. | Dirección URL completa: ___www.ingelsi.com.ec__<br>La dirección URL funciona: Sí |
| Especificar la conexión entre el equipo servidor ISA y el servidor Web interno. | HTTPS |
| Instalar el certificado de la entidad emisora de certificados (CA) raíz de confianza en el equipo servidor ISA, si la conexión al servidor Web interno es HTTPS, y el certificado de servidor Web en el servidor Web interno se emitirá desde una entidad emisora de certificados (CA) interna. | Realizado: Sí |

**Tabla. 5.8. Información General para publicación**.

Actualmente, cualquier empresa necesita tener la posibilidad de recibir mensajes de correo electrónico a través de Internet. ISA Server 2006 proporciona una característica para la publicación segura de recursos de correo electrónico en Internet con filtros de capa de aplicación.

ISA Server 2006 integra un asistente, denominado Asistente para nueva regla de publicación de servidor de correo, diseñado para facilitar la creación de las reglas necesarias en la publicación de servidores de correo y Exchange.

| Descripción | Valor |
|---|---|
| Enumerar los dominios de Internet que van a recibir mensajes de correo electrónico. | Dominio: ingelsi.com.ec<br>Por ejemplo: contoso.com |
| Cree un registro MX para cada dominio. Se crea un registro MX en un servidor DNS público. | Registro MX para cada dominio: Sí |
| Especifique el nombre de dominio completo para los servidores de correo en Internet. La entrada se crea en un servidor DNS público. | Nombre de dominio completo:<br>www.ingelsi.com.ec/owa<br>Por ejemplo: smtp.contoso.com<br>Dirección IP: 157.100.111.2 |
| Especifique la dirección IP del servidor de correo interno. | Dirección IP: 10.0.0.2 |

**Tabla. 5.9. Información General para acceso a correo.**

Para crear las reglas de acceso a se da un click sobre la regla de acceso a crear y añadimos en cada paso los datos proporcionados en las tablas anteriores.

Para este proyecto se crearon las reglas de publicación para:

- Ingreso y Salida del Correo.
- Outlook Web Access OWA.
- Correo Seguro (HTPS).
- Clientes MAPI.
- Correo para Usuarios Móviles.
- Salida de los Usuarios a Internet.
- Acceso a Clientes VPN.

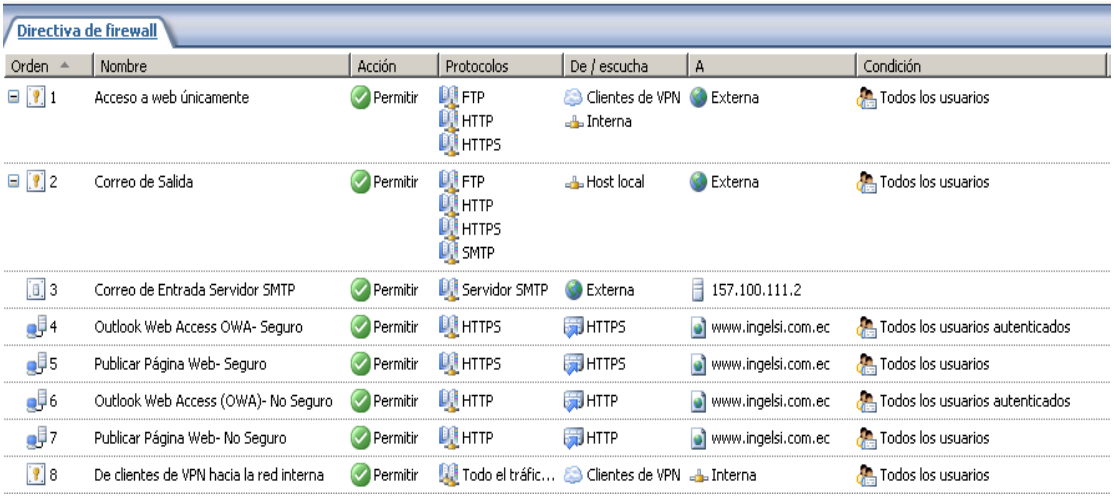



**Figura. 5.17. Directivas de Firewall.**

Microsoft Internet Security and Acceleration (ISA) Server 2006 permite configurar una VPN segura, a la que pueden tener acceso clientes y sitios remotos, según se especifique. Mediante el uso del equipo servidor ISA como servidor VPN, se beneficia de la protección de la red corporativa contra conexiones VPN malintencionadas. Puesto que el servidor VPN está integrado en la funcionalidad del firewall, sus usuarios están sujetos a la directiva de firewall del servidor ISA. Además, mediante el uso del equipo servidor ISA como servidor VPN, se puede administrar las conexiones VPN de sitio a sitio y el acceso de Clientes de VPN a la red corporativa.

El servidor ISA admite dos tipos de conexiones VPN:

- Conexión VPN de acceso remoto. Un cliente de acceso remoto realiza una conexión VPN de acceso remoto que se conecta a una red privada. El servidor ISA proporciona acceso a toda la red a la que está conectado el servidor VPN.
- Conexiones VPN de sitio a sitio. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor ISA proporciona una conexión a la red a la que está conectado el equipo servidor ISA.

Con el servidor ISA, cada tipo de conexión VPN se configura de forma ligeramente diferente. Cuando un solo Cliente de VPN remoto necesita acceso, la configuración va destinada a ese usuario individual. En una configuración de red de sitio a sitio, se debe

otorgar acceso a una red completa de usuarios remotos, es decir, se configura una red de usuarios de VPN.

Sin embargo, la mayor parte de la configuración de la red VPN es común en ambos escenarios. Por ejemplo, el servidor ISA detecta la petición de conexión inicial de una red de sitio remoto como lo haría con cualquier petición de un solo Cliente de VPN remoto. Se deben configurar los protocolos de túnel, los métodos de autenticación, la red de acceso y la asignación de direcciones para la conexión inicial como se haría para un cliente de acceso remoto.

Para crear el acceso a la Red Privada Virtual VPN es necesario habilitar el acceso en el Firewall como se muestra en la Figura 5.18., a continuación se deberá detallar si se desea que los usuarios obtengan direcciones fijas específicas o direcciones por medio de DHCP y finalmente se deberá detallar el grupo de usuarios los cuales puedan tener a acceso a esta red.

Para este proyecto se realizaron los siguientes puntos:

- Activar Acceso a Clientes VPN.
- Obtener direcciones IP por medio de DHCP.
- Grupo de Usuarios del Dominio podrán tener acceso a la misma.

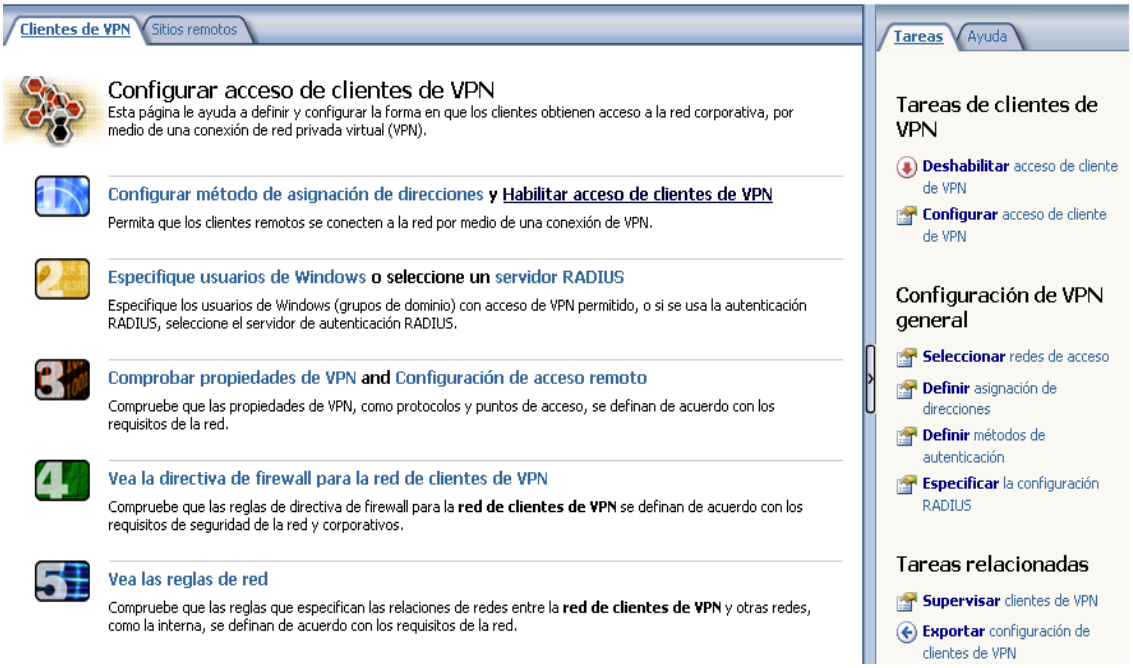



**Figura. 5.18. Acceso Clientes VPN.**

Una vez configurados estos pasos se crea una regla de acceso la cual se realizó en las directivas de acceso en el paso anterior para restringir ciertos recursos a los usuarios a estas redes.

Mediante esta configuración se puede dar acceso a los usuarios VPN y a los usuarios para Acceso Telefónico a Redes instalando previamente un módem en el servidor y en el usuario para que exista comunicación entre ellos, esto se lo puede hacer gracias a que el Firewall Isa Server 2006 controla el servicio de Enrutamiento y Acceso Remoto de Windows Server 2003 pero con muchas más ventajas que el servicio antes mencionado.

Para tener acceso a la Red VPN y al Acceso Telefónico a Redes el usuario debe crear una conexión en el equipo cliente mediante la opción Crear Nueva conexión en Conexiones de Redes de Microsoft, en este paso se debe ingresar información sobre el usuario y dirección IP del servidor a conectarse o ingresar el número de teléfono seguido de cinco comas en adelante seguido del número de la extensión para que el servidor responda ya que la línea del servidor llega a la central telefónica.

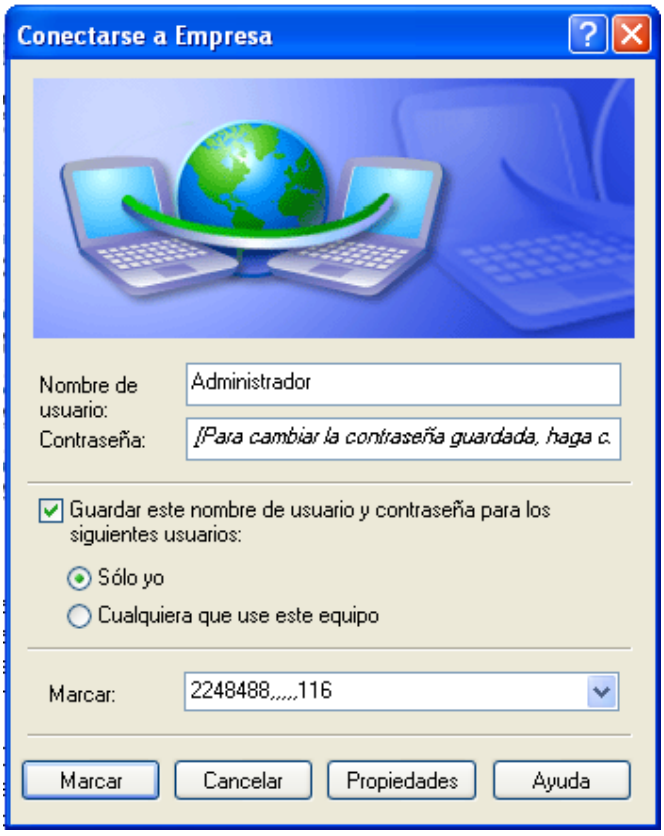



**Figura. 5.19. Acceso de usuarios a VPN.**

## 5.6. CONFIGURACIÓN DE LA CENTRAL TELEFÓNICA

El teléfono es una principal fuente de comunicación ya que se puede acceder para contactar con distribuidores, clientes, amigos, miembros de la oficina y familiares. El sistema Híbrido Avanzado KXTA616 es un sistema telefónico que puede manejar negocios y necesidades personales.

