UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"ARAGÓN"

"TEMAS SELECTOS SOBRE SEGURIDAD EN REDES DE ORDENADORES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

INGENIERO MECÁNICO ELECTRICISTA
(ÁREA ELÉCTRICA - ELECTRÓNICA)

P R E S E N T A :

RAMÓN PATIÑO RODRÍGUEZ

ASESOR:
ING. ADRIÁN PAREDES ROMERO

MÉXICO 2003

A

Agradecimientos:

A mi familia que ha sido una parte muy fundamental, los pilares en el desarrollo de mi vida y de mi desarrollo académico, no tengo con que agradecerles todo su cariño. Los llevo siempre en mi corazón:

Silvia:
Gracias por todo tu amor, tus desvelos, palabras de apoyo, motivaciones, sufrimientos, no tengo las palabras necesarias para poder decir todo lo que quisiera expresarte pues para mi eres lo máximo, por eso y por tu cariño muchas gracias mamá.

Ramón:
Al ingeniero que tengo en casa aunque no haya podido tener la oportunidad de haber cursado un estudio profesional, la persona a la cual admiro infinitamente por todo lo que me enseña día a día, por su creatividad su cariño, apoyo y su infinito amor de Padre.

Virginia:
Mi hermana del alma, te admiro mucho, por tu apoyo mil gracias por que siempre le has motivado y por ser un ejemplo para mi

Ricardo:
No sabes lo importante que has sido para mí, un gran ejemplo, aparte de tener la dicha de ser tu hermano, has sido mi brazo derecho y por tu apoyo te estoy eternamente agradecido.

Lidia:
Durante el tiempo que tenemos de convivir, me has enseñado mucho por tus palabras, apoyo y ejemplo y te lo agradezco de corazón, eres una gran persona.

A mi familia en general, por que siempre me han dado palabras de aliento para seguir adelante, a todos los aprecio mucho, siempre están en mi corazón..

Padrino Eduardo, Emmanuel, infinitamente agradecido por su apoyo desinteresado.

A mi asesor Adrián Paredes Romero por que me ha brindado su apoyo incondicional, una gran persona que he tenido la dicha de conocer.

Ing. Juan Gastaldi, una persona importante que siempre me ha brindado apoyo consejos, y que siempre esta dispuesto a escuchar y dar su punto de vista.

A mis Sinodales Ing. José Luis, Ing. David Moisés, Ing. Sergio Galicia y a todos los profesores (ingeniería, diseño industrial) que me han dado palabras de aliento, apoyo, ayuda, consejos, que desafortunadamente no puedo escribir el nombre de cada uno por espacio y por que me dolería dejar alguno fuera, solo me resta darles las gracias.

A mis profesores de educación básica y secundaria: Socorro (q.d.p), Efrén, Alicia, Martha, Leticia, y de mas profesores que se me llegan a escapar.

Y a los no menos importantes y si grandes personas que llevo en el corazón, mis amigos de formación escolar: Paty, Rubér., Víctor, Damaris, Mónica, Wendy, Dante, Armando, Juan Carlos, Pedro, Juan, Martha, Susana, Julio, Enrique, Dulce, Ericka, David, Judith, Angélica, Eva, Claudia, Chio, Isabel, David, Alexis, y tantos y tantos más que se me escapan pero que saben que son fundamentales en mi vida y que siempre los tengo presentes en mi mente y corazón. A ellos y a sus admirables familias, por el infinito aprecio que les tengo gracias.

INDICE.

C

INTRODUCCIÓN.

En el transcurso de la Historia, la evolución del ser humano siempre ha venido a la par con el desarrollo tecnológico, desde sus orígenes en la época prehistórica cuando accidentalmente observaron que una piedra golpeada por otra le daba un filo haciéndola una herramienta practica y rápida para sus actividades de la vida diaria, o en la caza para matar a sus presas con lanzas, en el corte de la piel y la carne de los animales, entre otras cosas.

Así el Hombre con las experiencia vividas y en base a las experiencias de otros, fue cómo poco a poco el desarrollo de elementos, herramientas y maquinaria fueron surgiendo, modificándose y perfeccionándose, poniéndose en práctica y así, creciendo a pasos agigantados desde las últimas décadas hasta nuestros días

La fusión de los Ordenadores y las Comunicaciones, ha tenido una profunda influencia en la forma en que estos Sistemas están organizados. El concepto de *"Centro de Cómputo"* como un cuarto con un Ordenador grande, al cual los Usuarios llevaban sus trabajos para su procesamiento, ha llegado a ser obsoleto.

Este modelo no tenía uno, sino al menos dos aspectos deficientes: Primero, el concepto de un sólo Ordenador grande haciendo todo el trabajo y, segundo, la idea de que los Usuarios lleven su trabajo a dónde se encuentra el Ordenador en lugar de llevar el Ordenador a dónde se encuentren los Usuarios (Beltrao, 1998).

El "viejo modelo" de tener un sólo Ordenador para satisfacer todas las necesidades de cálculo de una Organización, se está reemplazando con rapidez por otro que considera un número grande de Ordenadores separados, pero interconectadas, que efectúen el mismo trabajo. Estos *"Sistemas"*, se conocen como "Redes de Ordenadores".

La necesidad de mantener comunicados los diversos Departamentos existentes dentro de una misma Empresa ha impulsado a los conocedores del mundo de la Informática a buscar nuevas alternativas que den respuestas concretas.

Los Sistemas de Redes Locales de Ordenadores, han dado solución a muchos de los problemas a los que venían enfrentando quienes tenían a su cargo la responsabilidad del manejo de la Información generada dentro de las Empresas y han venido ganando terreno, y adquiriendo una importancia tal que han llegado a ser considerados como el medio más moderno y eficiente para la captación, administración, control e intercambio de datos; además de que es un Sistema que permite la máxima exploración de los recursos de la Arquitectura de Sistemas *("Hardware")* y de los Programas y Paquetes de Aplicación *("Software")*, con que cuenta una Empresa o Industria.

Otro aspecto importante a considerar, es que un Sistema de Red Local, proporciona a el Usuario mayor seguridad respecto a los datos almacenados ya que el acceso a ella o a los sistemas se lleva a cabo a través de una Clave Personal *("Password")*. Entendiendo ésta como la llave de acceso para la generación de aplicaciones del sistema de una Empresa (altas, bajas, consultas, reportes, etcétera), así lo establece Barlow, (1995).

Estos sistemas de Redes Locales, permiten la comunicación con máquinas de igual o de diferentes características. Lo anterior, significa flexibilidad y rapidez en la transmisión de Información que se tenga que realizar en cualquier momento. Siendo una de las alternativas más aceptadas por los Usuarios, para el manejo de Información que se genere dentro de cualquier Empresa o Industria, además:

- Las Redes Locales, permiten un mejor control e intercambio de Información en, y con el Departamento de Sistemas.

- Las Redes Locales, se consideran como una respuesta a las exigencias de los Usuarios del Departamento de Sistemas.

- Las Redes Locales, son una solución que permite captar, controlar e intercambiar Información en el Departamento de Sistemas.

Los ordenadores son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso de este siglo, el mundo ha sido testigo de la transformación de algunos aspectos de Seguridad y del Derecho. Durante mucho tiempo se consideró que los procedimientos de Auditoria y Seguridad eran responsabilidad de la persona que elabora los sistemas, sin considerar que son responsabilidad del área de Informática, en cuanto a la elaboración de los sistemas del usuario en cuanto a la utilización que se le dé a la información y a la forma de acceder a ella, y del Departamento de Auditoria Interna en cuanto a la supervisión y diseño de los controles necesarios. La seguridad del área de Informática tiene como objetivos:

Proteger la integridad, exactitud y confidencialidad de la información, los activos ante desastres provocados por la mano del hombre y de actos hostiles, a la Organización contra situaciones externas como desastres naturales y sabotajes.

En la actualidad, principalmente en los ordenadores personales, se ha dado otro factor que hay que considerar: el llamado **"Virus Informático"** de los ordenadores, el cual, aunque tiene diferentes intenciones, se encuentra principalmente en paquetes que son copiados sin autorización *("piratas")* y borra toda la información que se tiene en un disco. Además de incluir el surgimiento desmedido de los *hacker's* en los últimos años, y que destruyen la información personal solo con el fin de demostrar que pueden tener acceso a lugares restringidos para ellos, que al estar dentro del sistema de la Red se dedican a destruir, sabotear y robar información que solo para el interesado es de suma importancia.

Otro factor muy importante a esta consideración es que se debe de educar cibernéticamente a los empleados con el fin de que estén concientes que los Ordenadores de La Red de la Compañía son sólo para uso exclusivo a los intereses de la misma, y por consiguiente, no están sujetos a intereses particulares. Así pues, la Red estará segura en forma general tanto por los sistemas de seguridad *(software)* como con el uso adecuado de las Instalaciones de la Compañía.

CAPÍTULO I.

GENERALIDADES SOBRE REDES DE ORDENADORES.

Debido a las necesidades que ha tenido el ser humano por almacenar información impresa, los engorrosos papeleos con el conocido problema de trasladarlos y de llevarlos hacia otros lugares distantes para que esta información llegue a su destino final con la(s) persona(s) correspondiente(s), llevaba mucho tiempo, dinero y esfuerzo. Con el objetivo de reducir tiempos en estas actividades, distintas personas se dedicaron a desarrollar algo con que cubrir esas necesidades y después de tantas experimentaciones fue como surgieron los primeros ordenadores.

Estos ordenadores comenzaron con ciertas limitantes al inicio, pero con esta herramienta ya se comenzaron a cubrir y eliminar el almacenamiento de cientos y cientos de documentos, pero aún el resguardo de la información era en tarjetas perforadas que inevitablemente seguía siendo una problemática para la compañía, pues continuaba con el inconveniente de trasladar ahora las tarjetas perforadas de un departamento a otro, con el mismo inconveniente y una nueva necesidad de crear algo que permitiera cubrir esa problemática, y que la información fuera directamente al ordenador principal y que hubiera un medio de intercomunicación entre el usuario y el ordenador.

Con el surgimiento de las terminales en los años 60 se elimina el traslado de la información y todos los datos son enviados directamente a la unidad de proceso central donde se continuaba con el procesamiento de la misma reduciendo tiempos de operación, traslado y procesamiento ya que directamente al ser capturados los datos por el usuario, éstos inmediatamente se mandaban a la unidad central, pero cuanto más crecían las necesidades de la compañía, más crecía la utilización de terminales y periféricos que se interconectaban al ordenador principal, lo que provoco un inconveniente en la reducción de velocidad de respuesta; ya que sus prestaciones de comunicación llegaban al límite de operación.

Con el auge comercial que tuvieron los ordenadores en sus inicios surgieron varios fabricantes lo que dio una ventaja en el consumo de este elemento (recurso), ya que basándose en sus características y capacidades aunado a las necesidades de la compañía se adquiría la que más se adecuara y cubriera sus prioridades, este requisito era fundamental; por consiguiente, cada persona podía comprar a uno o a otro fabricante, esto dio pauta para que este producto tuviera un auge tecnológico poco tiempo después de su surgimiento.

En el transcurso de las décadas de los años 70 y 80, surgió primero el desarrollo de la electrónica a pequeña escala, dando origen entre otras cosas a desarrollar elementos electrónicos de pequeñas dimensiones, y entre esos aparatos electrónicos dio paso también a la reducción de los ordenadores, pasando a ser microordenadores.

Así con la nueva característica de estas máquinas pequeñas y con mayor capacidad, beneficio a que las compañías tuvieran un microordenador destinado específicamente en cada área correspondiente sin que esto provocara que se interconectaran al ordenador central, y permitiendo que el ordenador principal trabajara a toda su capacidad sin necesidad de utilizar sus recursos para que operaran las terminales y periféricos conectados a él.

Los microordenadores ayudaron enormemente a la captura de información escrita, pero con el inconveniente que ésta se tenía que almacenar en discos flexibles, pues ya no se conectaban al ordenador principal, esto causaba que nuevamente se requiriera de un traslado de un departamento a otro costando tiempo nuevamente, pero con la diferencia de que ahora no eran tarjetas perforadas, si no que el traslado de información se hacía por medio de los discos flexibles, pero en cantidades considerables porque estos discos tenían poca capacidad de almacenamiento.

Posteriormente surgió el disco duro (Hard Disk), en este dispositivo se podía almacenar una gran cantidad de información, donde sus capacidades variaban y se encontraban discos duros desde los 5 Mbytes hasta los 100 Mbytes pero como todo dispositivo que surge y es lanzado al mercado, éste tenía el inconveniente del costo, ya que era muy excesivo y provocaba que fuera incosteable el colocar un disco duro por cada microordenador que se contara en la compañía.

Conforme se inicio el desarrollo ordenadores con mayores cualidades (velocidad, rapidez de repuesta hombre-máquina, reducción física) y del surgimiento del disco duro, fue así como surgió la necesidad de conectar los microordenadores con el ordenador principal que tenía el dispositivo de almacenamiento, esto propicio que se comenzaran a construir redes locales; con esto, el envió y recepción de la información se llevaba a cabo en segundos, aunque solamente se pudieran hacer con los equipos de ordenadores de un solo fabricante, pues si se quería conectar o enlazar un ordenador de una marca distinta a las que ya se contaba en la compañía, esto resultaba ser absolutamente imposible pues cada fabricante de ordenadores le daba su toque especial de comunicación y de programación. Entonces, el traslado de la información era muy rápido, pero surgió un nuevo inconveniente: todos los usuarios tenían un acceso ilimitado a toda la información que estaba almacenada en el disco duro generando un gran riesgo, una gran inseguridad informática y peligro de que se perdiera información importante provocado por descuido o por venganza personal.

Esa heterogeneidad de los sistemas beneficia al usuario, que no está así limitado a un único tipo de sistemas para sus distintas aplicaciones. Así, se puede seleccionar el sistema que mejor se adapte a las condiciones de aplicación que interesen y el presupuesto disponible. Por otro lado, tal heterogeneidad dificulta considerablemente la interconexión de equipos de fabricantes diferentes, según Menascé, (1994).

El primer *"File Server"* fue creado por Novel Inc., con el cual todos los usuarios tenían acceso a la información pero con diferentes grados de acceso, ya que no era el mismo acceso para el personal de informática que para el de los usuarios en general, con este procedimiento se tenía la seguridad de que nadie que no fuera autorizado podía tener acceso y poder generar un daño informativo.

Novel baso su investigación y desarrollo en la idea de que son los *"Programas y Paquetes"* de la Red y no de la *"Arquitectura"* lo que hacía la diferencia en la operación de la Red. Esto se ha podido constatar y en la actualidad Novel soporta más de 20 tipos diferentes de Redes en base a la variedad de sus Sistemas Operativos, (Novel, 1995).

Así fue como por diferentes necesidades y después de mucho investigar, se dio origen a las Redes de Ordenadores de Área Local (Redes LAN) haciendo más eficiente y costeable el trabajo. Con este desarrollo ya se podía tener un intercambio de información segura, el servicio del sistema por consiguiente se volvió más eficiente, pues ahora si se dio fin a un engorroso traslado de información de departamento a departamento y los recursos se podían compartir al 100%.