La KX-TA616 acepta 6 líneas CO y 16 extensiones. Con tarjetas opcionales, se puede fácilmente incrementar la capacidad del sistema hasta 6 líneas CO y 24 extensiones dependiendo de las necesidades de la empresa. Este sistema provee las funciones que satisfacen la demanda de los usuarios más sofisticados y conscientes de los costos. Se podrá conectar una variedad de equipos de comunicación tales como teléfonos inalámbricos, maquinas contestadoras, módems verificadores de tarjetas de crédito, máquinas de fax y cualquier otro equipo que trabaje con líneas telefónicas convencionales.

Para empezar la programación de la central telefónica se debe adquirir un teléfono llamado principal el cual será conectado a la central telefónica en la primera extensión en este

proyecto se utilizará el teléfono Panasonic KX- T7030. A esta empresa se le ha asignado 4 líneas telefónicas, las cuales serán utilizadas de la siguiente manera: Dos líneas serán utilizadas como líneas externas o líneas de salida y las otras dos restantes como líneas de entrada, debido a que se requiere tener un número en particular para que funcione como Fax se utilizará una línea de salida para convertirla en entrada.

**Modo de programación.** Una vez conectado el teléfono principal a la central telefónica se procede a cambiar el modo del teléfono al modo de programación cambiando el switch de memoria de Set a Program e ingresamos la clave, digitamos *, # e ingresamos la contraseña por default es 1234.

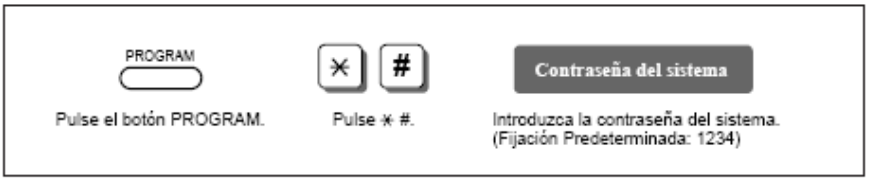



**Figura. 5.20. Iniciar programación.**

Después de entrar en el modo de programación se realiza los siguientes pasos para configurar cualquier función de la central telefónica.


**Figura. 5.21. Configuración definida.**

Al finalizar, salimos del modo de programación volviendo el switch de memoria de Program a Set.

A continuación se detalla las funciones que fueron configuradas para este proyecto:

**Función [008] Asignación de Operador.** Esta función asigna un número de toma de extensión para el operador.

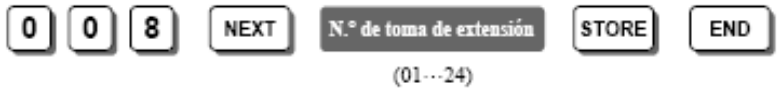



**Figura. 5.22. Asignación Operador.**

**Función [009] Asignación de Número de Extensión.** Selecciona un plan de numeración de extensiones, Plan 1, Plan 2 o Plan 3, y asigna un número de extensión a cada extensión.

**Plan 1**: Los números de extensión disponibles van del 100 al 199.

**Plan 2**: Los números de extensión disponibles van del 100 al 499.

**Plan 3**: Los números de extensión disponibles van del 10 al 49.

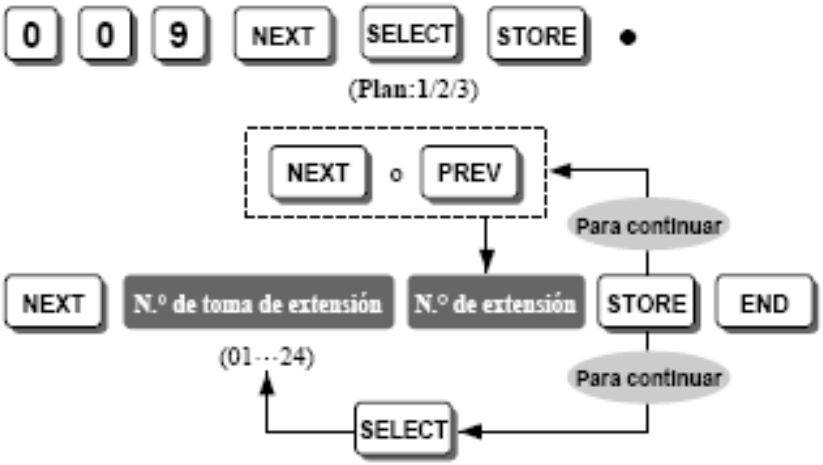



**Figura. 5.23. Números de extensión.**

Para este proyecto se escogió el Plan 1 el cual se distribuirá de la siguiente manera:

| | |
|---|---|
| 101 | Operadora o Recepción. |
| 102 | Fax. |
| 103 | Almacén. |
| 104 | Ventas (Cubículo 1). |
| 105 | Contabilidad (Cubículo 2). |
| 106 | Administración (Cubículo 3). |
| 107 | Ventas1 (Cubículo4). |

| | |
|---|---|
| 109 | Sala de Juntas. |
| 110 | Gerencia. |
| 111 | Presidencia. |
| 112 | Soporte. |
| 113 | Cuarto de Servidores. |

**Tabla 5.10. Ubicación de extensiones.**

**[100] Fijación del Grupo de Exploración.** Activa o desactiva la localización automática de una extensión libre en el mismo grupo de extensiones que la extensión marcada, cuando la extensión llamada está ocupada. Si se selecciona "Activar", asignar el siguiente programa [101] "Tipo de Exploración". Los grupos de extensiones se definen en el programa [600] "Asignación de Grupo de Extensiones".

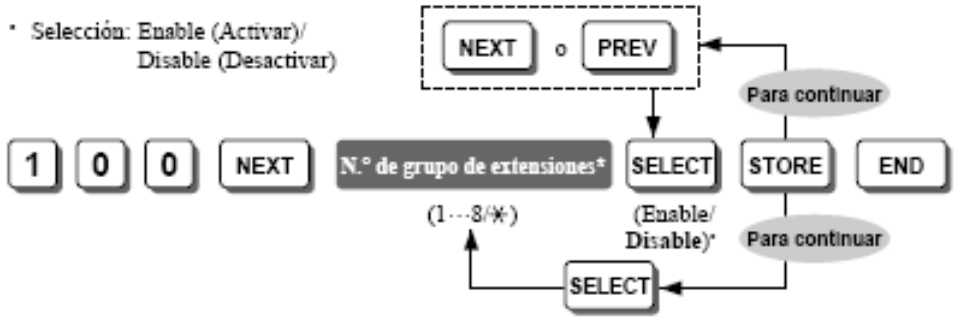



**Figura. 5.24. Grupo de exploración.**

Para este proyecto en esta función se selecciona la extensión 101 la cual es la operadora ya que cuando una extensión esté ocupada envié esa llamada a la operadora o recepción.

**[111] Selección de Música en Retención.** Selecciona la fuente de música, **Interna**, **Externa** o **Tono**, que un usuario exterior escuchará cuando una llamada exterior esté en retención.

**External (Externa):** Se utiliza una fuente de música exterior, tal como una radio.

**Internal (Interna):** Se utiliza una fuente de música equipada con el sistema.

**Tone (Tono):** Utiliza el tono cíclico de abajo equipado con el sistema.

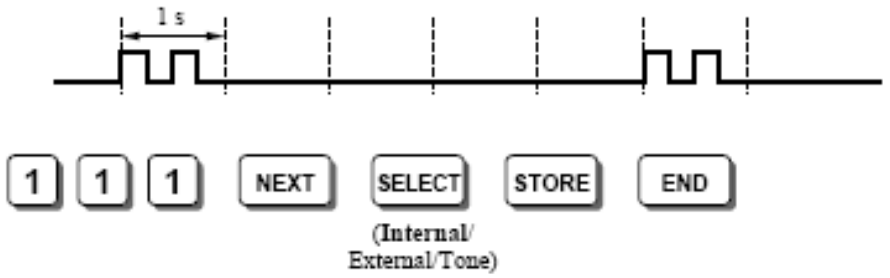



**Figura. 5.25. Selección música.**

Para este proyecto se toma la fuente Interna que proviene de la misma central telefónica.

**[115] Selección de Patrón de Timbre de Extensión.** Selecciona el patrón de timbre de una extensión cuando se recibe una llamada interna:

**Único**, **Doble** o **Triple**.

- Selección: Single (Único)/Double (Doble)/Triple (Triple)

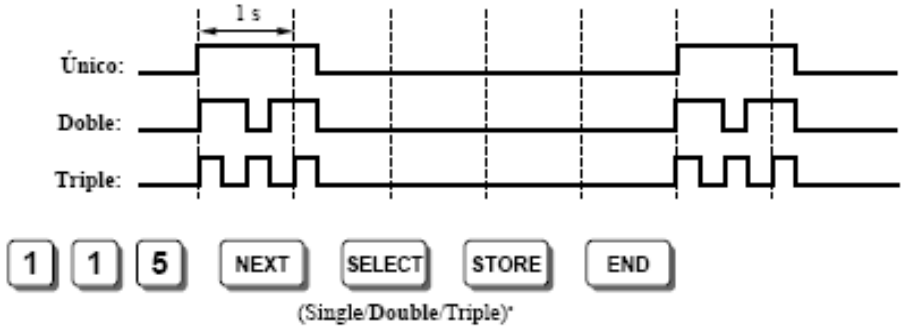



**Figura. 5.26. Selección de timbre.**

En este caso se opta por la opción Doble para diferenciar de las llamadas entrantes.

**[121] Selección de Número de Acceso Automático a Línea Exterior.** Selecciona el Número de Acceso Automático a Línea Exterior (LN) (0 a 9).

- Selección: Dial 0 (Marcar 0)/Dial 9 (Marcar 9)


**Figura. 5.27. Acceso a línea externa.**

Para esta función se escoge 9 para que el usuario que desee llamar al exterior deba digitar en primera instancia 9.

**[122] Rotación Automática para el Acceso a Línea Exterior.** Activa o desactiva la rotación de las líneas exteriores tomadas para el "Acceso Automático a Línea Exterior.

- Selección: Enable (Activar)/Disable (Desactivar)


**Figura. 5.28. Rotación automática.**

En esta función se opta por la opción Habilitar ya que cuando un usuario quiera tener una línea de salida la central telefónica rotará por todas las líneas de salida y así se encontrará una línea desocupada para su uso.

**[127] Fijación de Grupo de Captura.** Activa o desactiva la habilidad que tiene una extensión para capturar una llamada que suena en otra extensión simplemente descolgando la bocina. Si se activa, el número de función (40) no será necesario para capturar la llamada.

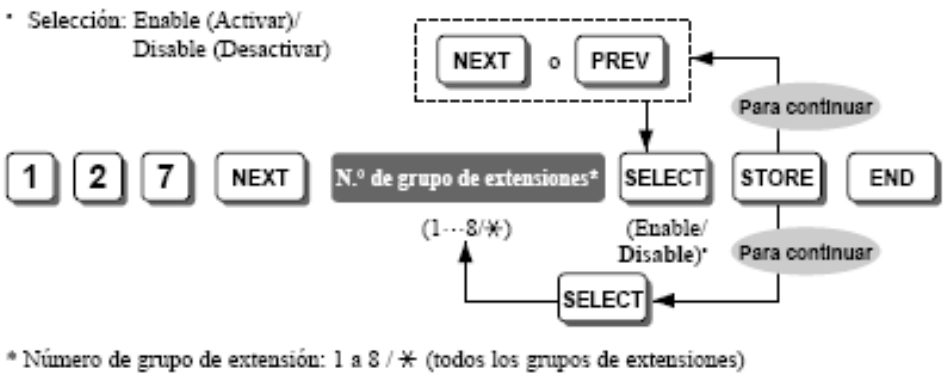



**Figura. 5.29. Grupo de captura.**

Para esta función se selecciona * el cual indica todas las extensiones y la deshabilitamos para que el usuario pueda coger una llamada de otra extensión descolgando y digitando 40.

**[400] Asignación de Conexión de Línea Exterior.** Asigna qué línea(s) exterior(es) va(n) a ser conectada(s) al sistema.

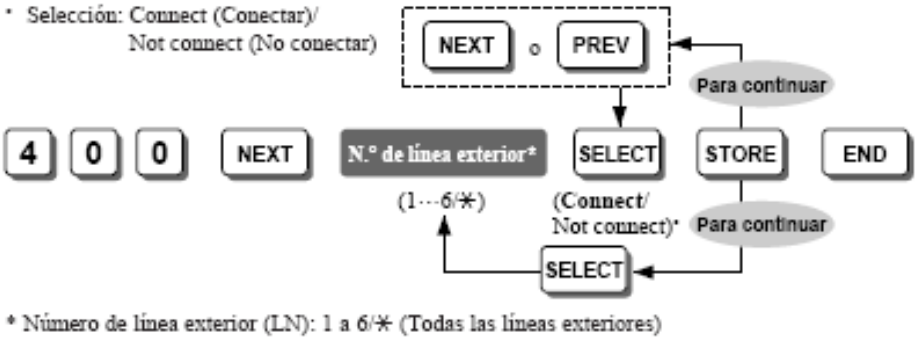



**Figura. 5.30. Conexión línea exterior.**

En esta función se escogen las líneas 4 y 5 a las cuales llegan las líneas que van hacer utilizadas para salir al exterior.

**[408]-[410] Asignación de Timbre Flexible — Día/Noche/Almuerzo.** Determina qué extensión(es) va(n) a sonar para las llamadas exteriores entrantes en los modos de día, noche y/o almuerzo.

- Selección: Enable (Activar)/Disable (Desactivar)

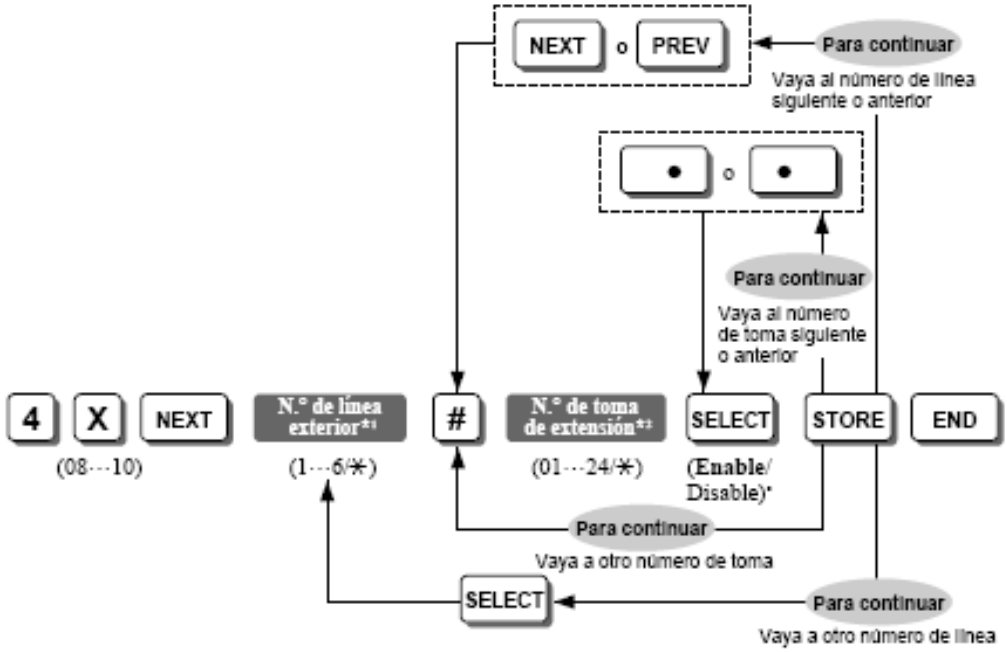



**Figura. 5.31. Habilitar timbre en extensiones.**

X – Número de selección de dirección de programa: 08 ([408] para día)/09 ([409] para noche)/10 ([410] para almuerzo).

Esta función resulta útil debido a que se debe asignar una línea para el Fax y cuando una línea externa ingrese sonará únicamente la extensión seleccionada en este caso 102- Fax.

**[414]-[416] Modo de Línea Exterior— Día/Noche/Almuerzo.** Selecciona el modo de una llamada exterior entrante en cada línea exterior en los modos de día, noche y almuerzo. Existen los cinco siguientes modos:

**Normal:** Se recibirá una llamada exterior entrante en la(s) extensión(es) asignada(s) en los programas [408]-[410] “Asignación de Timbre Flexible — Día/Noche/Almuerzo”.

**DIL:** Se recibirá una llamada exterior entrante en la extensión asignada en este programa.

**DISA1:** Se recibirá una llamada exterior entrante en una extensión a través de la función DISA. Una persona que llama oirá un tono o un mensaje saliente.

**DISA2:** Mediante la función DISA se recibirá una llamada exterior entrante en una extensión. El usuario que llama puede escuchar el OGM 2.

**UCD:** Se recibirá una llamada exterior entrante en una extensión a través de la función UCD.

X – Número de selección de dirección de programa: 14 ([414] para día)/15 ([415] para noche)/16 ([416] para almuerzo).

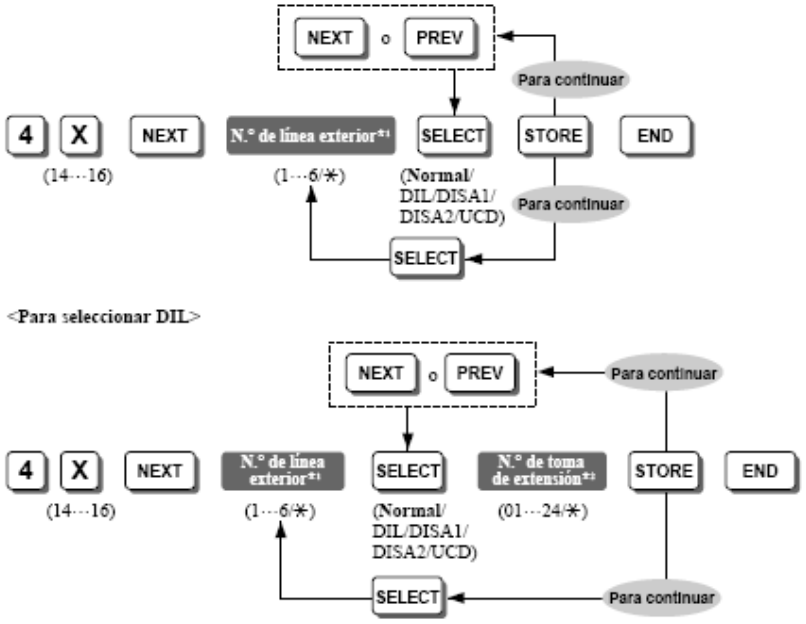



**Figura. 5.32. Acceso de exterior.**

Para esta función se opta por las líneas exteriores 1 y 2 las cuales se las utilizará para que usuarios que llamen puedan utilizar dos líneas en caso de que una se encuentre ocupada y seleccionamos DISA1 para que estos usuarios escuchen un mensaje explicando a que extensión pueden comunicarse digitando un número específico.

**[419] Acceso Automático a Línea Exterior Designada.** Selecciona qué línea exterior puede ser tomada automáticamente cuando el usuario de una extensión marca el número de Acceso Automático a Línea (0 ó 9) asignado en el programa [121] “Selección de Número de Acceso Automático a Línea Exterior”.

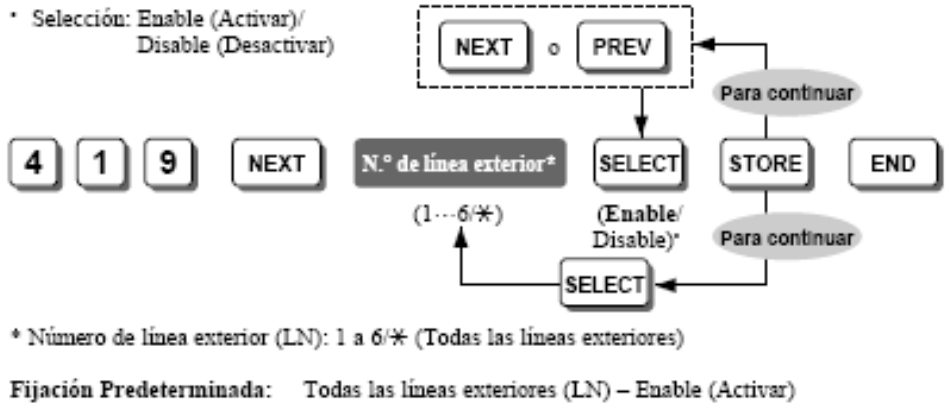



**Figura. 5.33. Asignación de líneas externas.**

Para este caso se escogen las líneas que fueron asignadas como líneas salientes anteriormente que son las líneas 4 y 5. Cuando el usuario digite 9 el cual sirve para buscar una línea externa la central telefónica irá a estas dos líneas que fueron asignadas como líneas externas.

**[500] Selección de Modo de Marcado Entrante DISA.** Selecciona el destino de una llamada exterior entrante mediante la función DISA cuando se selecciona “DISA 1” o “DISA 2” en los programas [414]-[416] “Modo de Línea Exterior (LN) - Día/Noche/Almuerzo”, Sin AA (asistencia automática) o con AA. Si selecciona “Con AA”, asigne el siguiente programa [501] “Asistencia Automática Incorporada DISA”.

**Without AA (Sin AA):** Los destinos disponibles son: números de extensiones asignados en el programa [009] “Asignación de Número de Extensión”, números de acceso a línea (0 o 9, 81 a 86) y el número del operador (0 ó 9).

**With AA (Con AA):** Los destinos disponibles son: números disponibles en el modo “Sin AA”, y números (0 a 9) asignados en el programa [501].

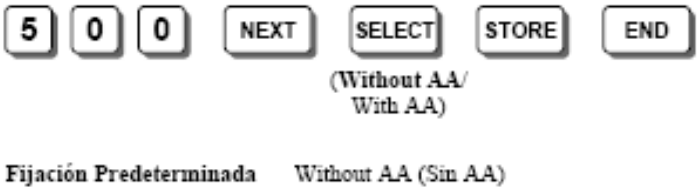



**Figura. 5.34. Modo de marcado entrante.**

Para esta función se selecciona Con AA para que el usuario que escuche el mensaje de entrada (OGM) deba marcar solo un número envés de una extensión de tres números, esto resulta útil para cuando se da el mensaje de entrada ejemplo: Seleccione 1 si desea ir a Gerencia, 2 Ventas, etc.