El principal propósito del surgimiento de las redes de ordenadores es el de agilizar los procesos, el compartir los recursos con que cuenta la red y accesos desde las terminales a impresoras, bases de datos, información digital, etcétera, y que el funcionamiento de ésta sea dentro de las mejores condiciones utilizando protocolos de comunicación y los canales necesarios que se obtienen al configurarla. El autor Green (1992) dice que una Red de Microordenadores es la intercor.exión de Estaciones de Trabajo que permite la comunicación entre ellas y co:mpartir recursos en forma coordinada e integral, aprovechando la base instalada de Ordenadores.

Las ventajas que ofrece este tipo de Red de Ordenadores son las siguientes:

1.- Compartir Hardware y Software.
2.- Intercambiar información.
3.- Respaldar datos.
4.-Tener flexibilidad en el manejo de la información.
5.- Propicia el crecimiento modular (Red esencial).
6.- Facilidad de adquisición pues hay una gran variedad en nuestro país.
7.- Son sistemas que permiten cambiar de recursos sin muchas dificultades.
8.- Servicios de Correo Electrónico y Mensajería.

I.1.- Elementos de una Red.

Según Tanenbaum, (1991) los elementos básicos de una Red de Ordenadores Área Local (LAN)) son:

I.1.1.- La Estación de Trabajo (Ordenadores).
I.1.2.- El Servidor de la Red.
I.1.3.- El Medio de Comunicación.
I.1.4.- Tarjetas de Interfase.
I.1.5.- Sistema Operativo.

I.1.1.- Estación de Trabajo.

Son Microordenadores que utiliza el usuario para Procesar su información. Estos Microordenadores pueden ser de tipo AT, con o sin Disco Duro, el usuario puede hacer uso de los recursos de la estación de trabajo o acceder a la Red LAN para utilizar sus recursos de memoria, impresoras, graficadores y Modems.

I.1.2.- El Servidor de la Red.

Es un microordenador de alto rendimiento que tiene uno o varios discos duros de alta velocidad y capacidad, gran capacidad de memoria, contando también con varios puertos para conectar las demás estaciones de trabajo y periféricos, así como también pueden existir uno o más servidores en la misma Red y su microprocesador puede ser de características mínimas como por ejemplo un Pentium de alta capacidad. Este microordenador ofrece sus recursos a los demás usuarios limitando el uso dependiendo la categoría y nivel de seguridad.

Además el servidor de una Red LAN puede dividirse en Servidor **DEDICADO** y servidor **CENTRALIZADO** o **DISTRIBUIDO.**

Servidor Dedicado. Su función es la de administrar solamente y específicamente administrar los recursos de la Red y controlar el acceso a datos y programas de aplicación restringiendo el grado de utilización de los usuarios de la Red.

Servidor no Dedicado. Es que además de lo antes mencionado, se utiliza también como una Estación de Trabajo de la Red de Ordenadores. Es poco recomendable ya que utilizando el Servidor en modo no dedicado, se hace más lento el funcionamiento de la Red.

Servidor Centralizado. Utilizan una solo Ordenador como Servidor de Archivos, Servidor de Impresoras y Administrador de la Red.

Servidor Distribuido. Las Redes con varias Estaciones de Trabajo, y gran tráfico de información, utilizan como Servidor Distribuido dos o más Ordenadores en donde una se encarga de Administrar el uso de Impresoras, otra para Administrar Archivos y proporcionar Programas de Aplicación y una tercera, para Comunicación con otras Redes o *"Mainframes"*. Una de las ventajas con que se cuenta en las Redes de Ordenadores, es que se puede aumentar la capacidad de almacenamiento con solo agregar más equipos y que la ubicación de éstos, se puede ajustar a la distribución física de los Departamentos de la Empresa que utilice la Red.

I.1.3.- El Medio de Comunicación.

Es la ruta física entre el transmisor y el receptor en la Red, este medio Físico se utiliza para realizar la comunicación y enviar o recibir mensajes de un Ordenador a otro. Son tres los medios de Comunicación para Redes Locales de Ordenadores y son:

- ✓ Cable Trenzado o Telefonico.

Es el medio más utilizado en redes para transmitir señales analógicas y señales digitales, su grosor es de 1mm aproximadamente y el ancho de banda que trabaja depende del grosor del conductor y de la distancia que deba cubrir, la velocidad está en el orden de 10-100 Mbps. Cada cable está compuesto por una serie de pares de cables trenzados. Estos son pares que son trenzados para reducir la interferencia entre pares adjuntos. Por lo regular una serie de pares, son agrupados en una funda de un color para reducir el número de cables físicos que se introducen en un conducto y que por ser de peso ligero proporciona mucha flexibilidad y se convierte en un cable de fácil manejo e instalación, no requiriendo grandes canalizaciones en su trazado.

Por la flexibilidad de sus características su utilización es diversa pudiendo integrar estos servicios: Red de Área Local ISO 8802.3 (Ethernet) y ISO 8802.5 (Token Ring), telefonía analógica y digital, terminales asíncronos, terminales síncronos, líneas de control y alarmas.

Para las señales analógicas se requieren amplificadores casi cada 5 o 6 Km, pero su uso más común es la transmisión de voz, tiene capacidad para más de 24 canales de voz con un ancho de banda mayor a 268 Khz. Para la trasmisión de datos este medio de comunicación soporta frecuencias de trasmisión de datos de más de 100 MHz, sin grado de atenuación considerable.

Existen tres tipos de cable: No apantallado, apantallado y uniforme.

- **UPT** No apantallado (*Unshield Twiested Pair*):

Es el normal y más usado en todas las redes locales por ser el más barato. Lo malo es que trabaja en distancias cortas, consta de 4 pares de hilos que tiene solo una cubierta de protección plástica.

- **SPT** apantallado (*Shield Twiested Pair)*:

El coaxial se recubre con una malla metálica y además una lámina que sirve de pantalla, consta de 2 pares de hilos. Es más caro pero reduce el error por interferencias.

- **FTP** uniforme:

Cada uno de los pares es trenzado uniformemente durante su creación. Esto elimina la mayoría de las interferencias entre cables y además protege al conjunto de los cables de interferencias exteriores. Se realiza un apantallamiento global de todos los pares mediante una lámina externa además de tener la malla metálica tiene en su interior un hilo metálico interno para eliminar inducciones electromagnéticas del cable. Estos cables se encuentran pares en conjuntos por cable son de 2, 3, 4, 6, 12, 16 y 25, 50, 100, 200 y 300 pares. Cuando el número de pares es superior a 4 se habla de cables multípar. (Si son 4 pares entonces hay un total de 8 cables).

Se tienen varios niveles de cable debido al tipo y grado del trenzado.

Categoría:	
1 y 2	Utilizado solamente para la comunicación de voz.
3	Van de 4 en 4 (8 cables), alcanzando 30 Mbps. Se utiliza para la transmisión de voz y datos y trabaja hasta los 10 MHz., se utilizo en el inicio de la Ethernet.
4	Se utiliza en la transmisión de voz/datos y trabaja hasta los 20 MHz. Se utilizo en el inicio de "Token Ring".
5	Más retorcidos y mejor aislante (teflón), este tipo de cable se utiliza para la Fast Ethernet y soporta hasta los 100 MHz.

El par torcido se puede utilizar para aplicaciones punto a punto, o punto a multipunto, para una conexión de multipunto es una gran opción ya que esto

implica menor costo y más fácil de trabajar que un cable coaxial aunque su capacidad de conexión de estaciones de trabajo es reducida y el conectar punto a punto es muy común, para realizar estas conexiones se utilizan los conectores RJ-45 y el RJ-11, su utilización de este medio de comunicación es principalmente cuando las Redes de Ordenadores se encuentran en un mismo edificio. El conector RJ-45 es parecido al conector telefónico pero son más grandes y con 8 entradas para 8 cables. Para unirlos hace falta un instrumento llamado gripadora, que es como unos alicates aunque más complejos que cubren totalmente el conector y que presionan suavemente las cuchillas que hacen contacto con los cables para que este tenga continuidad conector-cable-conector.

Tipo y Numeración del conector RJ45

Entre las ventajas de la utilización del par trenzado es la de fácil instalación, es compatible con diferentes estándares de comunicación como lo son Arcnet, Ethernet, StarLAN, Token Ring, FDI, el ancho de banda con el que trabaja es de hasta 100 Mbps, a relación costo-beneficio es muy aceptable, la distancia máxima que cubre este medio es de 150m para el cable UTP, y 500 m para el cable STP. Aunque hay una tecnología que proporciona buenas características de transmisión y con buena calidad de comunicación, esta es la tecnología **High bit rate Digital Subscriber Line (HDSL)** ya que cuenta con un ancho de banda que puede transmitir hasta 2.084 Mbps de señal digital de buena calidad comparando el costo que implica reparar los desperfectos del medio de transmisión de cobre y de fibra óptica.

En este tipo de medio se pueden realizar los siguientes servicios: video comprimido, video en tiempo real, televisión interactiva, videoconferencia,

acceso al rango primario de la Red Integral de Servicios Integrados (ISDN), interconexiones LAN, líneas privadas E1, entre otras; cubriendo una distancia máxima de 4.8 Km., con una conexión en dos pares de cobre. El implantar este tipo de medio es de bajo costo además de que se cuentan con equipos para esta plataforma por ejemplo se tiene el **E1 HDLS** y el **CAMPUS 384** del fabricante **PAIR GAIN** que incluye unidades modulares remotas y de oficina central, esta última da soporte a más de 16 módulos alojados en un bastidor estándar y la unidad remota tiene más de 4 puertos fraccionarios E1 en G1, V.35 y V.36 sobre de uno a tres pares y cable de cobre de calibre 24/26 AWG.

Conexión Straight Trough

Este tipo de conexión se usa en cables que van a conectar un *"host"* a una red Ethernet 10BaseT. Generalmente, un extremo del cable (terminal A) se conecta al Jack de la tarjeta de red del host, mientras que el otro extremo (terminal B) se conecta a un Concentrador Central, *("HUB")*. Se observa que las conexiones se realizan entre iguales, por lo que el cable de un color determinado se conecta en ambas terminales al mismo terminal del RJ-45. Es una conexión directa.

Conexión Cross-Over

Se utilizan en el caso de cables que deben unir dos host directamente, a través de sus correspondientes tarjetas de red. En este caso, es necesario realizar una inversión de cables en los pines terminales, para que cada cable activo cambie de funcionalidad (emisor o receptor) en cada uno de los Jacks. El esquema de este tipo de cables es el siguiente:

Conexión Roll-Over

También denominada conexión de cable de consola, es la usada en cables de conexión a una terminal de consola de un Ruteador *("Router")*, por ejemplo. En ella, todos los cables van invertidos de posición, como si se reflejaran en un espejo, siendo su esquema el siguiente:

Ventajas:

Su instalación es de bajo costo, de gran confiabilidad, rápida y flexible, su consumo energético es bajo, es compacta, cubre grandes distancias, se utilizan conectores RJ-45 DCE o RS-232, múltiples interfaces de red de datos, indicadores de estado y alarma, se puede realizar la conversión a fibra óptica.

- ✓ Cable Coaxial.

Los había de dos tipos: gruesos **(Thick)** y finos **(Thin)**. Los gruesos se utilizaron al principio en la conexión de Redes Locales de Ordenadores por su velocidad y capacidad, pero se manejaban muy mal, costaban mucho y eran poco operativos. El fino era más barato pero las distancias que cubría eran pequeñas, por lo que había que amplificar después de segmento la señal. Por lo cual, estos tipos de cable están en desuso.

Hay dos tipos de cable coaxial de 50 Ω: Banda base, utilizado en Ethernet, un canal y de 75 Ω banda ancha, utilizado en TV, distintos canales, 300MHz, está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre que servirán para evitar las interferencias. Entre el hilo de cobre y la malla hay una parte de plástico que separa los dos conductores y además todo ello está recubierto de un aislante.

El cable de 75 Ω se utiliza principalmente en sistemas de televisión por cable, se puede utilizar además; para señalización, pero analógica con FDM llamado también Banda Ancha. Las frecuencias para señales analógicas van desde los 300 a 400 MHz, los datos analógicos como video y audio pueden ser transferidos por este medio como las señales de radio y televisión abierta, ya

que los canales de televisión tienen un ancho de banda de 6 MHz, y el ancho de banda del canal de radio es muy pequeño, de esta forma se puede hacer una transmisión de canales considerable por medio del FDM, también puede funcionar este medio con PSK, ASK y FSK.

Para obtener velocidades mayores a los 20 Mbps se aplican dos métodos sin utilizar FDM, el primero es utilizando la señalización digital en el cable logrando una velocidad de 50 Mbps, la otra opción es utilizando modulación PSK y una frecuencia de 150 MHz, logrando una velocidad de 50 Mbps; el cable de 50 Ω se utiliza para señalización digital con FDM conocida también como banda base Es usado para la codificación Manchester, en esta codificacion se obtienen velocidades mayores a 10 Mbps.

Este medio de comunicación se utiliza para conexiones punto a punto y multipunto si se utiliza el cable de 50 Ω, se pueden conectar hasta 100 dispositivos por elemento logrando aumentar el sistema uniendo con repetidores los sistemas, y la distancia que puede cubrir este medio es de unos kilómetros; el cable de 75 Ω soporta infinidad de dispositivos, pero con el inconveniente de que acarrea es cuando se utilizan velocidades de 50 Mbps produce problemas técnicos y su distancia máxima de conexión es de decenas de kilómetros.

Se utiliza el MODEM de RF para interconectar la Red para convertir datos de información señales digitales a analógicas y en forma inversa. Cuando la Red utilizada cubre una distancia considerable, se utilizan amplificadores y acopladores de dirección para confirmar que las señales enviadas por los dispositivos de la Red lleguen al dispositivo de control. La transmisión de alta velocidad de 50 Kbps ya sea digital o analógica, limita la distancia de conexión reduciéndola a solo 1 Km.

En los extremos del cable coaxial se ponen conectores del tipo Neil (N) o BNC para la reducción de ruido y armónicas y su inmunidad depende, del tipo de conexión que se realice siendo éste mucho mejor que el par trenzado cuando es utilizado a altas frecuencias.

Algunos Conectores de Cable BNC.

10BASE5: Cable coaxial grueso, 500 metros, 10Mbps, conector "N".

10BASE2: Cable coaxial fino, 185 metros, 10 Mbps, conector "BNC".
10 BROAD 36: Cable coaxial de banda ancha de 75 Ω, 3600 m, 10 Mbps.

Ventajas:

Su instalación es muy fácil, soporta enormemente las transmisiones de datos, video y voz, es compatible con los estándares de Redes de Datos (Ethernet y Token Ring), no sufre interferencias ambientales, su costo lo hace muy accesible.

- ✓ Fibra Óptica.

Con la búsqueda de un medio que no sufra alteraciones ambientales, maneje más canales de información y que proporcione un ancho de banda que brinde una mayor ventaja entre otras cosas, fue como surgió el desarrollo la fibra óptica.

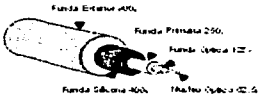
Ésta tiene gran capacidad de transmisión, pues su ancho de banda llega a ser hasta de 30000GHz y la velocidad de transmisión son grandes por ejemplo se puede trabajar entre 1,7 Gbps pero se puede llegar a alcanzar los 39 Gbps; puede transmitir la señal a una distancia de hasta casi 30 Km., y no necesita repetidores ya que la atenuación que se tiene en este medio es muy pequeña, después de esta distancia se necesita conectar repetidores para tener una buena transmisión; es de dimensiones pequeñas que van de 2 a 125 mm, lo que lo hace más ligero y de menor tamaño ya que es más delgado, por lo tanto es más flexible (pesa 8 veces menos que el cable par trenzado) que los otros medios de transmisión, no sufre alteraciones ambientales por electromagnetismo (no recibe interferencias ni de radio ni eléctricas) ya que éste no es un medio metálico; además de que no consume energía eléctrica, no hay disipación de calor, y su transmisión es por medios ópticos.