**[501] Asistencia Automática Incorporada DISA.** Asigna un máximo de 10 números de asistencia automática incorporada DISA cuando se selecciona "Con AA" en el programa [500] "Selección de Modo de Marcado Entrante DISA". El número de extensión asignado en el programa [009] "Asignación de Número de Extensión" y los números de grupos de extensiones asignados en el programa [600] "Asignación de Grupo de Extensiones" pueden asignarse como un número de 1 dígito y ser utilizados como números de asistencia automática incorporada DISA.

- Selección: Jack (Toma)/GRP (Grupo)/Not Stored (No almacenado)

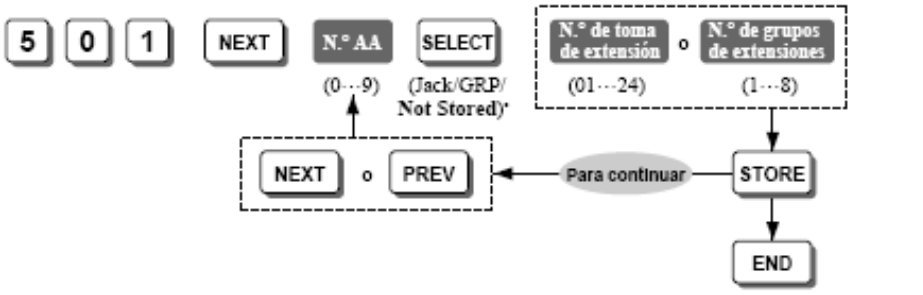



**Figura. 5.35. Asistencia DISA.**

**[502] Selección de Modo OGM.** Selecciona cómo se utilizan los 2 mensajes salientes (OGM1 y OGM2), **MODO1** a **MODO6**.

- Selección: MODE 1/2/3/4/5/6 (MODO 1/2/3/4/5/6)

| Modo | OGM1 | OGM2 | Descripción |
|---|---|---|---|
| 1 | DISA1 | DISA2 | El sistema puede recibir 2 llamadas entrantes al mismo tiempo mediante la función DISA. Esto es muy útil cuando se reciben muchas llamadas. |
| 2 | DISA1 | DISA2 | Un ejemplo: DISA1 se utiliza en el modo de día y DISA2 en el modo de noche. |
| 3 | UCD | UCD | El sistema, mediante la función UCD, puede retener 2 llamadas entrantes al mismo tiempo |

| | | | |
|---|---|---|---|
| | | | hasta que queda disponible cualquier extensión. |
| 4 | UCD | UCD-END | El sistema desconecta una llamada entrante mediante la función UCD cuando termina el tiempo de espera asignado en [521] "Tiempo de Espera en Ocupado UCD". |
| 5 | UCD | DISA1 | Un ejemplo: UCD se utiliza en el modo de día y DISA1 en el modo de noche. |
| 6 | UCD | DISA | El sistema conduce una llamada entrante, por medio de la función UCD, hacia la función DISA mediante OGM2 cuando expira el tiempo de espera asignado en [521] "Tiempo de Espera en Ocupado UCD" y se selecciona "Interceptación" en [523] "Modo de Ocupado UCD". |

**Tabla 5.11. Modos OGM.**


**Figura. 5.36. Selección modo OGM.**

Finalmente, en esta función se toma la opción MODO 1, de este modo dos líneas entrantes al mismo tiempo escucharán el mismo mensaje de entrada (OGM).

## 5.7. PRUEBAS

Se realizaron varias pruebas antes y después de realizar las redes antes mencionadas, en el caso de la Red Inalámbrica se realizaron diversas pruebas, primeramente se debía encontrar el lugar ideal del concentrador inalámbrico para que este pueda llegar con su señal a los sitios deseados, por ende se escogió en primera instancia un sitio central seguido de enganchar una portátil con acceso inalámbrico al concentrador y comprobar que exista señal en los lugares deseados haciendo un ping a la IP si la señal se pierde quiere decir que el lugar del concentrador es incorrecto.

Una vez encontrado el sitio ideal se procedió a verificar la potencia de la señal, velocidad y otras señales con sus respectivos canales, esto se lo pudo hacer mediante varios programas por ejemplo NetStumbler o mediante Conexiones de Red de Windows, estos instrumentos ayudarán al diseñador de la red a verificar la calidad de la señal además de verificar si esta no interfiere con otras señales caso contrario se deberá cambiar el canal de

la misma. Terminado de realizar estas pruebas se determina el lugar exacto del concentrador inalámbrico, para este proyecto se concluyó que el lugar adecuado del concentrador es en el cuarto de servidores, previamente se escogió este cuarto en un lugar central para este caso.

Por otra parte, se realizaron pruebas en el desarrollo de la Red Lan, una vez realizado el cableado del mismo se prosiguió a verificar los cables y las uniones de los mismos mediante un Lan Test diseñado para estos casos, este aparato es capaz de verificar las uniones enviando una señal desde cada uno de los cables desde un extremo y hacer que el otro extremo responda a la señal, si la comunicación esta bien se encenderán ocho leds indicando que el cable y las uniones se encuentran listas para ser usadas sin ningún problema. Una vez concluido este test se comprueba la conectividad y velocidad de la conexión mediante Conexiones de red de Windows verificando que la velocidad deseada concuerde.

Finalmente se realizaron pruebas con las conexiones VPN, OWA, clientes MAPI y central telefónica realizando varias conexiones verificando el acceso, permisos y la conexión de la misma a varias horas, se concluyó que todas las conexiones y permisos eran los correctos siendo aprobados por el Gerente de la empresa.

# CAPÍTULO VI

# CONCLUSIONES Y RECOMENDACIONES

- Para la construcción de redes bien diseñadas es necesario seguir normas y protocolos, de esta manera se garantiza el óptimo funcionamiento de las redes construidas.
- En la construcción de las redes es necesario la ayuda de varias herramientas para verificar su correcto funcionamiento, por ejemplo en la construcción de la red LAN es necesario un Lan Tester para comprobar que las conexiones sean correctas lo que dará lugar una buena comunicación, otro ejemplo de estas herramientas se puede apreciar en la construcción de la red WLAN, en la cual es necesario ciertas herramientas para verificar otras señales en la misma área, canales de transmisión de otras señales y potencia de la señal, existen varias herramientas para verificar estos datos, uno de ellos es un software llamado NetStumbler el cual verifica los datos antes mencionados.
- Es necesaria una correcta configuración de la central telefónica para que la empresa sea más eficiente y eficaz por ejemplo cuando los usuarios externos llamen a la empresa podrán escoger de entre varias opciones para comunicarse con un departamento específico sin necesidad de comunicarse con la operadora.
- Se recomienda en futuro actualizar la Red Telefónica a una Red de Voz sobre IP debido a que todos los programas para la administración de la red ya se encuentran trabajando con esta tecnología, un ejemplo notorio es el servicio de correo electrónico mediante el software Exchange Server 2007 el cual trabaja con telefonía IP para recibir mensajes tanto de texto como de voz, de esta manera cuando el usuario se encuentre fuera de la oficina podrá recibir sus correos y llamadas no contestadas desde cualquier lugar del mundo.
- Una ventaja importante de tener una red VPN es la comunicación total con la empresa sin importar el lugar que se encuentre el usuario, añadiendo a esto la telefonía IP los usuarios que posean teléfono móvil IP podrá ser localizado en

cualquier lugar y el podrá comunicarse con la empresa utilizando únicamente su conexión a Internet o una línea telefónica.

- Es muy importante tener control sobre ciertas actividades de los usuarios, por ende es necesario utilizar un Firewall el cual controle la seguridad de las redes, publicaciones seguras de los servidores, correcto flujo de correo hacia y fuera de la red, etc.
- Mediante una correcta configuración del Firewall se puede acceder a varios beneficios adicionales del mismo es tal el caso de los clientes MAPI, los cuales pueden acceder al correo seguro mediante HTTPS sin intervención del usuarios cuándo el dispositivo móvil o equipo de escritorio detecte una conexión a Internet.
- En la selección de los equipos es muy importante tomar el aspecto económico además de las características de los quipos, ya que de esto depende la aprobación del proyecto o futuros proyectos, otro punto importante en esta selección es conocer los equipos que se encuentran en el mercado para reducir la lista de selección de materiales.
- Se recomienda una vez implementadas las redes conocer la satisfacción del cliente y de esta manera llegar a la conclusión que se realizó un buen trabajo, en este proyecto la satisfacción del cliente fue total, al punto de que los servicios serán tomados en cuenta para futuros proyectos.
- Se recomienda realizar pruebas en horas pico para conocer el porcentaje máximo del uso de la red y así verificar si la red funciona correctamente o se satura.
- En la construcción de las redes, existían varios equipos que tenían problemas en la conexión de red debido a que utilizaban sistemas operativos diferentes, es tal el caso de Windows Vista ya que no existen drivers para algunas tarjetas de red o su funcionamiento no es aceptable, esto provoca inconvenientes económicos y de tiempo por lo que se recomienda migrar la mayoría de máquinas a un solo sistema operativo.
- Se recomienda actualizar o aplicar parches a todo tipo de software probando previamente en una red virtual.

# REFERENCIAS BIBLIOGRÁFICAS

HOLME, Dan y THOMAS, Orin, *Managing and Maintaining a Microsoft Windows Server 2003 Enviroment*, McGraw- Hill / Interamericana de España S.A.U., 61, 102, 211.

MICROSOFT, *2824B Implementing Microsoft Internet Security and Acceleration Server 2004*, 5-13, 5-26, 5-50, 6-32, 6-43, 6-54, 7-10.

MACKLIN, J.C. y MCLEAN, Ian, *Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*, McGraw- Hill / Interamericana de España S.A.U., 470, 485, 602.

PANASONIC, Telecomunicaciones, *Sistemas Híbridos Avanzados*, Teknos Chile S.A., 6, 13.

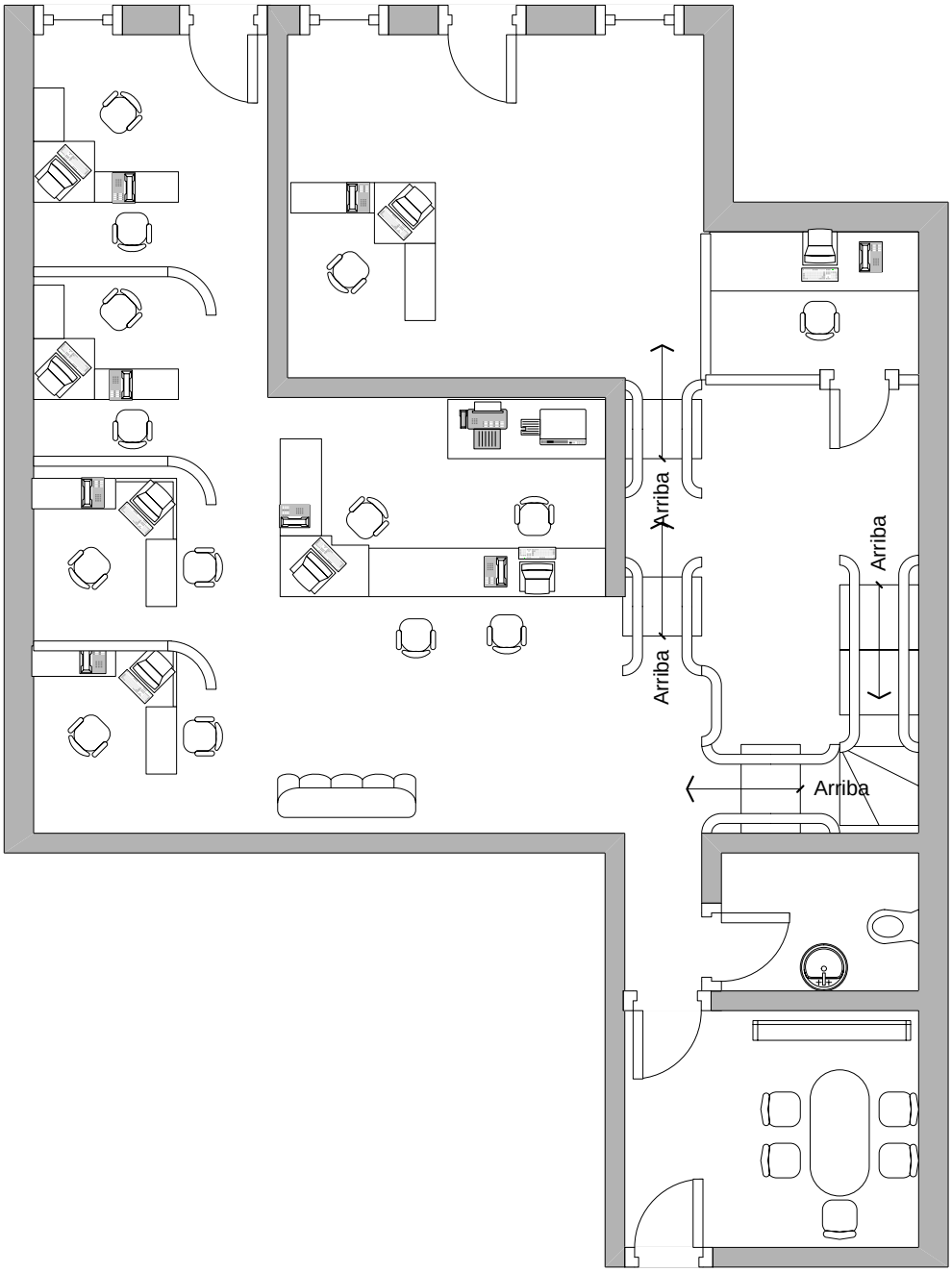
http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas.shtml, Las Redes Informáticas.

http://www.monografias.com/trabajos43/seguridad-redes/seguridad-redes.shtml, Seguridad en Redes de Computadoras.

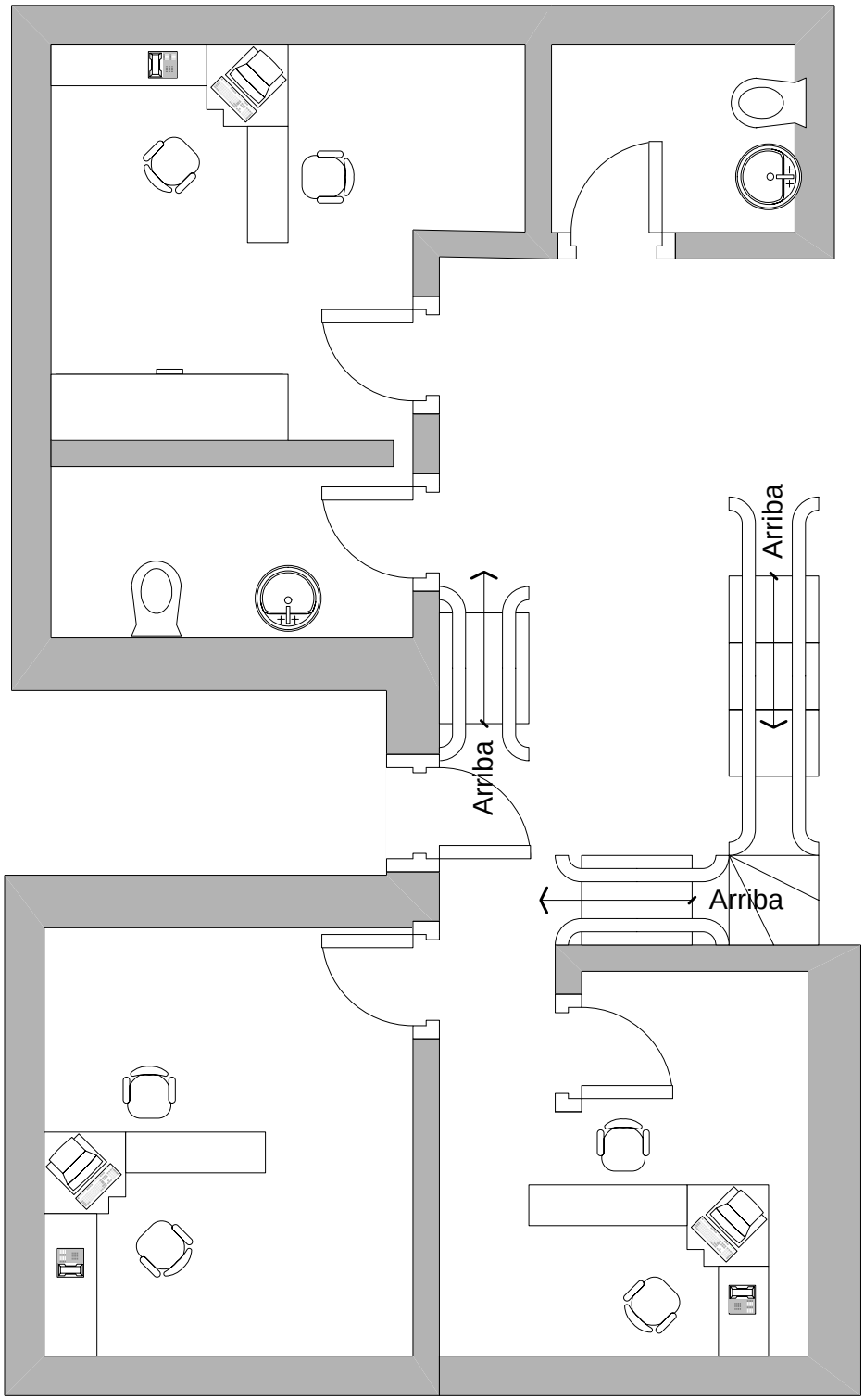
http://www.microsoft.com/spain/isaserver/prodinfo/whatis.mspx, ¿Qué es ISA Server 2006?.

# ANEXOS

## ANEXO 1.- INFRAESTRUCTURA DE INGELSI CIA. LTDA. PLANTA BAJA.


Arriba
Arriba
Arriba
Arriba

## ANEXO 2.- INFRAESTRUCTURA DE INGELSI CIA. LTDA. PLANTA ALTA.


Arriba
Arriba
Arriba

# ÍNDICE FIGURAS

# ÍNDICE TABLAS

# GLOSARIO

## A

**Ancho de Banda**

Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps). Una buena analogía es una autopista. Mientras más carriles tenga la calle, mayor cantidad de tráfico podrá transitar a mayores velocidades. El ancho de banda es un concepto muy parecido. Es la cantidad de información que puede transmitirse en una conexión durante una unidad de tiempo elegida.

**Antivirus**

Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

## B

**Backbone**

La parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región.

**Backup**

Copia de Respaldo o Seguridad. Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

**Bit**

Dígito Binario. Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1 (falso o verdadero respectivamente).

**Byte**

Conjunto de 8 bit, el cual suele representar un valor asignado a un carácter.

## C

**Cableado**

Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

**Cache**

Copia que mantiene una computadora de las páginas Web visitadas últimamente, de forma que si el usuario vuelve a solicitarlas, las mismas son leídas desde el disco duro sin necesidad de tener que conectarse de nuevo a la red; consiguiéndose así una mejora muy apreciable en la velocidad.

**Certificado Digital**

Acreditación emitida por una entidad o un particular debidamente autorizado garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone.

**Click**

Cuando se oprime alguno de lo botones de un mouse el sonido es parecido a un "click". La palabra click escrita, se usa generalmente para indicarle al usuario que oprima el botón del mouse encima de un área de la pantalla. También es comúnmente escrito así: clic. En español incluso se usa como un verbo, por ejemplo: al clickear en el enlace.

**Computación**

Es la ciencia que estudia el procesamiento automático de datos o información por medio de las computadoras.

**Computadora**

Dispositivo electrónico capaz de procesar información y ejecutar instrucciones de los programas. Una computadora (Hispanoamérica) u ordenador (España) es capaz de interpretar y ejecutar comandos programados para entrada, salida, cómputo y operaciones lógicas.

**Conexión Remota**

Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.

**Contraseña**

Password. Código utilizado para acceder a un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

**CPU**

De las siglas en inglés Central Processing Unit (Unidad Central de Procesos) -- Es la parte que constituye el cerebro de cualquier computadora, es el encargado de realizar y dirigir todas las sus funciones. Contiene memoria interna, la unidad aritmética / lógica. Realiza el procesamiento de los datos y además el control de las funciones del resto de los componentes de la computadora. Gobierna el sistema y dicta la velocidad de trabajo del mismo. Existen diferentes tipos de CPU, por ejemplo, los CPU de la familia 8086 de Intel: 80286, 80386, 80486 y Pentium, o de la marca AMD.

# D

**Descomprimir**

Acción de desempaquetar uno o más archivos que anteriormente han sido empaquetados, y habitualmente también comprimidos, en un solo archivo, con objeto de que ocupen menos espacio en disco y se precise menos tiempo para enviarlos por la red.

**Desencriptación/ Descifrado**

Recuperación del contenido real de una información previamente cifrada.

**Directorio Activo**

El Directorio Activo (Active Directory) es el servicio de directorio incluido en Windows 2000 Server y posterior. Extiende las características de las versiones anteriores de los El Directorio Activo, es un servicio de directorio patentado por Microsoft, que se encuentra integrado en la arquitectura de Windows 2000 Server y posterior. Es similar a otros servicios de directorio, como el de Novell (NDS). Es un sistema centralizado que automatiza en la red la gestión de los datos de usuario, seguridad, y recursos distribuidos; también permite la interacción con otros directorios. El Directorio Activo está diseñado especialmente para entornos de red distribuidos.

**Disco duro**

Disco de metal cubierto con una superficie de grabación magnética. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

**DNS**

Servidor de Nombres de Dominio. Servidor automatizado utilizado en el Internet cuya tares es convertir nombres fáciles de entender (como www.panamacom.com) a direcciones numéricas de IP.

**Dominio**

Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Los más comunes son .com, .edu, .net, .org y .gov; la mayoría de los países tienen su propio dominio, y en la actualidad se están ofreciendo muchos dominios nuevos debido a la saturación de los dominios .com (utilizados muchas por empresas).

**Duplex**

Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/ transmitir cualquier tipo de información. Existen dos modalidades HALF-DUPLEX cuando puede recibir y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

## E

**e-mail**

El e-mail, de las palabras inglesas electronic mail (correo electrónico), es uno de los medios de comunicación de más rápido crecimiento en la historia de la humanidad y más usados en Internet. Por medio del protocolo de comunicación TCP/IP, permite el intercambio de mensajes entre las personas conectadas a la red de manera similar al correo tradicional. Para ello es necesario disponer de una dirección de correo electrónico, compuesta por el nombre del usuario, la arroba "@" y el nombre del servidor de correo. Por ejemplo, sample@panamacom.com, donde 'sample' es el usuario y panamacom.com el nombre del host o servidor. El e-mail esta conformado por los siguientes encabezados principales:

**Encriptación**

Cifrado. Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

**Ethernet**

Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa.