Este cable está constituido por uno o más hilos de fibra de vidrio. Cada fibra de vidrio consta de:

- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evitando que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo.

Cada una de ellas está rodeada por un revestimiento y reforzada para proteger a la fibra, el último revestimiento más externo está formado por varias capas protectoras contra aplastamiento, la humedad y otros factores externos que pueden afectar considerablemente en su funcionamiento.

Se pueden tener varias clases de vidrio o plástico para crear la fibra óptica, siendo la de plástico la más barata pero con la limitante que no puede cubrir distancias grandes, por lo tanto es más recomendable que se implemente en Redes de Ordenadores donde las distancias son cortas para que las pérdidas no sean considerables.



La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta llevando una señal codificada por toda la longitud del cable de fibra óptica por medio de una modulación intensiva en donde el "1" lógico es un pulso luminoso, y el "0" lógico es la ausencia de luz (el nivel del "0" lógico es un pequeño haz luminoso y para el "1" lógico es con mayor intensidad); se ha observado que el haz de luz tiene menores pérdidas si su longitud de onda está en el rango de 850 nm, 1300 nm, y 1500 nm, y al final del recorrido ésta es recibida por un receptor optico y es convertida en señal eléctrica en la salida del receptor.

Según las tendencias, en poco tiempo todas las empresas que transmiten datos, voz, numéricos, vídeo, etcétera, acabarán utilizando este cable que aunque mucho más caro, es más seguro; la señal no se distorsiona y llega muy lejos sin tener que amplificarla.

Hay tres tipos de fibra óptica:

a) Múltimodo Abrupto:

Las fibras múltimodo de índice escalonado están fabricadas a base de vidrio, con una atenuación de 30 dB/km, o plástico, con una atenuación de 100 dB/km. Tienen una banda de paso que llega hasta los 40 MHz por kilómetro. En estas fibras, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea. El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice, de ahí su nombre de índice escalonado.

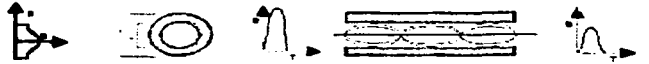
La luz se transmite en varios caminos dependiendo del ángulo en que incida formando varios ángulos en la señal digital por la fibra óptica, produciendo que las señales se reciban desfasadas en su transmisión, denominándose por este motivo fibra múltimodo. Es más barato aunque por la velocidad que maneja provoca que sea muy difícil su transmisión, debido a esto si su velocidad es de 100Mbps se tendrá que utilizar una distancia de 30 m, y si la velocidad fuera de 10 Mbps la distancia que hay que cubrir es de 3 Km.

b) Múltimodo Gradual:

Las fibras múltimodo de índice de gradiente gradual tienen una banda de paso que llega hasta los 500MHz por kilómetro. Su principio se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra, como se puede ver en el dibujo. Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra a una mayor velocidad que con el sistema Múltimodo Abrupto, produciendo que las fases lleguen aproximadas.

La fibra múltimodo de índice de gradiente gradual de tamaño 62,5/125 m (diámetro del núcleo/diámetro de la cubierta) está normalizado, pero se pueden encontrar otros tipos de fibras:

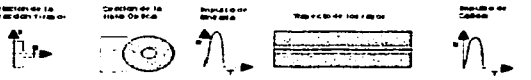
.múltimodo de índice escalonado 100/140 mm.
.múltimodo de índice de gradiente gradual 50/125 mm.



c) Monomodo:

Potencialmente, esta es la fibra que ofrece la mayor capacidad de transporte de información. Tiene una banda de paso del orden de los 100 GHz/km. Los mayores flujos se consiguen con esta fibra, pero también es la más compleja de implantar. El dibujo muestra que solo pueden ser transmitidos los rayos que tienen una trayectoria que sigue el eje de la fibra, por lo que se ha ganado el nombre de "monomodo" (modo de propagación, o camino del haz luminoso, único).

Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten, es decir, de unos 5 a 8 mm. Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Los elevados flujos que se pueden alcanzar constituyen la principal ventaja de las fibras monomodo, ya que sus pequeñas dimensiones implican un manejo delicado y entrañan dificultades de conexión. Utilizando una luz láser para que casi toda la señal llegue a su destino sin atenuaciones, reduciendo el núcleo a 50 micrometros se tiene una velocidad aproximada de 100 Gbps/Km.



En este tipo de transmisión se utilizan dos tipos de emisores luminosos el LED y el ILD

LED (diodo emisor de luz): dispositivo de estado sólido que emite un haz luminoso cuando la corriente aplicada lo polariza, es de costo accesible, tiene una vida de operación muy grande además de operar en un grande rango de temperatura duración.

ILD (diodo de inyeccion láser): la forma de operar de este dispositivo es en base al principio del rayo láser, el cual recibe una estimulación para producir un rayo de una gran intensidad luminosa y de un pequeño ancho de banda provocando que sea muy eficiente con la capacidad de trabajar con señales de transmisión muy alta.

Se utiliza en la actualidad para la transmisión de señal luminosa el LED de longitud de onda de 850 nm., ya que sus características proporcionan tanto buena calidad en la transmisión a una velocidad mayor a los 100 Mbps a unos cuantos kilómetros de distancia además de que es accesible económicamente hablando, se

puede utilizar un LED de 1300 nm., o láser para cubrir distancias y velocidades mayores

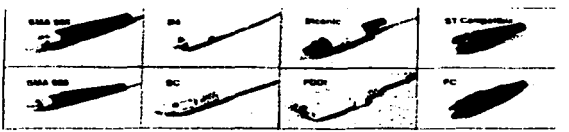
Por consiguiente se utilizan dos dispositivos receptores de señal luminosa:

Fotodiodo APD: es un fotodiodo que tiene un segmento de silicón intrínseco entre las capas P y N del diodo además de ser un diodo avalancha.

Fotodiodo PIN: es un fotodiodo que tiene un segmento de silicón intrínseco entre las capas P y N del diodo.

Ventajas:

- Proporciona un gran ancho de banda.
- Cubre una gran distancia (km) sin tener que usar un amplificador o un repetidor.
- La atenuación de la señal es de solamente 1 dB/Km.
- Aplicaciones de alta velocidad.
- Proporciona la característica de transmitir datos, voz y video por el mismo medio.
- No sufre de alteraciones en la señal por efectos electromagnéticos o ambientales.
- Debido a las características de flexibilidad que proporciona la fibra óptica se han adoptado o desarrollado estándares como los son: Ethernet, Token Ring, Arcnet, FDI, entre otros.



Conectores Fibra Optica.

Características	Fibras Múltimodo índice escalonado	Fibras Múltimodo índice de gradiante gradual	Fibras monomodo
Diámetro del núcleo	100μm<Ø<600μm	50μm<Ø<100μm	8μm<Ø<10μm

Diámetro de cubierta	140μm<Ø<1000μm	25μm<Ø<150μm	125μm
Índice del núcleo	constante	carece del centro a la periferia	creciente o decreciente
Apertura numérica	0.30	0.20 a 0.27	muy pequeña I=0
Banda de Paso	20 a 10 Mhz/Km	200 a 1200 Mhz/km	>10Ghz/Km, no significativa
Atenuación según las ventanas			
0,85μm	8 a 20 dB/Km		
1,3μm		2,5 a 4 dB/Km	0,3 a 0,5 dB/Km
1,55μm		0,6 a 1,5 dB/Km	0,150 a 0,3dB/KM

I.1.4.- Tarjetas de Interfase.

Las tarjetas Red *Network Interface Card (NIC),* es una tarjeta de hardware que esta alojada en el interior del Ordenador la cual nos permite tener un enlace físico de la Red con el exterior. Este elemento convierte los datos del Ordenador, los convierte a un formato apropiado para poder ser transportados y los envía por el cable para que puedan ser interpretados por otra tarjeta de interfase. Esta tarjeta cambia la información transformada al estado original y permite el enlace con el Ordenador.

Funciones:

- Almacenamiento de los datos en memoria
- Comunicaciones tarjeta de interfase – Ordenador

Estos elementos utilizan un ***"Buffer"***. Para compensar los retrasos inherentes a la transmisión y para ello almacena temporalmente los datos que serán transmitidos

a la Red o al Ordenador. Esto se debe a que la información de datos llega convertida en paquetes que recibe la tarjeta de interfase y su llegada es mucho más rápida que la conversión a su estado original por ese motivo se van almacenando en el *"Buffer"* para equilibrar la transferencia-información. Son más eficientes las tarjetas que cuentan con memoria independiente que las que tienen que utilizar la memoria del Ordenador para hacer su función.

c). Construcción de Paquetes.- La tarjeta de interfase es un dispositivo I/O (Entrada/Salida) en el que la memoria de su Microprocesador, es compartida tanto por el *CPU* (Unidad de Procesamiento Central), como por la tarjeta donde produce la partición de el mensaje en pequeños paquetes para que sean transmitidos de la tarjeta de interfase del Ordenador Emisor.

Para ello la información se codifica en señales binarias (nivel lógico "0" y nivel lógico "1") y después dicha información se debe estructurar para que pueda ser el mensaje interpretado por el Ordenador Receptor al momento de decodificarla al 100%. Además de que cada tarjeta contiene un controlador el cual los datos que recibe del Ordenador Emisor en donde esta alojado es en serie y envía los bits en paralelo para que la información sea transmitida por el medio elegido y al llegar al Ordenador Receptor esta sea convertida nuevamente pues llega la codificación en serie y a través de ella la interprete el Ordenador en paralelo, es decir se realiza un proceso inverso con respecto al Ordenador Emisor.

Las tarjetas de interfase cuentan con una serie de circuitos los cuales determinan el método para poder realizar la conexión de Red y poder así tener la comunicación con las demás Redes, los métodos utilizados son **Token Ring, Token Bus y CSMA/CD**. El proceso de comunicación entre dos tarjetas de interfase tiene su complejidad debido a la diversidad de fabricantes lo que da como resultado una variedad de tarjetas con diferentes características por consiguiente cuando sucede que se encuentran en la transmisión dos tarjetas diferentes el proceso de comunicación se hace de acuerdo a las características de la tarjeta con menos recursos, este proceso de intercomunicación entre dos tarjetas se conoce como *"handshaking"* es decir, utilizan un proceso de señalización para definir la forma de realizar la comunicación por ejemplo el tamaño de los paquetes de comunicación, tiempos de espera, etcétera.

I.1.5.- Sistema Operativo.

El Servidor requiere de software que le permita realizar la comunicación usuario-Ordenador, realizar el almacenamiento de información, el poder utilizar las terminales de las estaciones de trabajo y periféricos, además de proteger y administrar los recursos de la Red de Ordenadores para ello los sistemas operativos son ideales para cubrir esta necesidad, también en este caso hay diversidad de

software y entre ellos encontramos el **Lan Manager, IBM PC LAN, Sistema Operativo Novel Network** entre otros.

I.2.- Topologías y Métodos de Acceso.

"La Topología de una Red, es la forma física de conectar las Estaciones de Trabajo, adoptada por la persona que diseña la Red, así mismo, las Estaciones de Trabajo se comunican a la Red por un Método de Acceso Específico que depende del tipo de Red de que se trate". Según Madron (1997).

Así pues a la configuración de la Red de Ordenadores se le conoce como topología y ésta indica la forma en que se va a hacer la instalación física de la Red con el objetivo principal de que la Red de Ordenadores entregue al usuario el máximo rendimiento y tiempos de respuesta mínimos, tener un accesible tráfico de información sin demoras, perdidas y/o errores en las horas de máximo tráfico, esto se obtiene utilizando el canal de comunicación apropiado de mejor costo si así lo requiere la aplicación y el número real de elementos que se van a utilizar (Terminales, Impresoras, Graficadotes, Ordenadores Personales, etcétera).

Topología son:

1.- **Anillo.**
2.- **Árbol**
3.- **Bus Lineal.**
4.- **Estrella.**

El uso de la topología adecuada depende considerablemente de las caracteristicas y del tipo de Red de Ordenadores:

1.-Que tan flexible es la Red para poderse ampliar (conectar estaciones de trabajo)
2.-Los tiempos máximos de Transmisión – Recepción.
3.-El tráfico máximo de información que acepta la Red, sin que se produzcan interferencias continuas.
4.-El precio de la Red influye de sobremanera por que si se toma la elección errónea de elegir una topología que no es muy conveniente esto acarrea un gran costo.

I.3.- Características de cada Topologías.

I.3.a Topología Anillo.

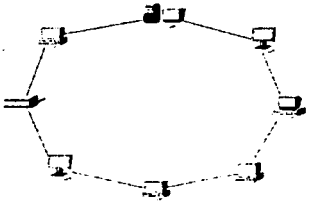
"En esta Topología, las Estaciones de Trabajo y el Servidor están conectados a través de un solo Cable de Comunicación de trayectoria cerrada, en donde la información fluye en un solo sentido.

El Método para Acceder al Cable se llama TOKEN-RING, en el cual, si una Estación de Trabajo quiere transmitir datos, envía un arreglo de bits de información (TOKEN) que son recibidos por el Ordenador más cercano, a cual los retransmite y los envía al siguiente Ordenador; y así sucesivamente hasta que el mensaje llega a su destinatario". (Giozza, De Araújo, Moura, 1996).

El Método utilizado para realizar la comunicación entre esta Red por medio del cable se llama *"TOKEN-RING"*, si alguna Estación de Trabajo quiere transmitir información de datos, envía un arreglo de bits de información (TOKEN) la cual se enviara de ordenador a ordenador hasta llegar a su destino final que son recibidos por el Ordenador más cercano, la cual los retransmite y los envía al siguiente Ordenador; y así sucesivamente hasta que el mensaje llega a su destinatario". (Giozza, De Araújo, Moura, 1996).

Las ventajas son:

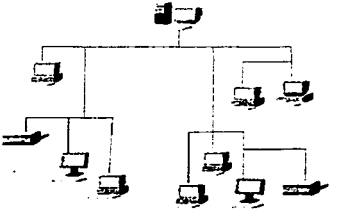
- Los tiempos de espera están bien definidos.
- El Servidor sondea las Estaciones de Trabajo para localizar la que quiere transmitir, por lo tanto cuando una Estación de Trabajo transmite no hay comunicación entre las otras y el Servidor, esto permite que no existan interferencias entre las Estaciones de Trabajo.
- Método de Acceso útil en Redes con gran carga de trabajo.
- Conexión de nodos en forma circular (por eso su nombre).
- Hay retransmisión entre nodo y nodo hasta llegar al que se quiere comunicar. Como es una conexión Serie si por algún motivo falla cualquier nodo de conexión esto provoca que la Red ya no funcione
- La ruptura de un cable de conexión en cualquier punto de la Red afecta a totalmente al circuito.
- Se necesita que un Ordenador cumpla la función de ***Monitoreo*** y esto se decide según criterios.



Topología Anillo

I.3.b Topología Árbol.