**Extranet**

Cuando una intranet tiene partes públicas, en donde posiblemente usuarios externos al intranet pueden llenar formularios que forman parte de procesos internos del intranet.

## F

**Filtro**

En referencia a e-mails, los filtros son creados por los usuarios y contienen reglas para distribuir e-mails dentro de carpetas, reenviarlos o eliminarlos, entre otras.

**Firewall**

Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

**Firma Digital**

Información cifrada que identifica al autor de un documento electrónico y autentifica su identidad.

**FQDN**

En inglés, Fully Qualified Domain Name. Nombre de Dominio Totalmente Calificado. Nombre completo de un sistema y no solo el nombre del sistema.

**FTP**

File Transfer Protocol. Protocolo de transferencia de archivos. Se usan programas clientes para FTP como son por ej. (para Windows) LeapFTP o Core FTP con soporte para ssl, por mencionar algunos. Se usan programas servidores de FTP como por ej. NcFTPd. Estos programas permiten la conexión entre dos computadoras, usando por lo general el puerto 21 para conectarse (aunque se puede usar otros puertos). Por medio del Protocolo de transferencia de archivos se pueden realizar upload y download de archivos entre el cliente y el host (servidor).

## G

**Gateway**

El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles. Gateway o pasarela es un dispositivo, con frecuencia un ordenador, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un gateway de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

**Gigabit**

No debe ser confundido con Gigabyte. Un gigabit es igual a 10^9 (1,000,000,000) bits, que equivalen a 125 megabytes decimales.

**Gigabyte**

El gigabyte (GB) equivale a 1.024 millones de bytes, o 1024 Megabytes. Se usa comúnmente para describir el espacio disponible en un medio de almacenamiento.

**Gusano**

Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron

definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Comunications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1988 y se propagó por sí solo a más de 6.000 sistemas a lo largo de Internet.

## H

**HTML**

Siglas en Inglés de Hypertext Markup Language (Lenguaje de Marcado Hipertexto). Es usada para crear los documentos de hipertexto para uso en el WWW. El HTML es un código, donde usted rodea un bloque de texto con los códigos que indican cómo debe aparecer, además, en HTML usted puede especificar que un bloque del texto, o una palabra, este ligado a otro archivo en el Internet. Los archivos del HTML pueden ser vistos usando un programa cliente de World Wide Web, tal como Netscape, IExplorer o Mosaic.

**HTTP**

En inglés Hypertext Transfer Protocol. Protocolo de Transferencia de Hipertexto. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia. HTTP ha sido usado por los servidores World Wide Web desde su inicio en 1993.

**HTTPS**

Creado por Netscape Comunications Corporation para designar documentos que llegan desde un servidor Web seguro. Esta seguridad es dada por el protocolo SSL (Secure Socket Layer) basado en la tecnología de encriptación y autenticación desarrollada por RSA Data Security Inc.

**Hub**

El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

# I

**ICANN**

Internet Corporation for Assigned Names and Numbers (ICANN) es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión [o administración] del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), así como de la administración del sistema de servidores raíz. Aunque en un principio estos servicios los desempeñaba Internet Assigned Numbers Authority (IANA) y otras entidades bajo contrato con el gobierno de EE.UU., actualmente son responsabilidad de ICANN.

**IDE**

Integrated/Intelligent Drive Electronics. Es una especificación ATA. Es la interface de disco mas común para discos duros, CD ROMS, etc. Es fácil de usar, pero también tiene muchas limitaciones. El IDE esta integrado a la tarjeta madre. El adaptador del computador central controla hasta dos unidades IDE, pero los adaptadores avanzados y los adaptadores IDE ampliados controlan hasta cuatro, máximo. Una alternativa es SCSI, que es más rápido, más complicado y permite conectar más unidades.

**IIS**

Microsoft Internet Information Services. Servicios de Información de Internet de Microsoft. IIS es un conjunto de servicios basados en Internet, para maquinas con Windows. Originalmente se proporcionaba como opcional en Windows NT, pero posteriormente fue integrado a Windows 2000 y Windows Server 2003. Incluye servidores para FTP, SMTP, NNTP y HTTP/HTTPS. Compite con Apache en el area de servidores Web.

**Intel**

El fabricante líder de microprocesadores para PC. Los procesadores Intel fueron usados en las primeras computadoras que incorporaban el sistema operativo DOS de Microsoft. Su línea de procesadores Pentium incremento los niveles de desempeño de las computadoras a niveles superiores. Intel también fabrica tarjetas madre (motherboards),

procesadores de red y un sin fin de circuitos procesadores que están pavimentando el futuro de la computación personal. Ver también Ley de Moore.

**Interfaz (Interface)**

Zona de contacto o conexión entre dos componentes de "hardware"; entre dos aplicaciones; o entre un usuario y una aplicación. Apariencia externa de una aplicación informática.

**Interfaz Gráfica de Usuario**

En inglés Graphic User Interface, corto como GUI. Componente de una aplicación informática que el usuario visualiza y a través de la cual opera con ella. Está formada por ventanas, botones, menús e iconos, entre otros elementos. Ejemplo, Windows y X Windows.

**Internet**

Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo. El Internet empezó en 1962 como una red para los militares llamada ARPANet, para que en sus comunicaciones no existan “puntos de falla”. Con el tiempo fue creciendo hasta convertirse en lo que es hoy en día, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo e-mails, WWW, etc. que usen TCP/IP.

**Internet Explorer**

Conocido también como IE es el browser Web de Microsoft, creado en 1995 para Windows y mucho después para Mac. No fue el primero en el mercado y Netscape le sacó la delantera por muchos años, pero la penetración de Windows en el mercado es muy fuerte. Microsoft empezó a distribuir Windows junto con IE. Poco a poco las personas simplemente preferían usar lo que venía en la computadora a tener que descargar una aplicación de gran tamaño como era Netscape. En la actualidad navegadores como Firefox están ganando terreno.

**Intranet**

Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menús con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras. Es como si fuera un sitio Web dentro de la empresa. Al usar los browser de Internet como Internet Explorer, Firefox o Safari el intranet se convierte en multiplataforma. No importa la marca o sistema operativo de las computadoras dentro de la red, todos se pueden comunicar.

**IP**

Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10

**ISP**

Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

**IT**

Del ingles Information Technology (Tecnología de Información). Término muy general que se refiere al campo entero de la tecnología informática - que incluye hardware de computadoras y programación hasta administración de redes. La mayoría de las empresas medianas y grandes tienen departamentos de IT (TI en español).

**J**

**JPEG, JPG**

Los datos de una imagen pueden ser grabados en diferentes formatos. El jpg es, sin duda, el formato más popular. Su gran ventaja es ser un formato comprimido, lo que le permite ocupar poquísimo espacio en la memoria de la cámara o ser enviado con rapidez por Internet. Su inconveniente es que esta compresión se hace simplificando la

información gráfica de la imagen tanto de color como de detalle. Si la compresión es muy alta la degradación en la calidad de la imagen se hace evidente a simple vista. Si la compresión es baja solo se apreciará con grandes ampliaciones. Además, cada vez que se guarda la imagen se reprocesa y recomprime, con la consiguiente acumulación de degradaciones. A pesar de todo es el formato más utilizado

## K

**Kbps**

Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación, como la velocidad de un cable modem por ejemplo.

**Kilobit**

Su abreviatura es Kb. Aproximadamente mil bits (exactamente 1024). Se usa generalmente para referirse a velocidades de transmisión de datos.

**Kilobyte**

Unidad de medida equivalente a 1024 (dos elevado a la 10) bytes. Se usa frecuentemente para referirse a la capacidad de almacenamiento o tamaño de un archivo.

## L

**LAN**

Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones. Por ejemplo, computadoras conectadas en una oficina, en un edificio o en varios. Se pueden optimizarse los protocolos de señal de la red hasta alcanzar velocidades de transmisión de 100 Mbps.

**Laptop**

Computadora portátil que pesa aproximadamente dos o tres kilogramos. Existen distintos modelos, desde las notebooks comunes hasta las multimedia (dotadas de parlantes, lectora de CD-ROMs, monitor color, etc.). Según su capacidad, tienen una autonomía de corriente eléctrica de dos a seis horas de duración. A raíz de que la tecnología compacta es bastante cara, estos equipos suelen costar prácticamente el doble que sus pares de escritorio, comparando sistemas de capacidades equivalentes.

**Last mile**

Se refiere al último tramo de una línea de comunicación (línea telefónica o cable óptico) que da el servicio al usuario. Es el más costoso.

**Línea Dedicada**

Línea privada que se utiliza para conectar redes de área local de tamaño moderado a un proveedor de servicios de Internet y se caracteriza por ser una conexión permanente.

**Linux**

Versión de libre distribución del sistema operativo UNIX el cual tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitasking (multi tarea), memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP.

**Lista de Correo**

Mailing List. Listado de direcciones electrónicas utilizado para distribuir mensajes a un grupo de personas y generalmente se utiliza para discutir acerca de un determinado tema. Una lista de distribución puede ser abierta o cerrada y puede tener o no un moderador. Si es abierta significa que cualquiera puede suscribirse a ella; si tiene un moderador los mensajes enviados a la lista por cualquier suscriptor pasan primero por aquel, quien decidirá si distribuirlos o no a los demás suscriptores.

**Login**

Clave de acceso que se le asigna a un usuario con el propósito de que pueda utilizar los recursos de una computadora. El login define al usuario y lo identifica dentro de Internet junto con la dirección electrónica de la computadora que utiliza.

# M

**Mail**

Programa en ambiente UNIX para la edición lectura y respuesta de e-mails.

**Malware**

Cualquier programa cuyo objetivo sea causar daños a computadoras, sistemas o redes y, por extensión, a sus usuarios.

**Mbps**

Megabits por Segundo. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación donde cada megabit está formado por 1.048.576 bits.

**Megabyte**

El Megabyte (MB) equivale a un millón de bytes, o mil kilobytes (exactamente 1,048,576 bytes).

**Mensajería Instantánea**

Instant Messaging (IM), en inglés. Sistema de intercambio de mensajes escritos en tiempo real a través de la red. Se usan programas como ICQ, Trillian o MSN Messenger, por mencionar algunos.

**Messenger**

Programa de mensajería instantánea de la empresa Microsoft.

**MHz**

Unidad de frecuencia que equivale a un millón de ciclos por segundo.

**Microprocesador**

Microchip. Circuito integrado en un soporte de silicón el cual está formado por transistores y otros elementos electrónicos miniaturizados. Es uno de los elementos esenciales de una computadora. Ver Pentium o AMD.

**Microsoft**

Compañía creadora de los sistemas operativos Windows 95, 98, NT, 2000, XP; de los controles Active X, y del navegador IE de WWW entre otros recursos. Fundado por Bill Gates. www.microsoft.com

**Modelo Cliente-Servidor**

Sistema que se apoya en terminales (clientes) conectadas a una computadora que los provee de un recurso (servidor). De esta manera los clientes son los elementos que necesitan servicios del recurso y el servidor es la entidad que lo posee. Los clientes, sin embargo, no dependen totalmente del servidor debido a que pueden realizar los procesamientos para desplegar la información (por ejemplo en forma gráfica). El servidor los provee únicamente de la información sin hacerse cargo de otros procesos de forma que el tráfico en la red se ve aligerado y las comunicaciones entre las computadoras se realizan más rápido.

**Módem**

Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una ISDN, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información). La velocidad máxima que puede alcanzar un módem para línea telefónica es de 33 kBps, sin embargo los más comerciales actualmente son los de 28 kBps. Un módem debe cumplir con los estándares de MNP5 y V42.bis para considerar su adquisición. Los módems pueden ser en internos (los que se colocan en una ranura de la computadora) y en externos (que se conectan a un puerto serial de la computadora).

**MS-DOS**

Sistema operativo DOS, de Microsoft. Su entorno es de texto, tipo consola, y no gráfico. Sigue siendo parte importante de los sistemas operativos gráficos de Windows.

**Multidifusión**

Método de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y, por lo tanto, por múltiples usuarios.

## N

**Navegando la red**

Explorar el Internet en busca de información.

**Networking**

Término utilizado para referirse a las redes de telecomunicaciones en general.

**NIC**

Siglas de Network Information Center (Centro de Información de la Red) -- El NIC (Network Information Center) es la autoridad que delega los nombres de dominio a quienes los solicitan. Cada país en el mundo (o propiamente dicho cada Top-Level Domain o TLD) cuenta con una autoridad que registra los nombres bajo su jurisdicción. Por autoridad no nos referimos a una dependencia de un gobierno, muchos NIC´s en el mundo son operados por universidades o compañías privadas. En otras palabras, el NIC es quien se encarga de registrar los dominios de un país.

## O

**Octeto**

Término utilizado para referirse a los ocho bits que conforman un byte. No obstante, este término se usa a veces en vez de byte en la terminología de redes porque algunos sistemas tienen bytes que no están formados por 8 bits.

**OSI**

Interconexión de Sistemas Abiertos (Open Systems Interconnect). Es el protocolo en el que se apoya Internet. Establece la manera como se realiza la comunicación entre dos computadoras a través de siete capas: Física, Datos, Red, Transporte, Sesión, Presentación y Aplicación.

# P

**Página Web**

Resultado en hipertexto o hipermedia que proporciona un navegador del WWW después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. Algunas veces el citado término es utilizado incorrectamente en orden de designar el contenido global de un sitio Web, cuando en ese caso debería decirse "Web site".

**Paquete**

Un paquete es un pedazo de información enviada a través de la red. La unidad de datos que se envía a través de una red la cual se compone de un conjunto de bits que viajan juntos. En Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino.

**Par Trenzado**

Dispositivo parecido al cable telefónico el cual contiene una mayor cantidad de cables. Es el medio físico por el cual pueden conectarse varias computadoras.

**Pentium**

Microprocesador de 64 bits, sucesor del chip 80468, de la empresa Intel. Lo llamaron así puesto que la corte Norteamericana no aceptó 586 o 80586 como marca registrada. Fue lanzado al mercado en 1993. Al pasar los años, Pentium ha evolucionado a P1, P2, P3 y P4, P4EE.

**Periféricos**

Aparatos o equipos electrónicos, (como impresoras, teclados, escaners, etc), adicionales a una computadora (formada por memoria principal y CPU); se usa habitualmente para definir a los elementos que se conectan externamente a un puerto de la computadora.

**Phishing**

"Phishing" (pronunciado como "fishing", "pescar" en inglés) se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros. El correo electrónico comúnmente es utilizado como una herramienta de "phishing" debido a su bajo costo, mayor anonimato para quien lo envía, la habilidad de alcanzar instantáneamente a un grupo grande de usuarios, y el potencial de solicitar una respuesta inmediata. Sin embargo, los estafadores también han usado ventanas "pop-up", correo directo y llamadas telefónicas. Este tipo de correos electrónicos generalmente parecen provenir de instituciones financieras, compañías de seguros o minoristas legítimos. Técnicas tales como una dirección "De" o "From" falsa, el uso de logos aparentemente auténticos de instituciones financieras, o gráficos y ligas a sitios, suelen ser usados para engañar a los clientes y hacerles creer que están tratando con un pedido legítimo acerca de su información personal. Estos correos electrónicos fraudulentos usualmente crean un falso sentido de urgencia destinado a provocar que el destinatario tome una acción inmediata; por ejemplo, frecuentemente invitan a los destinatarios a validar o actualizar información de su cuenta, o a llevar a cabo una cancelación.

**PING**

Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. Lo que se está haciendo en realidad es mandar paquetes a donde se le indique y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras informaciones. Entre sus usos más comunes: resolver el nombre de host para saber su IP o simplemente verificar si una máquina está prendida. Un "ping" sin respuesta no necesariamente significa que la computadora no existe o esta apagada. Si el host o ip al cual se le hace ping tiene un firewall que no permite las respuestas al protocolo ICMP, entonces el "ping" no puede proporcionarnos información. En una ventana de MS-DOS o Unix/Linux, uso del comando: ping "*nombre del host*", por ejemplo: ping panamacom.com.

**Postmaster**

Administrador de Correos. Persona responsable de solucionar problemas en el correo electrónico, responder a preguntas sobre usuarios así como otros asuntos de una determinada instalación.

**Protocolo**

Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

**Protocolo Punto a Punto (PPP)**

Implementación del protocolo TCP/IP por líneas seriales (como en el caso del módem). Es más reciente y complejo que SLIP.

**Proxy**

Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada. También se le conoce como servidor cache.

**Puerto**

Número que aparece tras un nombre de dominio en una URL. Dicho número va precedido del signo (dos puntos). Canal de entrada/salida de una computadora.

## R

**Rack**

El Rack es un armario que ayuda a tener organizado todo el sistema informático de una empresa. Posee unos soportes para conectar los equipos con una separación estándar de 19". Debe estar provisto de ventiladores y extractores de aire, además de conexiones

adecuadas de corriente. Hay modelos abiertos que sólo tienen los soportes con la separación de 19" y otros más costosos cerrados y con puerta panorámica para supervisar el funcionamiento de los equipos activos y el estado de las conexiones. También existen otros modelos que son para sujetar en la pared, estos no son de gran tamaño.

**Raid**

Array Independent Disk. RAID es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante. Ofrece mayor tolerancia a fallos y más altos niveles de rendimiento que un sólo disco duro o un grupo de discos duros independientes.

**Raíz (Root)**

Directorio inicial de un sistema de archivos mientras que en entornos UNIX también se refiere al usuario principal.

**RAM**

Random Access Memory (memoria de acceso aleatorio). Por lo general el término RAM es comprendido generalmente como la memoria volátil (los datos e instrucciones se borran al apagarse la PC) que puede ser escrita y leída. La memoria del equipo permite almacenar datos de entrada, instrucciones de los programas que se están ejecutando en ese momento, los datos resultados del procesamiento y los datos que se preparan para la salida.

**Ratón**

(Mouse) Dispositivo electrónico de pequeño tamaño operable con la mano y mediante el cual se puede dar instrucciones la computadora, para que lleve a cabo una determinada acción.

**Red**

Network en inglés. Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

**Red de Acceso**

Conjunto de elementos que permiten conectar a cada abonado con la central local de la que es dependiente.

**Red Inalámbrica**

Red que no utiliza como medio físico el cableado sino el aire y generalmente utiliza microondas o rayos infrarrojos.

**Red Privada Virtual**

Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

**RJ45**

Es uno de los dos tipos de conectores usados en las computadoras, emplea un cable y un conector muy similares a los del teléfono, donde cada PC tiene su propio cable y todos ellos pueden unirse a un HUB. En caso de dañarse uno de los cables o conectores, este equipo quedará desconectado de los otros pero la red sigue funcionando con normalidad.

**ROM**

Read Only Memory (memoria de solo lectura). en la cual se almacena ciertos programas e información que necesita la computadora las cuales están grabadas permanentemente y no pueden ser cambiadas por el programador (puede ser leído pero no modificado). Las instrucciones básicas para arrancar una computadora están grabadas aquí y en algunas notebooks han grabado hojas de cálculo, basic, etc.

**Router**

Un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino. El router esta conectado por lo menos a dos redes, y determina hacia que lado enviar el paquete de data dependiendo en el entendimiento del router sobre las redes que esta conectado. Los routers crean o mantienen una "tabla" de rutas disponibles, y usa esta información para darle la mejor ruta a un paquete, en un determinado momento.

# S

**Sector de arranque**

Parte de un disco reservada para el bootstrap loader de un sistema operativo, un pequeño programa en lenguaje de máquina que reside en la ROM y que se ejecuta automáticamente cuando la PC es reiniciada o apagada, después de algunas pruebas básicas de hardware el programa llama a otros programas mayores que a su vez llaman al sistema operativo.

**Servidor**

Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes). También puede referirse a un software específico, como lo es el servidor WWW. Una computadora puede tener distintos software de servidor, proporcionando muchos servidores a clientes en la red. Por ejemplo, las computadoras que contienen sitios Web se llaman servidores ya que “sirven” recursos de Web para aplicaciones cliente como los navegadores o browsers.

**Servidor de Correo**

Un servidor de correo (mail server) es la computadora donde se ejecuta un programa de gestión de emails, como por ejemplo Sendmail, Qmail y Microsoft Exchange.

**Servidor de Noticias**

Servidor de Internet cuya misión es distribuir los grupos de noticias.

**Servidor Seguro**

Tipo especial de servidor diseñado con el propósito de dificultar, en la mayor medida posible, el acceso de personas no autorizadas a la información en él contenida. Se destaca que un tipo de servidor seguro especialmente protegido es el utilizado en las transacciones de comercio electrónico.

**Servidor Web**

Un servidor Web es el programa, y la computadora que lo corre, que maneja los dominios y páginas Web, interpretando lenguajes como html y php, entre otros.

**Sesión Remota**

Uso de los recursos de una computadora desde una terminal la cual no se encuentra cercana a dicha computadora.

**Sistema Operativo**

Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

**SMTP**

Protocolo Simple de Transferencia de Correo. Es definido en STD 10, RFC 821, y se usa para la transferencia de correo electrónico entre computadoras. Es un protocolo de servidor a servidor, de forma que para poder leer los mensajes se deben utilizar otros protocolos.

**Software**

Se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

**Software libre**

Programas desarrollados y distribuidos dándole al usuario la libertad de ejecutar, copiar, distribuir, cambiar y mejorar dicho programa (Linux es un ejemplo) mediante su código fuente. El software libre no es siempre software gratuito (equivocación bastante habitual que tiene su origen de la palabra en inglés "free" que significa tanto "libre" como "gratuito").

**Spam**

Envío masivo, indiscriminado y no solicitado de publicidad a través de e-mail.

**Spyware**

Spyware son unos pequeños programas cuyo objetivo es mandar información, generalmente a empresas de mercadeo, del uso de Internet, websites visitados, etc. del usuario, por medio del Internet. Usualmente estas acciones son llevadas a cabo sin el conocimiento del usuario, y consumen ancho de banda, la computadora se pone lenta, etc.

**SQL**

Structured Query Language. Es un lenguaje especializado de programación que permite realizar consultas (queries) a bases de datos. Los orígenes del SQL están ligados a los de las bases de datos relacionales. En 1970 Dr. E.F. Codd, investigador de IBM, propone el modelo relacional y asociado a este un sublenguaje de acceso a los datos basado en el cálculo de predicados. Basándose en estas ideas los laboratorios de IBM definen el lenguaje SEQUEL (Structured English Query Language) que más tarde sería ampliamente implementado por el SGBD experimental System R, desarrollado en 1977 también por IBM. Sin embargo, fue Oracle quien lo introdujo por primera vez en 1979 en un programa comercial. El SEQUEL terminaría siendo el predecesor de SQL. La mayoría de las aplicaciones de bases de datos complejas y muchas otras más pequeñas pueden ser manejadas usando SQL. Es un lenguaje de programación interactivo y estandarizado para extraer información y actualizar una base de datos.