Esta topología es una de las más usadas ya que su software no es muy elaborado además de proporcionar un punto para el control y la resolución de errores siendo la Raíz (Ordenador principal) el que tiene el control de toda la Red de Ordenadores. Aunque esta topología es sencilla acarrea algunos inconvenientes ya que si existe un alto índice de envío de información, ésta puede sufrir un cuello de botella en el tráfico informativo en los niveles superiores además de que si el Ordenador Raíz sufre algún averío la Red queda totalmente inutilizada. El método de acceso utilizado es el ***TOKEN PASSING***, el software que se utiliza es muy sencillo y fácil de utilizar, concentra en una unidad (Ordenador) la solución de errores y el control, y lo más importante es que se pueden añadir más nodos.



Topología Árbol.

I.3. c Topología Bus Lineal.

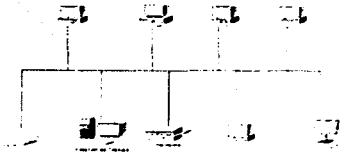
Utilizan un solo cable como medio de comunicación para realizar la transferencia de información entre las estaciones de trabajo, pudiendo utilizar como método de acceso el Token Passing, o el Carrier Sense Multiple Access With / Colision Detection (*CSMA/CD*). En este último método se compite entre Estaciones de Trabajo para ver cual de ellas es la primera que utiliza el cable de transmisión (Conant, 1996).

La Estación de Trabajo transfiere un mensaje esperando que éste llegue a su destino y que el destinatario envíe un mensaje de confirmación, si el mensaje de respuesta no llega es porque hubo una COLISION en el medio de transmisión porque otras Estaciones de Trabajo enviaron información al mismo tiempo, cuando esto sucede los equipos deben esperar un tiempo prudente y a diferentes secuencias para que puedan volver a enviar la información por el medio de comunicación, y que ahora sí llegue la información a su destino sin que haya otro percance de transferencia de información, aunque el problema se genera cuando hay una gran demanda de tráfico por que estas colisiones generan que las Terminales pierdan más tiempo que en condiciones normales provocando que el tráfico sea muy lento.

Pueden trabajar con Bus Unidireccional el cual permite alcanzar mayores distancias con amplificadores sencillos y el Bus Bidireccional el cual transmite la señal en ambas direcciones por el mismo medio o por un medio paralelo, ésta se lleva a cabo por medio de división espectral, por transformadores híbridos o duplexores (es poco usual), asignación secuencial en el tiempo.

Características:

1.- Topología simple.
2.- El principal inconveniente es que si el cable se daña la Red es inoperable.
3.- No hay retransmisión de información de nodo a nodo.
4.- La transmisión de comunicación de un nodo es en sentido bidireccional.
5.- Cuando algún nodo llega a fallar, este no provoca que la Red deje de operar.



Topología Bus Lineal.

I.3.d Topología Estrella.

"Es una combinación de la Red de Anillo y la Red tipo Lineal. Se dice que físicamente es una Red Lineal, porque tiene un bus central de comunicaciones al que se conectan las Estaciones de Trabajo en forma directa o a través de ramificaciones.

Por otra parte, su Método para Acceder, llamado TOKEN PASSING, hace que lógicamente funcione como si fuera una Red tipo Anillo". (Bates, 1994).

La forma en que las Estaciones de Trabajo se comunican con el Ordenador Central es conocido como *Token Passing*, lo que realiza este método es el envío de información en tramos de bits de una estación de trabajo a otra dando un turno para cada Terminal para que puedan realizar su transferencia de datos como si fuera una Red tipo Anillo. (Bates, 1994).

Ventajas:

1.- El Ordenador Central tiene conectados todos los nodos
2.- Si falla un nodo o una terminal no afecta la funcionalidad de la Red de Ordenadores en general.
3.- El repetidor Reenvía la información n-1 veces.
4.- El tráfico de información es proporcional con el incremento de puertos.

Según Black (1994) las características comunes más importantes, se desprenden de las topologías anteriores:

1.- Una Red de Ordenadores de Área Local (LAN) permite interconectar diferentes dispositivos y la comunicación entre ellos permitiendo acceder a todos los servicios de Red.

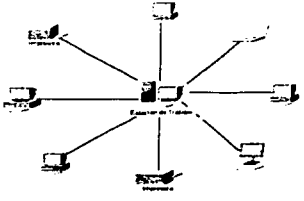
2.- El objetivo principal es permitir a las Organizaciones tener grandes ganancias en productividad y ahorros en costos mediante las eficiencias inherentes de que se comparten los recursos.

3.- Son propiedad privada y no interfieren con las leyes de comunicaciones por ende no son sujetas a la Jurisdicción de las Agencias Federales o Estatales de regulación.

4.- Las Redes de Ordenadores de Área Local (LAN) están concentradas en una sola ubicación (edificio) o a una serie de ellos, aunque esto no limita que la distancia de ubicación de algún(os) dispositivos estén a una distancia mayor puede conectar dispositivos de comunicación ubicados en diferentes pisos de un edificio o en edificios adjuntos.

5.- Las velocidades de transmisión se encuentran entre 1 y 10 Mbps, pero algunas superan la velocidad de 10 Mbps. Esto tiene como resultado que entre más rápida sea la transferencia de información se eleva el costo de la Red LAN.

6.- Las Topologías de Bus y de Anillo por el hecho de utilizar un solo medio de comunicación tiene como consecuencia que se pierda y se retarde su envió, por eso es más eficiente una topología estrella. Los dispositivos transmiten los datos de acuerdo a un determinado método de acceso esperando su secuencia para poder transmitir su información utiliza un token (Bus Lineal) o un Ordenador Central (concentrador) para la Red Estrella.

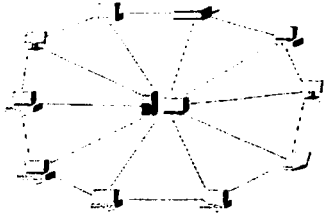


Topología Estrella.

I.3. e Topología Malla.

Esta topología es una combinación de la topología lineal y de la topología anillo conocida también como **Anillo Modificado**, este arreglo cuenta con un bus Central de Comunicaciones y en él son conectadas las Terminales de Trabajo en cada extremo de la maquina central y la información es canalizada directamente por ella, y con este arreglo se obtiene una velocidad de transferencia grande por que las Terminales no compiten unas con otras por enviar y transferir la información. (Bates, 1994).

Con la característica de que es inmune colisiones, fallas, saturación del medio de transmisión, aunque es muy costosa es muy confiable aunque con el inconveniente de que se tienen que utilizar pocos nodos.



Topología Malla.

I.4 Técnicas de Comunicación.

La transmisión de bits de información a través del Cable de Comunicación, se realiza en dos formas: En Banda Base y en Banda Ancha. (De Prycker, 1993).

Debido a que el Ordenador se comunica internamente con señales digitales y también la información que va de ella al exterior es digital, se aprovecha para que la transmisión se haga de manera digital y los elementos de conexión que se requieren para la comunicación son sencillos, por tal motivo el sistema de transmisión es la Banda Base.

También se pueden enviar varias señales de información en forma simultánea a través de un solo medio debido a que cada señal maneja diferente frecuencia se

pueden transmitir, voz, datos, video, telefonía, etcétera. Este sistema de transmisión se conoce como Banda Ancha. Algunas compañías utilizan el servicio de este sistema por que con ello pueden transmitir todas sus señales (circuito cerrado, ordenadores, telefonía, faxes, entre otros) reduciendo considerablemente el costo del servicio.

Características de las Redes de Ordenadores:

En Banda Base:

1.- Fácil mantenimiento e instalación, no requiere Módem.
2.- El número de Ordenadores que se conectan a la Red es reducido.
3.- Las distancias son pequeñas entre elementos de la Red que las distancias que se cubren en Banda Ancha.
4.- la transmisión se hace con Señales Digitales.

En Banda Ancha:

1.- Puede hacerse una a Red robusta con cables de longitudes grandes para su conexión.
2.- Permite enviar señales de diferentes frecuencias (Datos, Voz, Fax, CTV, TV, entre otros), al mismo tiempo simultáneamente.
3.- Las velocidades de comunicación en general son grandes.
4.- Utilizan un cable de transmisión y uno para recepción
5.-Se utilizan Moduladores y Demoduladores para convertir la Señal además de filtros de frecuencia y amplificadores, por consecuencia la instalación y mantenimiento de estas Redes es más costoso y complejo.

BANDA BASE	BANDA ANCHA
✓ Señalización digital.	✓ Señalización analógica utiliza MODEM de radio frecuencia para ello.
✓ El ancho de banda es consumido por la señal y no utiliza FDM.	✓ Se puede utilizar FDM y canales múltiples de datos, audio, video.
✓ Es bidireccional.	✓ Es unidireccional
✓ Topología de Bus.	✓ Topología de Bus o Árbol.
✓ Distancia: algunos Km.	✓ Distancia: superior a los 10 Km.

En base a la gran diversidad de Ordenadores que existen en el mercado local para adquirir una Red Local de Ordenadores se debe de tener en cuenta sus

características y diferencias como lo son los Estándares Internacionales que las rigen, por la Topología y el Método de Acceso que utilicen, y lo más importante por sus características individuales que las hacen útiles dependiendo de las necesidades o aplicación que les dé el usuario. Entre estas redes podemos contar la Red Local de Ordenadores: ARCNET, ETHERNET, TOKEN RING,

I.5 Red Local de Ordenadores.

Red Local ARCNET.

La Red Attached Resource Computer Network (ARCNET), es de topología de tipo Árbol con capacidad de interconectar hasta 255 nodos. Por nodo se refiere a cualquier dispositivo conectado a la Red como Periféricos y Estaciónes de Trabajo. (Black, 1999).

Características:

1.- Estructura de topología: Árbol.
2.- Utiliza el método *Token Passing* para transferir información.
3.- Utiliza el cable coaxial de 93 Ω como medio de transmisión.
4.- Transmite en banda base.
5.-. Tiempo de respuesta es determinístico.
6.- Alcanza una velocidad 2.5 Mbits/segundo.

Cuando se utilizan unidades repetidoras de para Redes Locales *ARCNET* podemos encontrar dos tipos pasivas y activas las cuales también clasifican en internas y externas.

Repetidoras Pasivas:

Si entre los nodos de la Red se encuentra poca distancia de conexión siendo esta 10, 20 , 30 50, y hasta 60 metros, y de éstos son mínimo 4, se utiliza una unidad Repetidora Pasiva, ésta contiene 4 puertos de conexión y cada conexión cubre una distancia de 30 m; conectada (unidad repetidora pasiva) a la tarjeta de Red o también se puede realizar la conexión al puerto de la unidad Repetidora Activa con la reserva de que no se pueden conectar unidades pasivas de otra unidad pasiva ni conectar unidades activas de unidades pasivas.

Repetidoras Activas:

Estas unidades cubren el inconveniente de conectar nodos que están a distancias considerables pues por sus características los hacen óptimos ya que cubren distancias de cientos de metros (máximo 600m) y se deben conectar al tomacorriente, teniendo la ventaja de poderse conectar entre ellas y con unidades repetidoras pasivas. Por consiguiente se puede hacer más grande el tamaño de la Red con solo la

utilización de estos elementos, claro si así lo requiere el caso. Estos repetidores cuentan con 8 puertos y amplifica la señal si esta llega atenuada para que la recepción en los nodos conectados a el reciban la señal en óptimas condiciones.

Ventajas:

1.- Red de uso general.
2.- Excelente comparando el costo-beneficio.
3.- El tiempo de respuesta es estable en carga de trabajo.
4.- permite un fácil crecimiento si la compañía lo necesita.

I.5.b Red Local ETHERNET.

Este Red es de tipo Bus Lineal, y recibe el nombre en analogía a la Teoría del Éter de la transmisión de la luz, para Black (1999).

Es muy práctica para la transferencia de grandes cargas de información ya que alcanza una velocidad hasta de 10 Mbps aunque tiene el inconveniente de que al utilizar el método de acceso CSMA/CD en Banda Base, su cualidad se reduce conforme aumenta el número de usuarios por consiguiente el rango de Estaciones de Trabajo sea entre 10 a 15 Activas. Este tipo de Redes puede incrementarse a un número final de 86 nodos que pueden dividirse en tres segmentos a una distancia límite de 200 m cada segmento utilizando solamente dos repetidores. Hay tres estándares de Ethernet 10 base 2, 10 base 5 y 10 base T que definen el tipo de cable y la longitud a usar, topología física para la conexión de los nodos utilizando además la topología Bus Lineal.

TIPOS DE REDES ETHERNET

Tipo	Velocidad (Mbps)	Distancia máxima (m)	Características
10 Base 5	10	500	Cable coaxial de sección gruesa conectando los nodos a través de un transceiver (tranceptor Ethernet o emisor-receptor). Utiliza codificación Manchester.
10 Base 2	10	185	Se utiliza cable coaxial de sección fina y de 50 Ω.
10 Broand 36	10	360	Cable coaxial de 75 Ω para banda ancha.

1 Base 5	1	250	Cable de par trenzado sin apantallar utilizado en redes de bajo costo.
10 Base T	10	100	Cable de par trenzado sin apantallar utilizado usualmente en la topología estrella.
100 Base X	100	Hasta 2 Km	Se pueden utilizar tres sistemas de cableado: par trenzado apantallado (UPT). no apantallado (SPT). fibra óptica (100 Base TX).

El cable y los conectores vistos bajo la norma Ethernet 802.3

	Tipo de cable	Conexión	Longitud máxima	Nº máx. de estaciónes	Observaciones
10 base 5	Coaxial grueso, 50 ohmios, o cable amarillo,	Conectores tipo vampiro	500 m	100	Líneas acabadas en una impedancia del mismo valor que la Z característica, Líneas libres acabadas en tapones para evitar los rebotes
10 base 2	Coaxial fino,50 ohmios RG58	BNC	185 m	30	conexión por "T" [Problema: hay que abrir la red] Líneas libres acabadas en tapones para evitar los rebotes
10 base T 100 base T	Par trenzado UTP categoría 5	RJ-45 (ISO 8877).	100 m		Hub: Bus lógico en una caja y todas las estaciónes colgando

Ethernet 10Base-T (T568A cc lores)

RJ45	Colores	Código	Utilidad	Pares
1	Blanco/Verde o el blanco del par verde	T3	RecvData +	PAR 3
2	Verde o Verde/blanco	R3	RecvData -	
3	Blanco/Naranja o el blanco del par naranja	T2	Txdata +	PAR 2
4	Azul o azul/blanco	R1		PAR 1
5	Blanco/Azul o el blanco del par azul	T1		
6	Naranja o naranja/blanco	R2	TxData -	PAR 2
7	Blanco/marron o el blanco del par marron	T4		PAR 4
8	Marron o marron/blanco	R4		

Ethernet 10Base-T (T568B colores)

RJ45	Colores	Código	Utilidad	Pares
1	Blanco/Naranja o el blanco del par naranja	T2	Txdata +	PAR 2
2	Naranja o naranja/blanco	R2	TxData -	
3	Blanco/verde o el blanco del par verde	T3	RecvData +	PAR 3
4	Azul o azul/blanco	R1		PAR 1
5	Blanco/azul o el blanco del par azul	T1		
6	Verde o verde/blanco	R3	RecvData -	PAR 3
7	Blanco/marron o el blanco del par marron	T4		PAR 4
8	Marron o marron/blanco	R4		

Pares usados según norma

ATM	155Mbps	usa los pares 2 y 4	(pines 1-2, 7-8)
Ethernet	10Base - T4	usa los pares 2 y 3	(pines 1-2, 3-6)
Ethernet	100Base-T4	usa los pares 2 y 3 (4T+)	(pines 1-2, 3-6)
Ethernet	100Base-T8	usa los pares 1,2,3 y 4	(pines 4-5, 1-2, 3-6, 7-8)

Si el cable utilizado como medio de comunicación es el Coaxial de 50 Ω tenemos dos opciones

Si el medio de comunicación seleccionado es el cable grueso podemos utilizar como máximo hasta 500 Metros/Segmento de longitud además de necesitar dos terminadores por segmento y un *"Transceiver"* por cada estación de trabajo; si queremos realizar la conexión mínima entre nodos es 2.5 m entre estaciones de trabajo sin sobrepasar ambos límites.

Si el medio de comunicación seleccionado es el cable delgado podemos llegar a un límite de cable de conexión de hasta 300 Metros/Segmento de longitud; y para cubrir distancias pequeñas tenemos como límite mínimo hasta 3 m de distancia entre estaciones de Trabajo requiriendo para ello dos terminadores por segmento y conector del tipo "T" por Estación.

Por último:

La distancia total que debe cubrir la Red de Ordenadores es de 555 m como límite además de que cada segmento debe de tener como longitud máxima 185 m, y un mínimo de medio metro, teniendo un total de 5 segmentos por repetidores, conectados dos segmentos pasivos y tres segmentos activos.

Ventajas:

1.- Excelente capacidad de trabajo con pocos nodos.
2.- Flexible la conectividad a otros ambientes (uso específico).
3.- Está apoyado por varias Empresas Transnacionales de importancia.

Principales desventajas:

Tiempo de respuesta decreciente cuando la componen numerosos nodos, y también bajo carga de trabajo. Además se deben de dejar líneas de conexión para la futura ampliación de la Red.

I.5.c Red TOKEN-RING.

Este Red utiliza la tecnología de paso de señal en forma secuencial Utiliza el *MAU* (Multi Acces Unit), este dispositivo permite que la Red en topología anillo se mantenga cerrada aunque algunas estaciones estén o no estén trabajando (apagadas), por consiguiente cuando se manda una señal y si detecta algún nodo apagado la MAU

lo brinca para seguir con el que si esté encendido, aunque se tiene el inconveniente de que cada nodo de Red *Token Ring* primero examina y posteriormente re-envía la señal y si en este proceso el nodo no opera en óptimas condiciones provocará que la Red deje de funcionar, por este motivo para que siga manteniendo cerrado el Anillo, es necesario que se sigan conectando las Unidades Centralizadoras entre sí y como cada unidad tiene dos puertos adicionales por ellos se mantiene la interconexión.

Por lo tanto; *Token Ring* puede ser menos eficiente comparado con CSMA/CD en condiciones inferiores a la actividad normal ya que este tipo de Redes de Ordenadores trabaja mucho mejor en condiciones de carga de trabajo excesivo por lo tanto cada estación de la Red recibe la señal y la pasa a la siguiente estación, esta Red surgió a finales de 1985 con el patrocinio de IBM y utiliza el par trenzado como medio de comunicación, y transmite a 4 o a 16 Mbps permitiendo tener hasta un total de 255 nodos conectados, con el gran inconveniente de que algunos dispositivos son difíciles de localizar y si están disponibles éstos se encuentran a un costo muy elevado a comparación de los dispositivos para Red Ethernet.

Esta Red es muy recomendada cuando se tiene la necesidad de que la Red se comunique con un Mini Ordenador o un *"Mainframe"* IBM. Las *MAU's* que hay en el mercado son de 4 puertos, por lo que solamente se pueden tener cuatro máquinas conectadas a él; sin embargo, si se requiere de más equipo en la Red, es necesario que se coloquen más unidades de este tipo.

características del cableado:

1.- Se utiliza el cable tipo 3 (AWG 22/24) de dos pares trenzados (Telefónico).
2.- Se pueden instalar hasta 72 nodos como máximo.
3.- El número de *MAU's* que se pueden conectar es de 18 solamente conectados en cascada.
4.- La distancia máxima entre el *MAU* y Estación de Trabajo es de 150 m.
5.- La distancia máxima entre *MAU's* es de 150 m.

Ventajas:

1.- Tiempo de respuesta estable.
2.- Conecta gran cantidad de nodos.
3.- Conectividad a otros productos IBM.
4.- El Sistema Operativo *IBM PC LAN,* está diseñado específicamente para esta Red.
5.- El inconveniente es que decae su ventaja cuando se compara el costo con los demás tipos de Redes.

I.6.- Redes Inalámbricas.

Estas Redes de Ordenadores son necesarias cuando la información que se necesita enviar a otra parte de la Red, no puede ser comunicada por un medio de una transmisión física debido al lugar en donde se encuentre ubicada, ya sea por que el muro es difícil de perforar para hacer ductos, que se encuentren las Estaciones de Trabajo a una distancia muy considerable y que el tráfico vehicular obstaculice ya que sus ubicaciones son de un edificio a otro, que sean edificios o museos de gran valor cultural. Por tal motivo, se utiliza como elemento principal de transmisión las tarjetas que trabajan con señales de microondas para que la información sea transferida de un Ordenador a otro y así evitar los inconvenientes mencionados anteriormente

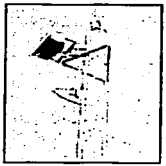
WAP-1950 cumple con las especificaciones estándar IEEE802.11b de alta velocidad, y soporta dos conectores estándar SMA para antenas direccionales externas, para añadir la capacidad de conexiones a larga distancia con el objeto de realizar conexiones LAN-to-LAN entre edificios remotos

Características:

Si se quiere utilizar una tarjeta inalámbrica, se deben tomar en cuenta varias condiciones entre las que destacan la distancia, la línea de vista entre las Estaciones de Trabajo y el Servidor; si no existe esta línea de vista, hay que tener en cuenta la atenuación en la señal al estar en el interior por las pérdidas en muros y/o otros objetos entre las Estaciones de Trabajo y el Servidor provocando una disminución en el alcance de la señal, la máxima velocidad con que puede trabajar la tarjeta, compatibilidad con los Sistemas Operativos además de la compatibilidad con otras tarjetas de Red y que se cuente Soporte Técnico garantizado aquí en el país.

Se pueden usar en combinación con otras tarjetas de Red como por ejemplo ARCNET, Ethernet y/o Token-Ring. Permitiendo unir dos Redes Ordenadores ubicadas en localidades diferentes y distantes, esta distancia puede ser de unos metros hasta algunos kilómetros. Estas contienen un sistema de seguridad para mantener protegida la información que se envía por medio de microondas utilizando códigos de envío que solamente la tarjeta que recibe la información la puede interpretar.

Las tarjetas pueden utilizar o no utilizar una antena, si no es utilizada solo puede cubrir unos 250 metros, si la antena es utilizada se pueden cubrir distancias de 8 Km., la antena es un cable aproximadamente de dos metros de longitud, un extremo tiene un conector que va a la tarjeta y el otro extremo un solenoide simulando una antena parecida a la de los radios tipo AM. También hay otro tipo de antena utilizado que es una antena rígida de unos 20 o 40 cm., de altura, muy similar a las de los radiotransmisores.



Antena de Alta Ganancia

Antena Típica

En nuestro país (México), la Compañía *NCR*, vende tarjetas inalámbricas **"WaveLan"**, la cual tiene un alcance de 250 Metros sin antena y de 8 Kilómetros con antena omnidireccional de formato *ISA y MicroCaral* con un costo alrededor de $ 2,400 dólares

Ventajas:

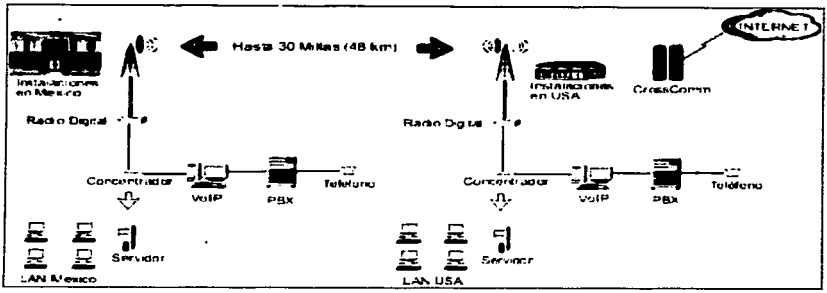
1.- Se elimina el realizar nuevos ductos para el paso del medio de comunicación de una Estación de Trabajo a otra.

2.- Este tipo de elementos permiten que el reacomodo o cambio de ubicación de los Ordenadores sea más fácil sin preocuparse por el movimiento de los cables que lo unirían a los demás elementos de la Red de Ordenadores.

3.- Cambiar una oficina de un piso a otro, sin que el cambio físico de la Red sea un problema y reduciendo costos generados por el mismo movimiento.

4.- Útil en el cableado de Redes que se instalan en Edificios Históricos.

5.- Se reducen en gran número las fallas de comunicación, considerando que entre el 50% y el 70% de los problemas presentados en una Red Local, son ocasionados por malas conexiones del cable.



Desventajas:

1.- Incompatibilidad de este tipo de Redes con los Sistemas Operativos conocidos (Novel o LAN MANAGER, por ejemplo).

2.- Su velocidad de trabajo es inferior comparándola con las Redes Estándares o Comerciales (Ethernet, Arcnet y/o Token-Ring).

3.- Las tarjetas para Red Inalámbrica son incosteables que si se realizara una Red de Ordenadores normal de cable coaxial o cable telefónico

4.- Cuando se instala este tipo de Redes, se tiene que dar aviso a la Secretaría de Comunicaciones, dado que se están utilizando Microondas para la transmisión de datos además de que en nuestro país no hay con quien comunicarse para el soporte técnico para estas tarjetas.

I.7.- Sistemás Operativos para Redes.

"El Sistema Operativo de la Red, es un conjunto de programas que residen en el Servidor y que se encargan de comunicar a las Estaciones de Trabajo entre sí, garantizar la integridad de la información y controlar el uso de los recursos de la Red". (Milenkovic, 1998).

El Sistema Operativo proporciona un método de trabajo sencillo, claro y seguro que faciliten la utilización y la exploración de la Red, es instalado en el Servidor y cada Estación Trabajo, necesita algunas rutinas de software para comenzar con la comunicación entre ambos y se pueda comenzar a trabajar.

Para elegir el Sistema Operativo adecuado a nuestras necesidades debemos tener presente si es (abierto) compatible con la mayor parte de tarjetas de Red, Ordenadores y Periféricos de las diferentes marcas y los diferentes modelos, que permita la intercomunicación con otros Sistemas Operativos *(minis, mainframes, y Ordenadores de otros fabricantes)* y que tenga la capacidad de permitir la interconexión de Redes de Área Local *(LAN)* de diferentes Topologías, proporcionar un gran nivel de seguridad, mantener la integridad de los datos, evitando corrupción de información, proporcionar jerarquías de acceso dependiendo el rango y uso de cada usuario así como negar el acceso a personas que traten de entrar a una sesión que no les corresponde, proporcione tolerancia a fallas eléctricas o a fallas del disco, que sea de gran eficiencia sea flexible y que sea muy fácil de usar.

Podemos encontrar en el mercado los Sistemas Operativos para Redes basadas en Servidores, y los Sistemas Operativos para Redes Distribuidas *("Peer to Peer")*.

Las Redes basadas en Servidor:

El Servidor es un Ordenador de muy alta capacidad donde reside todo el software de aplicación para la Red y se encuentran interconectados todos los Periféricos a utilizar. Los Sistemas Operativos usados en estas Redes son de gran costo y medianamente complejos, por este motivo se necesita que el personal este capacitado para su uso; aunque se tiene este inconveniente su contraparte es que estos Sistemas son de gran eficiencia, soportan una gran cantidad de usuarios, tienen la capacidad de que se pueden interconectar Ordenadores de distintas marcas y modelos.

Por el gran beneficio que proporcionan son sumamente usados en Grupos Industriales y Negocios, Bancos, Casas de Bolsa, con grandes necesidades de captura, cálculos, comunicaciones y reportes. Entre estos Sistemas Operativos podemos contar a Novel NetWare, LAN Manager de Microsoft, Vines, 3+Open LAN Manager, Nexos y muchas más marcas, siendo Novel Netware y Windows NT son los Sistemas Operativos más utilizados en México.

Las Redes Distribuidas:

Cualquier Ordenador de la Red puede ser Estación de Trabajo y Servidor a la vez, con ello se puede compartir cualquier programa o periférico de cualquier otro de los Ordenadores que forman parte de la Red. Éstos son muy sencillos y baratos, sólo

son recomendables para Redes que no son muy grandes, es decir que el número de elementos que la conforman pueden llegar a ser hasta 12 nodos, proporcionando rendimiento y un costo muy aceptable, es decir que si queremos lograr un estado optimo solo podemos conectar hasta 7 nodos.

Los Sistemas Operativos más populares para este tipo de Redes son NetwareLite de Novel, Great OS de Gateway Communications y LANTASTIC de Artisoft donde sus características en común son:

1.- Facilidad en su adquisición y costo accesible.
2.- Permite una rápida instalación.
3.- Fáciles de aprender a usar.
4.- Simples para darles mantenimiento (dar de alta usuarios y recursos, cancelar impresiones, corregir fallas de comunicación, etcétera).
5.- No requieren equipo especial.
6.- No requieren personal especializado, para dar mantenimiento.
7.- Son totalmente confiables.

9.- Son compatibles con los Paquetes y la Programación *("Software")* ya que trabajan sobre el Sistema Operativo *DOS*.
10.- Es esencial para Empresas Pequeñas, Consultorios Médicos o Bufetes de Abogados y Contadores.

I.7.1.- NETWARE de NOVELL.

Este Sistema Operativo es el de más popularidad y hasta hace poco el más común para Ordenadores Personales compatibles con Intel. Es funcional en diferentes Topologías de Red y dependiendo que hardware sea el seleccionado este Sistema Operativo, puede ejecutarse en una Red de configuración Estrella, agrupamiento de Estrellas, Token Ring y hasta en Red de tipo Bus Lineal. Este Sistema Operativo, es diseñado para proporcionar soporte de Servidor de Archivos de Red; en el modelo OSI de Software de Servidor de Archivos reside en la capa de aplicaciones, y el Software Operativo de disco "DOS" reside en la capa de presentación. El software de Servidores de archivos forma una cubierta alrededor de los Sistemas Operativos, como el DOS y tiene la capacidad de interceptar comandos de programas de aplicaciones antes de que lleguen al procesador de comandos del Sistema Operativo. El usuario no se preocupa por saber el proceso que se realiza para poder tener acceso a alguna información en específico, pues nada más preocupa solicitarla y que el ordenador proporcione el archivo solicitado.

I.7.2.- WINDOWS NT SERVER.

Este es un Sistema Operativo de 32 bits poderoso, disponible en versiones *"cliente"*, cuenta con la característica de multitarea prioritaria, proceso de

multilectura, soporte para multiprocesamiento simétrico y portabilidad, permitiendo con estas características realizar tareas preferentes y subordinadas, siendo el propio Sistema Operativo, el que determine cual programa debe interrumpirse y comenzar a ejecutarse otro, realizar procesos de lectura múltiple o hebras esto es que se puede ejecutar un proceso de manera simultanea diferentes partes de un programa en diferentes procesadores. El multiprocesamiento permite que los requerimientos de sistema y de aplicación se distribuyan de manera uniforme entre todos los procesadores disponibles haciendo que la ejecución resulte de manera más rápida.