**SSL**

Acrónimo en inglés de Secure Socket Layer. Protocolo creado por Netscape con el fin de hacer posible la transmisión encriptada y por ende segura, de información a través de la red donde sólo el servidor y el cliente podrán entender un determinado texto. Utiliza una llave de 50 hasta 128 bits (más bits, mayor el grado de encriptación de la data). El browser del cliente dictamina el rango. En muchos países está estrictamente regulado los niveles máximos de encriptación permisibles. Por ejemplo en USA permiten el uso de 256 bits para instituciones financieras. Para ilustrar el concepto de SSL, supongamos que tiene en su computadora un virus o backdoor que permite que personas ajenas a usted puedan monitorear lo que se transmite en su conexión por el puerto 80 (www). Esto significa que si usted hace una compra en algún sitio de comercio electrónico, en esencia, la persona(s) que lo este monitoreando podrá robarse su número de tarjeta de

crédito en el momento que usted lo escriba. Pero, aunque su computadora se encuentre en el escenario descrito arriba, un sitio Web que tenga SSL hace que los que están monitoreando su computadora vean “basura” (caracteres ilegibles) en vez de lo que realmente se esta llenando en el formulario del sitio, protegiendo efectivamente su información personal, tarjeta de crédito, etc. Por lo general las páginas Web con SSL empiezan con https en vez de http, tienen un certificado digital, y funcionan en el puerto 443.

## T

**T-1**

Una línea dedicada capaz de transferir datos a 1,544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta un megabyte en menos de 10 segundos. Sin embargo, esto no es lo suficiente rápido para pantallas completas con movimiento general, para las cuales se requiere al menos 10,00,000 bits-por-segundo. Una T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.

**T-3**

Es una conexión a través de una línea conmutada capaz de transmitir datos a 44,736,000 bits por segundo. Esto es más que suficiente para desplegar video en pantalla completa con movimiento continuo.

**Tarjeta Madre**

Motherboard en ingles. Es una tarjeta de circuitos integrados que contiene varios microchips, como lo son normalmente: el microprocesador, circuitos electrónicos de soporte, ranuras para conectar parte o toda la RAM del sistema, la ROM y ranuras especiales (slots) que permiten la conexión de tarjetas adaptadoras adicionales (como por ejemplo, tarjetas de video y de sonido).

**TCP/IP**

El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet. Forma de comunicación básica que usa el Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

**Teclado**

Periférico de entrada utilizado para dar instrucciones y/o datos a la computadora a la que está conectada. Existen distintas disposiciones de teclado, para que se puedan utilizar en diversos idiomas. El tipo estándar de teclado inglés se conoce como QWERTY. El teclado extendido es el que tiene 101 ó 102 teclas. Las primeras computadoras personales tenían un teclado que incorporaba letras, números y signos, con algo más de 80 teclas, a su lado, se incorporó el conjunto de teclas de números, por lo que recibió la nueva denominación.

**Teleconferencia**

Consiste en mantener una conferencia por TV con varias personas a la vez. Se logra mediante cámaras y monitores de videos ubicados en las instalaciones del cliente o en un centro de conferencias público. El video de pantalla completa y de movimiento pleno a 30 cuadros por segundo requiere una red con un gran ancho de banda.

**Telefonía IP**

La señal analógica de la voz es convertida en señal digital que puede transitar por Internet. La calidad del sonido en las redes TCP/IP depende del ancho de banda del que se dispone.

**Terabyte**

Un Terabyte (TB) equivale a algo más de mil billones de bytes, concretamente 1,024 (2^40) o 1024 Gigabytes. Todavía no se han desarrollado memorias de esta capacidad aunque sí dispositivos de almacenamiento.

**Topología de Red**

Se refiere a cómo se establece y se cablea físicamente una red. La elección de la topología afectará la facilidad de la instalación, el costo del cable y la confiabilidad de la red. Existen tres topologías principales de red anillo, bus y estrella. *Topología de Anillo.* Topología en donde las estaciones de trabajo se conectan físicamente en un anillo, terminando el cable en la misma estación de donde se originó. *Topología de bus.* En donde todas las estaciones se conectan a un cable central llamado "bus". Este tipo de topología es fácil de instalar y requiere menos cable que la topología de estrella. *Topología de Estrella.* Topología en donde cada estación se conecta con su propio cable a un dispositivo de conexión central, ya sea a un servidor de archivos o un repetidor.

**Transferencia de Archivos**

Copia de un archivo desde un ordenador a otro a través de una red de computadoras.

**Tunneling**

Tecnología que permite que una red mande su data por medio de las conexiones de otra red. Funciona encapsulando un protocolo de red dentro de los paquetes de la segunda red. Es el acto de encapsular un protocolo de comunicación dentro de otro a través de dispositivos y Routers.

## U

**UNIX**

Sistema operativo especializado en capacidades de multiusuario y multitarea. Fue la base inicial de Internet. Entre sus características más importantes se encuentran: Redireccionamiento de Entrada/Salida. Alta portabilidad al estar escrito en lenguaje C, lo que lo hace independiente del hardware. Interface simple e interactivo con el usuario

Sus componentes básicos son: Kernel Parte del sistema operativo que reside permanentemente en memoria. Dirige los recursos del sistema, memoria, E/S de archivos y procesos. Shell Intérprete de comandos. Interpreta y activa los comandos o utilidades introducidos por el usuario. Es un programa ordinario (ejecutable) cuya

particularidad es que sirve de interface entre el Kernel y el usuario. Es también un lenguaje de programación (similar al C), y como tal permite el usar variables, estructuras sintácticas, entradas/salidas etc.

**URL**

Acrónimo de Uniform Resource Locator. Localizador Uniforme de Recurso. Es el sistema de direcciones en Internet. El modo estándar de escribir la dirección de un sitio específico o parte de una información en el Web. El URL está conformado por a) El protocolo de servicio (http://); b) El nombre de la computadora (www.panamacom.com); y c) El directorio y el archivo referido.

**Usuario**

Persona que tiene una cuenta en una determinada computadora por medio de la cual puede acceder a los recursos y servicios que ofrece una red. Puede ser tanto usuario de correo electrónico como de acceso al servidor en modo terminal. Un usuario que reside en una determinada computadora tiene una dirección única de correo electrónico.

## V

**Vínculo**

Link. Apuntadores hipertexto que sirven para saltar de una información a otra, o de un servidor Web a otro, cuando se navega por Internet.

**Virtual**

Término de frecuente utilización en el mundo de las tecnologías de la información y de las comunicaciones el cual designa dispositivos o funciones simulados.

**Virus**

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente.

b) Tratar de pasar desapercibidos para causar el mayor daño posible.

c) Adueñarse de las funciones principales (infectar los archivos de sistema). Los virus no pueden viajar en mensajes de correo electrónico, ya que únicamente utilizan el formato de 7 bits para transferir texto. La única manera en que pueden viajar es por archivos binarios que se envían mediante un adjunto (attachment) al mensaje de texto (y que el MIME convierte automáticamente). Es recomendable revisar estos archivos con un antivirus antes de su lectura. También existen otros tipos de virus, como por ejemplo el que afecta la función de macros de Word y Excel.

**VoIP**

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways, teléfonos IP y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

## W

**WAN**

(Wide Area Network, Red de Área Amplia). Red de computadoras conectadas entre sí. Usando líneas terrestres o incluso satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

**Web Site**

Conjunto de páginas Web que usualmente comparten un mismo tema e intención.

**Webcam**

Cámara Web. Cámara de video cuyas imágenes, bien en directo bien en diferido, son difundidas por Internet desde un sitio Web.

**Webmail**

Servicio que permite gestionar el correo electrónico desde un sitio Web el cual es de gran utilidad para personas que tienen que desplazarse con frecuencia y lo ofrecen habitualmente los proveedores de acceso a Internet.

**Webmaster**

Administrador de Web - Persona responsable de la gestión y mantenimiento de un servidor Web, principalmente desde el punto de vista técnico; por lo que no debe ser confundido con un editor de Web. Por ejemplo, el webmaster es el que usualmente recibe los emails enviados por el servidor, anunciando errores o cualquier tipo de actividad.

**WiFi**

Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz. Ha ganado aceptación en mucho ambientes como una alternativa viable a los LANs cableados. Muchos hoteles, restaurantes, aeropuertos, etc. ofrecen acceso público a Internet por medio de WiFi. A estos lugares se les conoce como “hotspots”. Se deben tomar las medidas mínimas de seguridad (firewall) en las computadoras con capacidad WiFi, y sobretodo en los routers inalámbricos para proteger el acceso a la red por personas ajenas a la misma. Sin los controles necesarios, cualquier persona cerca al radio de transmisión de su router inalámbrico puede conseguir conexión a Internet, navegar con su ancho de banda e incluso hackear su red privada.

**Windows**

Sistema operativo desarrollado por la empresa Microsoft cuyas diversas versiones (3.1, 95, 98, NT, 2000, XP, ME, etc) han dominado de forma abrumadora el mercado de las computadoras personales, aunque no se puede decir lo mismo del mercado de redes corporativas. Windows proporciona una interfaz estándar basada en menús desplegables, ventanas en pantalla y un dispositivo señalador como el ratón. Los programas deben estar especialmente diseñados para aprovechar estas características. La unión de Windows NT/2000 y la familia de Windows 9.x se alcanzó con Windows XP puesto en venta en 2001 en su versión Home y Professional. Windows XP usa el núcleo

de Windows NT. La futura versión de Windows que sucederá a Windows XP y saldrá a inicios de 2007 para negocios y para el público se llama Windows Vista.

**WLAN**

Acrónimo en inglés para Wireless Local Area Network. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio. Hoy en día puede cubrir áreas desde 20 a 70 metros dentro de edificios y hasta 350 metros afuera. Este sistema de transmisión inalámbrica permite velocidades de hasta 3 a 4 Mbps. WLAN es un término genérico para referirse a una Red inalámbrica de área local, mientras que WiFi se refiere al set de estándares para la Red inalámbrica de área local.

**Word**

Programa de la empresa Microsoft, parte del paquete de software "Office". Word es un procesador de palabras que permite la elaboración de documentos. Existe una versión gratuita de un programa similar a Microsoft Office, que es compatible con Word, Excel y PowerPoint, creado por la empresa SUN.

**World Wide Web**

Comúnmente conocido como WWW. Es el sistema de información basado en hipertexto, cuya función es buscar y tener acceso a documentos a través de la red de forma que un usuario pueda acceder usando un navegador Web. Creada a principios de los años 90 por Tim Berners-Lee, investigador en el CERN, Suiza. La información transmitida por el www puede ser de cualquier formato (texto, gráfico, audio y video).

**XML**

Extensible Markup Language. Lenguaje Extensible de Marcado. Lenguaje desarrollado por el W3 Consortium para permitir la descripción de información contenida en el WWW a través de estándares y formatos comunes, de manera que tanto los usuarios de Internet como programas específicos (agentes) puedan buscar, comparar y compartir información en la red. El formato de XML es muy parecido al del HTML aunque no es una extensión ni un componente de éste.

# FECHA DE ENTREGA Y PIE DE FIRMAS

Sangolquí……..:……

**Elaborado por:**

_____

Acero Palácios Ricardo Vladimir

**Coordinador De Carrera**

_____

Ing. Gonzalo Olmedo