Emplea el sistema de archivos NTFS que permite que los archivos tengan nombres de hasta 256 caracteres, permite el rastreo de trasacciones es decir que si NT sufre un fallo los datos se recuperan en el estado anterior al fallo o caída del sistema; este Sistema Operativo, fue diseñado para que fuera portátil ya que cuenta con un kernel o núcleo, diferentes subsistemas de sistema, cuenta con subsistemas disponibles para aplicaciones que ejecutan programas basados en OS/2 y POSIX, además de un procesador DOS virtual VDM, MS-Dos, aplicaciones de Windows de 16 bits, software de Red de punto a punto para que usuarios de requieran Windows trabajo en grupo lo utilicen o utilicen NT.

1.7.3.- UNIX.

El Sistema Operativo de UNIX ha tenido una evolución durante los últimos años desde su creación como experimento, hasta convertirse en uno de los sistemas operativos más populares e influyentes en el mundo, el objetivo de la creación de este sistema es la de distribuir la funcionalidad en pequeñas partes: Los *programas*, de esta manera se pueden obtener nuevas funcionalidades y nuevas características de una manera sencilla mediante las combinaciones de pequeños programas y conforme se van actualizando estos se pueden integrar al área de trabajo. La utilidad de este sistema es principalmente en lugares donde se desarrolla investigación científica. Las características del UNIX actual son que tiene memoria virtual, multitarea y multiusuario.

En nuestros días las nuevas versiones UNIX para un uso de Red fácil y funcional, por lo que es muy común encontrar versiones de este sistema en grandes unidades centrales con capacidad de soportar grandes números (cientos) de usuarios al mismo tiempo trabajando. Su capacidad y su gran base de software de comunicaciones propicia que la computación por Red sea simple permitiendo que se compartan dispositivos como impresoras, base de datos y disco duro.

UNIX cuenta con la versión **SVR4 (Sistema Versión 4)** la más actual de UNIX, ha sido mejorado con respecto a las versiones anteriores por ejemplo con la interfase grafica de usuario **"GUI"** que permite utilizar X Windows, además de incluir soporte completo para las Redes de Área Local de Ordenadores, se mejoro la administración de ordenadores conectadas en Red y se puede realizar la administración remota por

medio de la misma; los sistemas como UnixWare de SCO y Solaris de Sun Microsistems están también basados en el SRV4

I.7.4.- LINUX

Éste es una derivación del Sistema UNIX que puede correr en varias plataformas, preferentemente en ordenadores que tienen procesador Intel. Este Sistema Operativo, permite que cualquier Ordenador lo podamos convertir en una Estación de Trabajo con las mejores cualidades de UNIX. LINUX fue y sigue en desarrollo por un grupo de voluntarios que intercambian códigos, trucos, además de resolver problemas de sistema en un ambiente abierto, LINUX esta dentro de la estandarización de IEEE denominados POXI (documentos de estandarización), estando dentro de los POXI-1 y POXI-2. Además de estas características cuenta con una antememoria caché que permite que el disco duro trabaje en mejores condiciones, es decir que almacena temporalmente la información en la memoria RAM antes de guardarla en el disco duro; además de que cuenta con una sincronización de lo que LINUX cree que tiene en disco y lo que realmente hay almacenado con un tiempo de sincronización de 30.

La ventaja que nos proporciona LINUX es que casi todo el software para UNIX puede correr sin problema incluyendo el sistema de Windows X, o solo X es una interfase gráfica de usuario estándar para maquinas UNIX es un poderoso ambiente que soporta muchas aplicaciones como por ejemplo: Se pueden tener activas varias ventanas de terminales a la vez (consolas virtuales), teniendo una sesión de trabajo diferente cada ventana.

Para establecer comunicación en la Red, este Sistema Operativo, soporta dos protocolos de Red, el TCP/IP y el UUCP. Con TCP/ IP y una conexión a Internet los usuarios pueden tener comunicación con otros ordenadores, por último LINUX soporta conectividad con Microsoft Windows, Macintosh Apple Talk y Local Talk y el protocolo IPX de Novell.

CAPÍTULO II.

PROTOCOLOS PARA REDES DE ORDENADORES.

Introducción:

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de máquinas que estén conectadas (PC, Mac,AS-400...).
- Abstraer a los usuarios de los enlaces utilizados (red telefónica, radioenlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de ordenadores, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.

Diferentes empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando diferentes familias de protocolos, y dándole diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etcétera).

II.1.- Definición.

Cuando se realiza una comunicación entre dos personas ya sea en persona o por medio teléfono, hay momentos que surge un intercambio tal que los dos hablan en el mismo momento que ya no se entiende lo que se esta conversando y por consiguiente el mensaje se trunca y hay que volver a comenzar desde el punto de falla esta conversación.

Dentro del desarrollo de las Redes, se ha buscado siempre el incremento en la velocidad de procesamiento y para evitar este riesgo de empalme de información provocando las colisiones, es necesario implantar Reglas de Comunicación.

Sin importar el tipo de Comunicación entre Sistemas comunes son necesarias un conjunto de Reglas que rijan la transferencia de información para que ésta pueda ser provechosa totalmente.

Por lo cual se creo un conjunto implícito de Normas que reglamentan la Comunicación, este conjunto de Reglas recibe el nombre de *"Protocolo"*. Por lo cual, cualquier Proceso de Comunicación independientemente de los Sistemas que se traten, y el nivel de comunicación, presupone la existencia de cierto(s) Protocolo(s). Pero un Protocolo debe reunir ciertas características y/o propiedades que son de sello general; es decir, se encuentran implícitas en la mayoría de las especificaciones, estas son:

1.- Ausencia de retardo.

Garantiza que el Protocolo, bajo ninguna circunstancia, llegará a un estado de inactividad total, permaneciendo ahí por largo tiempo.

2.- Complitud.

Asegura que la especificación para cada estado, dé una respuesta a todas las entradas posibles.

3.- Actividad.

Asegura el cambio de Protocolo de un estado a otro, de manera que partiendo de cualquier otro estado, se enlacen (eventualmente), todos los demás estados de forma automática.

4.- Realización de progreso.

El Protocolo, no presenta comportamientos inútiles, o de forma equivalente; no permanezca en un estado de inactividad más que en un tiempo finito.

5.- Terminación.

Cada operación termina eventualmente en un intervalo de tiempo finito.

6.- Corrección parcial.

Al término de una Operación se produce un resultado correcto.

7.- Minimizado.

El Protocolo engloba sólo las situaciones que puedan producirse.

8.- Estabilidad.

Después de un fallo, el Protocolo vuelve al funcionamiento normal de un intervalo finito (autosincronización).

La mayoría de estos Protocolos, aunque realizan una función específica son comúnmente confundidos con otros elementos participantes en el proceso de Comunicación de Datos.

II.2 Función.

Para que entre los diferentes componentes de una Red Local se realice de forma ordenada y/o eficaz el intercambio de información, se tiene que establecer una serie de Protocolos que definen las Reglas a seguir cuando se efectúa una Comunicación.

Cada interfase de una Sub-Red, se responsabiliza a llevar a cabo el Protocolo de acceso al medio que controla las comunicaciones a través del medio; el Protocolo de enlace que regula una comunicación entre interfases, y el Protocolo de acceso a la Red que especifica y supervisa las interacciones entre una interfase y un usuario.

Estos se conocen comúnmente como de bajo nivel. Además, encima de los Protocolos de bajo nivel, existe otro conjunto llamado Protocolos de alto nivel. Estos últimos definen y supervisan una comunicación entre usuarios ó sus Procesos. Tienen significado límite a límite; es decir, se aplican a la comunicación entre usuarios propiamente dichos; puntos finales de la comunicación.

La función del Protocolo es ofrecer servicios que determinen el orden entre los elementos que participan en el Sistema de Comunicación, sin importar en qué nivel se encuentra; ya que en cada nivel, se encontrará un Protocolo. (Black, 1995).

Por lo tanto un Protocolo puede encontrarse en la comunicación entre interfases en la descripción del comportamiento de Entrada/Salida. Este depende de una serie de acciones que determinan su estado ó alguna excitación a la cual responde ejecutando un proceso.
Las alteraciones del estado pueden ser funciones de interacciones pasadas al sistema local, restricciones locales y/o interacciones anteriores en sistemas remotos; restricciones globales.

Por ejemplo, si al llamar a un teléfono que se marca se contesta levantando el auricular del teléfono marcado, esta es una acción de restricción local.

El ver quien habla primero o segundo, es una restricción global.

Por consiguiente podemos ver que un Protocolo tiene una función específica, pero va a depender del nivel donde se encuentre, y a las acciones que sobre él sean ejecutadas.

II.3 Protocolo INTERNET.

Los Usuarios y los Proveedores, normalmente emplean niveles híbridos de Protocolos a partir del Modelo OSI, y del Estándar del Protocolo de Control de Transmisiones/Protocolo Internet. El TCP/IP, desarrollado por el Departamento de Defensa, se ocupa del tercer y cuarto estrato de el Modelo OSI.

El TCP/IP abre una *"Tubería"* transparente de datos entre los nodos externos de la Red, y asegura que los datos sean enviados correctamente y entregados sin errores.

Este transporte físico de datos, se logra mediante una Red de Área Local (LAN) ó una Red de Área Amplia (WAN) empleando la interfase de Comunicación por Paquete X.25.

Una de las debilidades del Modelo OSI, es su incapacidad para enlazar diferentes Redes. La fuerza del TCP/IP, se encuentra en su capacidad para enviar datos entre diferentes Redes; por ejemplo, *X.25, Ethernet y Token Ring*.

Y para el manejo de Redes que incluyan miles de nodos. Algunos se refieren al TCP/IP como el "superaglutinante que puede conectar a todos los dispositivos".

II.4 Protocolo Técnico de Oficinas.

Otro punto importante en la Estandarización de Arquitecturas de Redes de Sistemas es la creación el Protocolo de Automatización de Manufactura, desarrollado por la *General Motors Corporation*, y el Protocolo Técnico de Oficinas, desarrollado por *Boeing*. Como se sabe, el objetivo del Protocolo de Automatizacion de Manufactura (MAP), es definir una Red Local y los Protocolos asociados de comunicaciones para los recursos de los Ordenadores, Controladores Programables y Robots dentro de una Planta o Complejo Fabril.

El Protocolo de Automatización de Manufactura (MAP), utiliza como referencia al Modelo OSI, en especial el Estrato de Transporte. Utiliza la Red de Token Bus, que es generalmente el Protocolo preferido en un ambiente de manufactura. El Protocolo de Automatización de Manufactura (MAP) requiere una

Red de Banda Ancha en vez de una Red de Banda Base. La Banda Ancha es necesaria, debido a su habilidad para manejar Voz y Vídeo, así como la Transmisión de Datos. Además, las Redes de Banda Ancha poseen altas tolerancias necesarias en un ambiente de fabricación.

Unos cuantos dispositivos adyacentes se pueden unir fácilmente, mediante el cableado de par trenzado; sin embargo, en una Planta de Manufactura, en donde muchos Dispositivos están distribuidos a lo largo de miles de pies cuadrados, un sólo cable coaxial de Banda Ancha proporciona una conexión fácil y permite una mayor flexibilidad.

El crecimiento en las operaciones puede dar por resultado un enmarañamiento en el cableado, ocupando espacio y haciendo imposible el diagnóstico de los problemas de la Red. Cada, que se agrega un dispositivo con par trenzado se incurre en costos adicionales de cableado.

Además, la Banda Ancha puede manejar concurrentemente dispositivos síncronos y asíncronos, y conectar dispositivos con diferentes velocidades de datos.

En consecuencia, los productos de el Protocolo de Automatización de Manufactura (MAP) son más fáciles de instalar e intercambiar, debido a que se requieren menos cables y menor tiempo de cableado.

II.5 Normalización Internacional de Protocolos de Alto Nivel.

El esfuerzo de Normalización de Redes Locales (a nivel Internacional), se inició en Febrero de 1980 con la creación de el Comité 802 del IEEE.

Las Normas de Redes Locales propuestas por el Comité IEEE 802, deberían ser compatibles con el Modelo OSI, en lo que se refiere a Protocolos de Red y deberían tener en cuenta los esfuerzos de Normalización de los Protocolos de Nivel más altos; es decir, los Protocolos de las capas 4 a la 7 del Modelo OSI. (Comer, 1995).

Se propuso un conjunto de Normas con los siguientes puntos:

- **1.- Las aplicaciones pretendidas son sencillas Comerciales e Industriales**
- **2.- La longitud máxima del medio es de 2 Kilómetros, y la velocidad de transmisión entre 1 y 20 Mbps.**

- **3.- Conexión mínima de 200 Estaciones al mismo cable.**
- **4.- La Norma debe ser independiente del tipo de medio de transmisión y de la técnica de señalización.**
- **5.- La fiabilidad de la Red sólo puede presentar un error detectado por año, y el fallo de un equipo en la Red no debe comprometer su operatividad.**
- **6.- La comunicación entre dos equipos cualesquiera conectados a la Red debe ser directa, sin pasar por equipos intermedios.**

La razón del Comité IEEE 802 para proponer un conjunto de Normas, y no una sola Norma; es que existían Arquitecturas de Redes Locales, que cumplían los puntos anteriores sin que ninguna de ellas se mostrara claramente superior a las restantes.

Por ello, la propuesta del Comité IEEE 802 incorpora dos Técnicas de Acceso al Medio de Transmisión (o Protocolo de Acceso), dos Topologías inspiradas básicamente en la segunda mitad del punto 5 y del punto 6; y establece además, variaciones en el tipo de medio de Transmisión, Velocidad de Transmisión, Número de Bits de Direccionamiento, etcétera.

Complican Topologías donde las características de difusión, pueden ser fácilmente implantadas (es decir, la transmisión de informaciones o Paquetes de la Red, a una determinada Estación, es captada por todas las demás Estaciones de la Red). Se seleccionaron las Topologías en Línea y en Anillo. En la Topología en Línea, la transmisión de una estación o interfase, se propaga a los puntos terminales de la Línea, siendo captada por todas las interfases a la derecha y a la izquierda de la interfase transmisora. En la Topología en Anillo, la transmisión de una interfase recorre toda la extensión del Anillo, hasta volver a la interfase transmisora, siendo de esta forma captada eventualmente por todas las otras interfases, eliminando la necesidad de las funciones de ruta, presentes en la capa de la Red de el Modelo OSI. Además, el Protocolo de Acceso, es el que regula las entradas de las interfases al único medio de transmisión (dispuesto en Línea o en Anillo).

Se limitó la propuesta de Redes Locales a las Capas 1 y 2 de el Modelo OSI; es decir, a las Capas de Medios Físicos y Enlace de Datos respectivamente, dejando vacía la capa de Red (3). Las Capas 4 y 7 son independientes de las características de la Red, y por tanto, sólo son relativas a las Capas 1 y 2; toma la Capa 2 del Modelo OSI y la divide en dos Subcapas: Control de Enlace Lógico y Control de Acceso al Medio. La Capa 1, está lógicamente organizada por una parte de señalización física y otra para la conexión a los medios físicos. La interfase para la unidad de conexión, y entre la parte

de conexión de los medios físicos y el medio propiamente dicho; se define la interfase dependiente del medio.

La Capa 1 de Medios Físicos **Capa Física**; se ocupa de: La forma de transmisión (Banda Básica contra Banda Larga), forma de Codificación y de Decodificación de las señales binarias, detección de transmisiones simultáneas ("Colisiones"), niveles de voltaje, definición de conectores y terminales, etcétera.

La Capa 2 o Subcapa para el Control de Acceso al Medio (MAC), especifica el Protocolo de Acceso al Medio y las posibles funciones de prioridad para este acceso. Adoptando dos Protocolos de Acceso: CSMA-CD y el Protocolo con transferencia de Ficha. En el Protocolo CSMA-CD, cada interfase "escucha" al medio de transmisión, y transmite sólo cuando el medio está libre. Las interfases escuchan sus propias transmisiones y dejan de transmitir, las interfases involucradas en colisiones esperan durante un intervalo de tiempo (intervalo de retirada), uniformemente distribuido cuyo valor medio se duplica en cada colisión de un mismo Paquete (tiene un límite del valor medio, que cuando se alcanza, hace que la interfase en cuestión cancele el intento de transmisión).

En el Protocolo inferior, pasa una ficha de estación a estación siguiendo el orden de Acceso al Medio de Transmisión. Cada interfase sólo puede transmitir un paquete al medio, cuando posee la ficha, el intervalo de retirada y la posesión de la ficha, sirven para regular indirectamente la congestión en el medio de transmisión. Con relación nuevamente al asunto de identificación, para atender las tendencias actuales; la Capa para el Control de Acceso al Medio (MAC), permite dos tamaños de direcciones en su estructura de cuadros (unidad de servicio).

Los dos Protocolos de acceso descritos pueden ser integrados en una Topología en Línea ó en Anillo. Por ello, el Comité IEEE 802, descartó la alternativa la cual el Protocolo CSMA-CD es propio de una Red de Anillo.

Se sugirió para la Subcapa MAC [IEEE 802]:

- ✓ 1.- Norma IEEE 802.3.- Que corresponde a la línea CSMA-CD.
- ✓ 2.- Norma IEEE 303.4.- Que corresponde a la línea con transferencia de ficha.
- ✓ 3.- Norma IEEE 802.5.- Que corresponde al anillo con transferencia de ficha.

La Norma IEEE 802.6, en fase de estudio, establece un Método de Acceso para Redes Metropolitanas.

Las Normas para la Subcapa de Control de Enlace Lógico (LLC), bautizada como IEEE 802.2, puede utilizarse conjuntamente con cualquiera de las Normas de la

Subcapa MAC. El IEEE 802.2, define dos tipos de servicios ofrecidos a la capa inmediatamente superior.

El tipo 1, es un servicio de diagrama de tiempos simple, donde la entidad-fuente puede enviar sólo un *Paquete* a una entidad-destino, y no tiene garantía en entregar correctamente la información, ni indicación de recibido.

El tipo 2 es un servicio orientado a la conexión, donde el Control de Enlace Lógico (LLC) permite el envío de múltiples unidades de información, y garantiza la entrega correcta de la información a través de retransmisiones, en caso de error.

El servicio tipo 2 evita recibir información equivocada ó información entregada fuera de la secuencia del servicio. El Protocolo de Control de Enlace Lógico (LLC) orientado a conexiones, se asemeja al Protocolo HDLC de la ISO. Los dos tipos de servicios de la Subcapa de Control de Enlace Lógico (LLC) deben satisfacer las diversas aplicaciones potenciales, dejando a las Capas superiores que escojan la calidad del servicio deseado en función de sus características.

El proyecto IEEE 802 (recoge diversas Normas), ofrece opciones en cada una de las Capas consideradas, pero no se adoptan todas las combinaciones posibles con la integración de las dos Capas.

Existe otro esfuerzo internacional, para hacer compatibles Protocolos de Redes de Área Local (LAN), es el que está haciendo:
The European Computer's Manufactures Association: **ECMA.**

Afortunadamente, la ECMA, está trabajando con estrecha colaboración con el Comité IEEE 802. En Junio de 1982, la ECMA ratificó un conjunto de Normas para Redes Locales entre las cuales se seleccionó la combinación CSMA-CD. Lista básica y servicio de transferencia de información orientados a diagramas de tiempo. Las otras combinaciones deberán ser ratificadas en el futuro [ECMA 82].

Los Protocolos de Comunicaciones en épocas pasadas, se desarrollaron individualmente para cada aplicación. Los Protocolos para un entorno cerrado, no funcionan bien se hacen más complejos a medida que las aplicaciones cambian. (Fischer, Wallmeier, Woster, Davis y Hayter, 1994).

Dando como resultado una serie de Protocolos no estructurados y de difícil mantenimiento. Los Protocolos que gobiernan los servicios de Telex y de TeleFax, grupos 1, 2 y 3 están pensados para un único Servicio y no pueden, fácilmente incluir nuevas funciones.

En el Modelo OSI de la ISO, se permite un desarrollo ordenado de nuevos Protocolos de Comunicación. La estructura en capas del Modelo OSI minimiza la dependencia entre varias funciones, y permite alterar una capa sin que ello afecte

necesariamente a las demás, permitiendo así; un mejor mantenimiento y ampliación futura de los Protocolos.

Hay que resaltar aquí que, inicialmente, la ISO prefirió no definir las interfases entre las diferentes capas. Así se permitió una cierta libertad a los diseñadores para que realizaran cambios a corto plazo de Tecnología en el desarrollo de sus productos. Observando que estos cambios de Tecnología afectaron a los Protocolos más que a las interfases, y que la Normalización de interfases facilitaría sustancialmente la portabilidad de las implementaciones.

La Normalización de una Arquitectura ó de un Protocolo, debe permitir la flexibilidad de ampliación futura, debido a la imposibilidad de prever las nuevas aplicaciones. Por consiguiente, las Normas deben evolucionar.

El Modelo OSI (que normaliza una Arquitectura), por ejemplo; está evolucionando y continuará evolucionando, por la necesidad de incluir aspectos no considerados inicialmente, según Perlman (1992); tales como:

- 1.- Transmisión de datos sin conexión (el Modelo OSI estaba basado inicialmente en el concepto de *"Conexiones"* entre dos entidades).
- 2.- Redes locales.
- 3.- Redes integradas.
- 4.- Interconexión de Redes.
- 5.- Servicios transaccionales.
- 6.- Servicios Electrónicos de Mensajes, aspectos de seguridad, interfases de lenguajes, etcétera.

Estos aspectos están forzando la elaboración, interpretación y esclarecimiento del Modelo OSI. Las únicas capas del Modelo OSI que están bien atendidas por las Normas Internacionales actuales son las capas de bajo nivel; es decir, Física, de Enlace y de Red.

En consecuencia, sólo son abordados totalmente por estas Normas los aspectos técnicos de transferencia de datos en varios tipos de Redes. Las propuestas de Normalización de Protocolos para Redes Locales, se concentran también sólo en estas capas.

Como ejemplo de Normas Internacionales para las Capas 1 y 3, se citan los Protocolos RS-232 (Capa Física), HDLC (Capa de Enlace), y X.25, nivel 3 (Capa de Red). Es interesante observar, que estos Protocolos (y otros de las Series V y X del CCITT) fueron Normalizados antes de la propuesta de el Modelo OSI.

Esta propuesta, dio fuerza al desarrollo de Protocolos de Alto Nivel (Protocolos Capas 4 a 7) que son comunes a varias aplicaciones, esto es satisfactorio para las Capas de Transporte y Sesión.

Para los Protocolos de las Capas superiores a la de Sesión, se supone que próximamente, serán dedicados a la elaboración de Normas a nivel de representación y aplicación. La previsión, es de que una interconexión universal de sistemas abiertos.

En cuanto a las técnicas de especificación de Protocolos, la Norma ISO ha utilizado métodos informales sujetos a ambigüedades y a interpretaciones diferentes. Para resolver este problema, la Norma ISO, formó un Grupo de Trabajo para estudiar técnicas formales de especificación. Este grupo de trabajo, está actualmente investigando las técnicas de Ordenación Temporal y máquinas de estados finitos ampliadas, consideradas muy prometedoras.

II.6 Normalización Internacional de Protocolos de Transporte.

En el ámbito Internacional, los Organismos, *CCITT, ISO y ECMA;* están trabajando activamente en la Normalización de Protocolos de Transporte compatibles. En los Estados Unidos, la Normalización de Protocolos de Transporte se está produciendo en los tres Organismos principales de Normalización: **A**merican **N**ational **S**tandards **I**nstitute *(ANSI),* **N.B.S.**, y el **D**epartamento **de** Defensa (**DoD**).

La ANSI apoya el esfuerzo Internacional y NBS normalizó un Protocolo compatible con la propuesta de la ISO, el DoD adoptó un Protocolo incompatible llamado *"Transport Control Protocol" (TCP).*

Históricamente, el ímpetu del desarrollo de una Norma Internacional, para el Protocolo de Transporte fue dado por el Grupo de Estudios VIII de el CCITT, en Noviembre de 1980; con la Normalización de un nuevo servicio llamado *Teletexto*. El servicio Teletexto, está definido por las recomendaciones *F.200, S.60, S.61, S.62 y S.70.*

Esta última define el Servicio Básico de Transporte. Este Protocolo, a pesar de ser simple (no incluye multiplexado, control de flujo, detección ó recuperación de errores), tiene la gran ventaja de ofrecer los mismos servicios, independientemente del tipo de Red de Comunicación utilizada.

Además de su independencia, en cuanto al tipo de Red utilizada; la importancia del Protocolo S.70 se fundamenta en las siguientes consideraciones:

1.- S.70 es una Norma Internacional implantada por varios fabricantes de equipos de oficina.

2.- A pesar de que el Protocolo S.70, está orientado para el servicio Teletexto; su desarrollo, que utiliza la Norma y la filosofía del Modelo OSI; hace que sirva para otras aplicaciones. Es decir uno es de los Protocolos Comunes.

3.- El Protocolo S.70 fue incluido como subconjunto de otros Protocolos de Transporte.

En Junio de 1982, el Subcomité SC16, de la Norma ISO; aprobó una propuesta de una Norma Internacional para el Protocolo de Transporte. Este Protocolo consta de 5 clases de potencialidades diferentes (el Protocolo S.70 es idéntico a la clase 0, la clase más simple).

La inclusión de 5 clases permite que las aplicaciones menos críticas (por ejemplo, los Servicios Públicos de Telemática de el CCITT: Teletexto, Telefax y Videotexto), utilicen las clases de servicios mínimos (Clases 0 y 1), y para las aplicaciones más complejas (transferencia de archivos, dispositivos virtuales, transferencia y manipulación de tareas, gestión de Red), a las Clases 2, 3 y 4.

Con relación al trabajo que está siendo desarrollado actualmente en el área de Protocolos de Transporte, un Subgrupo del Working Party 4 del Grupo de Estudios VIII del CCITT; está evaluando aspectos de implantación del S.70, y está considerando alteraciones para atender a los requisitos de los otros servicios de Telemática de el CCITT.

El NBS de los Estados Unidos, adoptó como Protocolo de Transporte un conjunto de dos clases compatibles con el Protocolo de Transporte de la ISO. Hay una gran diferencia entre esos dos Protocolos, ya que el Protocolo de la ISO, fue especificado informalmente utilizando la Automatización de Estados Finitos y un Lenguaje de Especificación de Alto Nivel.

La Especificación consta de cerca de 70 páginas de descripción formal y 70 páginas de comentarios informales. La implantación de este Protocolo en Lenguaje "C" y bajo el Sistema Operativo UNIX, dieron lugar a 400 líneas de Código generadas automáticamente y a 6000 líneas generadas manualmente.

La experiencia de el NBS con la implantación semiautomática de Protocolos, ha sido muy positiva, asegurando un muy alto nivel de confianza en la implantación y un tiempo relativamente corto entre dos alteraciones cualesquiera en la especificación y en la generación de una nueva implantación.

II.7 Normalización Internacional de Protocolos de Sesión.

Las recomendaciones de el CCITT definiendo el servicio Teletexto en 1980, incluyeron el S.62, la primera Norma Internacional para el Protocolo de Sesión. No se trataba entonces, de un Protocolo común a varios servicios, sino de un Protocolo orientado a una única aplicación de Teletexto.

En 1981, ocurrió un cambio importante en el CCITT: El Grupo de Estudio XIV, responsable del servicio de Telefax, fue incorporado al Grupo de Estudio VIII que acababa de definir el servicio de Teletexto.

Como resultado de esta Organización, el Grupo de Estudio VIII modificó la recomendación S.62, y la adoptó para el servicio Telefax grupo 4. Este cambio del **S.62 para un Protocolo común permite la interconexión de terminales de** texto y terminales gráficas, además de ofrecer las otras ventajas de los Protocolos comunes.

Paralelamente al desarrollo del servicio Teletexto por el CCITT, el Organismo de Normalización Internacional ECMA, preparaba también un Protocolo de Sesión, la Norma ECMA-75. En Diciembre de 1981, la ISO (el CCITT se integró meses después) inició el desarrollo de un Protocolo común de Sesión, basado en las Normas ECMA-75 y S.62.

El retraso en Normalizar este Protocolo se debió a la dificultad de especificar un único Protocolo capaz de atender a todas las necesidades de las Capas de Presentación y Aplicación. La dificultad vino por la decisión sobre qué incluir en la Capa de Sesión y qué dejar en las Capas de Presentación y Aplicación. Finalmente, en 1983, la ISO terminó la propuesta de Norma Internacional para el Protocolo de Sesión.

El resultado es un Protocolo con 5 Clases, siendo 4 de ellas, semejantes a el ECMA-75 y una (incluida en Septiembre de 1982) basada en el S.62 de el CCITT.

Como el caso del Protocolo de Transporte; se proyectó que los Servicios Públicos de Telemática del CCITT utilizaran las clases básicas y las aplicaciones más complejas, se utilizaran las Clases más poderosas. Por consiguiente, esta expectativa no concreta si los servicios de Telemática pueden ser utilizados para aplicaciones más críticas, tales como las transacciones financieras. En el campo de las implantaciones, el **NBS** de los Estados Unidos adoptó el Protocolo **ISO/CCITT** y generó una implantación semiautomática a partir de una especificación formal de el Protocolo.

II.8 Normalización Internacional de Protocolos de Presentación y Aplicación.

Los Organismos Internacionales de Normalización, agrupan normalmente las dos Capas Superiores del Modelo OSI. (Santifaller, 1994).

Se seguirá el mismo procedimiento y se presentará una visión de los trabajos de Normalización en esta área, la más activa de las áreas de Normalización actualmente.

Los servicios ofrecidos por la Capa de Aplicación, pueden dividirse en dos subconjuntos: Servicios para la localización de recursos de la Red (Gestión de Red), y Servicios de Comunicación para el usuario.

La ISO, inició su trabajo en el área de Servicios de Gestión de la Red recientemente, y produjo un primer documento llamado *"OSI Management Framework"*, que deja entrever la complejidad del problema. Por ejemplo; existen varios problemas relacionados con la compatibilización de los Servicios necesarios para una Red Pública.

Aún más, el documento ni llega a definir cuáles son los Servicios que pueden ser controlados por el Modelo OSI, y cuáles por el Sistema Operativo Local del Usuario. Un aspecto interesante de *"OSI Management Framework"*, es que establece una Arquitectura que incluye interfases con todas las capas del Modelo OSI. A su vez, la propia definición de las Capas del Modelo OSI, sólo considera superficialmente el aspecto de Gestión de Red.

En resumen, el área de Normalización de Servicios de Gestión de Red, está solamente, comenzando a ser estudiada. En el área de Servicios para el usuario, los tres Organismos Internacionales principales de Normalización *(CCITT, ISO, ECMA)*, están desarrollando activamente Protocolos de Presentación/Aplicación; pero desgraciadamente, pueden surgir indicaciones de Protocolos Incompatibles.

El Grupo de Trabajo del SC16 de la ISO, está definiendo los Servicios de Presentación-Aplicación comunes a todas las aplicaciones. El resultado de este esfuerzo deber incluir un único Protocolo de Presentación y varios Protocolos de Aplicación. Los principales Protocolos de Presentación-Aplicación, que están surgiendo actualmente en la ISO son:

1.- **Transferencia de Archivos.**
2.- **Terminal Virtual.**
3.- **Transferencia y Manipulación de Tareas.**
4.- **Revisión de Mensajes.**
5.- **Formatos de Mensajes.**
6.- **Gestión de Red.**

7.- Gestión de Aplicaciones.

Los Protocolos de Revisión de Mensajes, son los más discutidos actualmente en el Subcomité SC18 de la ISO. Los rápidos avances de la Tecnología están abriendo la posibilidad de interconectar los diversos Servicios de Telemática (Teletexto, Telefax y Videotexto); y éstos a los *Servicios Electrónicos de Mensajes Basados en Ordenadores (CBMS).*

Se resalta que la adopción y el uso de un conjunto pequeño de Protocolos Normalizados, permitirá la formación de un gran Mercado Internacional de Mensajes en el cual los usuarios de Sistemas Privados y Públicos de CBMS, Teletexto, Telefax, Videotexto y Telex podrán comunicarse en beneficio de todos.

II.8.1.- TeleTexto.

En Noviembre de 1980, en la VII Asamblea Plenaria, el CCITT aprobó las Normas *F.200, S.60, S.61, S.62 y S.70,* definiendo un nuevo Servicio de Telecomunicaciones: TeleTexto. Este Servicio ya se está implantando en varios Países del mundo. El TeleTexto, puede ser visto como un Servicio avanzado de Telex, que incluye la preparación, el almacenamiento y el envío de documentos.

Las diferencias básicas entre el Telex y el TeleTexto; son que éste incluye un mejor formato de documentos, un Alfabeto más amplio (309 caracteres), y una transmisión más rápida (2400 bps), a pesar de mantener la característica de transmisión directa entre los dos equipos. En este sentido el servicio TeleTexto, es un avance en la implantación de Servicios para la Automatización de oficinas, combinando comunicaciones y procesamiento de texto.

El TeleTexto, ofrece la capacidad de procesar el texto para definir su apariencia final, pero sin incluir el procesamiento sistemático de su contenido. Aunque los Protocolos de TeleTexto, han sido desarrollados para un único Servicio, su aplicación no está restringida solamente a esta área.

En realidad, los Protocolos de TeleTexto, pueden ser aplicados a varios servicios del Tipo *"Batch"* (no interactivos), tales como el TeleFax, transferencia de archivos, etcétera. Por esta razón, los Protocolos de TeleTexto, están sirviendo como punto de partida para el desarrollo de Protocolos comunes a todos los Servicios de Telemática.

II.8.2 TeleFax.

La Organización Internacional con mayor actuación en la definición de un Servicio Internacional de TeleFax; es el CCITT. En Noviembre de 1980, el Grupo de Estudio XIV (hoy mezclado con el Grupo VIII), adoptó las Normas para TeleFax, Grupo 3 (las recomendaciones son la T.30 y la T.31). En Octubre de 1981, el CCITT inició estudios en el área del TeleFax (Grupo 4), un Servicio semejante al TeleFax Digital (Grupo 3), pero orientado a Redes de Datos. Las decisiones iniciales de el CCITT fueron definir los Servicios del TeleFax, Grupo 4, a partir de los Servicios de el Grupo 3, pero basándose en los procedimientos de control de el Protocolo S.62 del Servicio de TeleTexto.

Esto tiene la gran ventaja de promover una estructura de Sesión común a varios Servicios, haciendo posible la intercomunicación de éstos, en particular en el modo de operación mixto del Servicio de TeleTexto.

II.8.3 VideoTexto.

El VideoTexto, es un servicio interactivo de recuperación de información que incluye la posibilidad de representar informaciones gráficas. La importancia de Normalización de este Servicio puede ser medida, si se considera que a finales de la década de 1980, una gran parte de la información procesada existente en el mundo estará disponible en Bancos de Datos de VideoTexto.

En 1978, la "British Post Office" **(BPO)**, sometió su Sistema de VideoTexto *(Prestel)* a el CCITT (el Organismo más activo en la Normalización Internacional del VideoTexto) para la Normalización. En el mismo año el Gobierno Francés también sometió su Sistema *(Antiope)* a la Normalización del CCITT. Estas dos propuestas son funcionalmente semejantes, pero utilizan técnicas diferentes para la Codificación de Información.

En 1979, fue el Gobierno Canadiense el que sometió su sistema *(Teledion)* a el CCITT para la Normalización. El resultado fue que en Noviembre de 1980, el *"Working Party 5"* del Grupo de Estudio I del CCITT adoptó la Recomendación F.300, que incluía los tres sistemas incompatibles. Enseguida, la AT&T (American Telephone and Telegraph), anunció en Abril de 1981 la adopción de una ampliación del "Teledion" Canadiense, llamada "Presentation Level Protocol" **(PLP)**.

Paralelamente, los Países Europeos llegaron a un acuerdo sobre un único Sistema de VideoTexto basado en las propuestas del BPO y del Gobierno Francés (propuesta CEPT).

Finalmente, en Octubre de 1982, la ANSI de los Estados Unidos y la "Canadian Standards Association" *(CSA)*, adoptaron la propuesta PLP de la AT&T que fue denominada *"North American Presentation Level Protocol Syntax" (NAPLPS)*, para VideoTexto y TeleTexto. Actualmente, la situación en el ámbito Internacional, es que habiendo recibido las propuestas CEPT, NAPLPS y CAPTAIN (del Japón); el CCITT está revisando activamente dichas formulaciones y lo había sido alcanzado.

Hay que resaltar aquí que la previsión es de que el NAPLPS debe ser incluido en alguna forma en la Norma Internacional, por tener las siguientes ventajas sobre la propuesta CEPT:

1.- El NAPLPS es independiente de la terminal de VideoTexto utilizada, mientras que la propuesta CEPT depende de la terminal.

2.- IBM anunció que incluirá NAPLPS en sus Productos.

3.- Ya fueron lanzados al mercado varios paquetes de Programación *("Software")* convirtiendo a Ordenadores en Terminales de VideoTexto interactivas que utilizan la Norma NAPLPS.

II.8.4 CBMS.

Los Servicios Electrónicos de Mensajes Basados en Ordenadores *(**CBMS**)*; pueden ser vistos como una ampliación del TeleTexto, donde el Procesamiento semántico del mensaje es realizado por el remitente ó por el destinatario, donde la modalidad de transmisión puede ser de almacenamiento ó reenvío, y donde la información enviada puede ser cualquier información binaria. La Normalización de Servicios y Protocolos del CBMS constituye hoy, el área más activa de los Organismos CCITT, ISO y ECMA.

Desgraciadamente, debido a los objetivos y requisitos diferentes de estos Organismos, las formas de abordarlos parecen ser divergentes, lo que contraria el objetivo de que sean Normas Internacionales compatibles.

Por tanto; el objetivo común de los tres Organismos es obtener un grado de compatibilidad con los Servicios de Telemática, formando un Sistema Global de Transferencia de Mensajes.

Este objetivo es de gran importancia, ya que, a finales de la década de 1980, la mayoría de los documentos transferidos por el Comercio y por el Gobierno deberán utilizar medios electrónicos basados en estos Servicios. Existen varios problemas para alcanzar la compatibilidad de Telemática y CBMS, se destacan:

1.- Formato de Datos.- El TeleTexto utiliza texto, el CPMS utiliza información binaria sin restricciones.

2.- Protocolos.- Será necesaria una compuerta para hacer compatibles las modalidades de transmisión directa y "almacenamiento y re-envío".

3.- Direccionamiento.- El TeleTexto utiliza direcciones; el CBMS utiliza nombres.

4.- Servicios.- Ciertos servicios del CBMS son muy complejos para ser implantados en un equipo electrónico de TeleTexto. El problema principal, es compatibilizar los servicios para las dos modalidades de transmisión.

Una vez Normalizado el Servicio CBMS, se piensa que será utilizado en aplicaciones que no estén normalmente asociadas a la Comunicación de Mensajes, y estas pueden ser:

1.- Comunicación de Mensajes que incluyen Texto, Gráficos y Voz Digitalizada.
2.- Acceso a Bancos de Datos con el Procesamiento Automático de Mensajes y la Generación de Respuestas.
3.- Distribución de Documentos.
4.- Transferencia de Archivos.
5.- Procesamiento de Transacciones.

Por lo tanto el CBMS debe proveer una estructura de aplicación general para la transferencia de informaciones arbitrarias.

CAPÍTULO III.

EQUIPO DE CONECTIVIDAD PARA REDES DE ORDENADORES.

III.1 Introducción.

Cuando se quiere realizar una ampliación de la Red que fue diseñada idealmente con ciertas características o de determinado tamaño se encuentra con la problemática que con el paso del tiempo la Red resulta pequeña y surge la necesidad de agregarle elementos para que siga siendo funcional aunque también surge la necesidad de interconectar la Red con otra pero que es de características diferentes a la que se tiene, para ello se han desarrollado dispositivos que nos permitan realizar la ampliación de Redes de Área Local (LAN) Remotas ó Sistemas diferentes, los "Bridges" y "Routers" son la mejor solución (Frank y Frisch, 1991).

Observaremos los conceptos de los dispositivos de tecnología de una forma general para tener un conocimiento de los elementos que hay en el mercado para interconectar las Redes y ver los rangos que nos proporcionan estos elementos disponibles para poder realizar la expansión, así como muchos productos específicos para la interconexión.

Entre estos dispositivos para interconectar las Redes de Ordenadores de Área Local podemos contar al Ruteador que es utilizado para conectar Sistemas que son físicamente separados ó que son de topología ó Arquitectura diferente, el Bridge permite a los nodos, en los dos Sistemas, comunicarse uno con el otro a través de Protocolos compartidos. Todos los Bridges y Ruteadores tienen un propósito común, conectar dos Sistemas para el intercambio de información.

El Puente o Bridge se puede encontrar en dos tipos: Internos y Externos, la diferencia es solamente física por que los dos tipos trabajan de igual manera. Es importante señalar que la mayoría de las Plataformas de "Bridges" pueden también sostener mecanismos para "Gateways", (Floyd, S. y Jacobson, 1993).

El desarrollo tecnológico en el ámbito de la Computación conforme avanza el tiempo es más vertiginoso su avance haciendo provocando qué al surgimiento de un dispositivo en seis meses o más aparezca el mismo dispositivo con mas cualidades por ejemplo la reducción de tamaño, mayor velocidad, el doble de su funcionamiento o conexiones, etcétera.

Como los Sistemas crecen y evolucionan rápidamente, cabe la necesidad de interconexión con otras Redes distintas. Esto se está convirtiendo cada día en algo más común, el resultado; "Sistemas de Información Distribuidos".

Al crecer la popularidad de estos Sistemas basados en Redes de Ordenadores, se encontró con la necesidad de normalizar estos sistemas para que no hubiera tanta diversidad y sí la mayor compatibilidad entre el diseño y construcción de equipos de Ordenadores de distintos fabricantes.

Por tal motivo se creo **La Organización Internacional de Normas ISO (International Standard Organization)**; que fue uno de los primeros Organismos que se preocupo de resolver este problema, creando un Modelo de Interconexión de Sistemas Abiertos ("heterogéneos"), el cual se conoce como Modelo **OSI (Open System Interconection)**.

El objetivo fundamental de este sistema es la de facilitar las comunicaciones entre Ordenadores a través de recomendaciones de Diseño a Fabricantes de la Arquitectura de Sistemas, de Paquetes y Programas tanto en el Hardware como en el Software, teniendo como consecuencia las siguientes ventajas:

- Independencia del fabricante.- Con el desarrollo de la compatibilidad de los Ordenadores y dispositivos; el usuario puede recurrir a cualquier otro fabricante.

- Se puede encontrar compatibilidad completa con los nuevos equipos y el Software que hay en el Mercado.

- Se puede realizar una expansión de la Red más rápidamente.

El Modelo OSI consta de 7 niveles, cada nivel es independiente y agrupa un conjunto específico de funciones realizadas por los elementos del Ordenador, colaborando además con los demás niveles de forma jerárquica y coordinada para lograr la comunicación eficiente de datos entre Ordenadores.

En 1977 la Organización I.S.O creó un Sub-Comité para desarrollar comunicaciones Estándares de datos que fomentan la interoperación entre vendedores, y la accesibilidad universal. El resultado de estos esfuerzos es el Modelo de referencia de Sistema Abierto de Interconexión (OSI).

El Modelo OSI sirve como una Norma funcional para comunicaciones y, por consiguiente, no especifica alguna comunicación Estándar para que realice estas tareas; sin embargo, muchos Estándares y Protocolos cumplen con la Norma del Modelo OSI (International Organization for Standarization, 1988a), este modelo utiliza la estrategia **"divide y vencerás"**. ya que cada capa ejecuta funciones específicas; éstas y sus funciones fueron basadas sobre divisiones de subtareas. La comunicación entre las capas es la Capa **"N"** usa los Servicios de la Capa **"N-1"**, y provee Servicios a la capa **"N+1"**.

Las Unidades de Información son llamadas por varios nombres, dependiendo del Modelo de Capa que esté siendo discutido

- Capa Física se refiere a los **Bits**.
- Capa de Enlace de Datos, los grupos lógicos de información son llamados **Frames**.
- Capa de Red frecuentemente se habla de los **Datagrams**.
- Capa de Transporte las mismas unidades básicas son llamadas **Segmentos**.
- Capas de Aplicación son comúnmente llamadas **"Mensajes"**.

El Modelo por sí mismo no causa Comunicación en la Red. La Comunicación de la Red requiere de un Protocolo. El Protocolo lo definiremos como llamadas de especificación para una implantación particular de una ó más capas del Modelo OSI.

III.2 Elementos para la Conectividad de Redes de Área Local (LAN).

III.2.1 MODEM (*Modulador*-*Demodulador*).

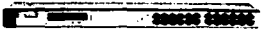
Este dispositivo transforma las señales binarias que proporciona el ordenador en señal analógica para que esta sea enviada por el cable telefónico hasta otro punto de la red y al llegar a su destino se haga la conversión inversa analógica- digital. Es un dispositivo que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas, esta comunicación se realiza a través de la modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras, las señales ana'ógicas se convierten en digitales y viceversa.

Los módems pueden ser externos o internos dependiendo de su ubicación física en la red. Entre los mayores fabricantes tenemos a 3COM, AT&T, Motorola, US Robotics y NEC.

La transmisión por Módem se divide en tres tipos:

SIMPLEX: Permite enviar información solo en un sentido.
HALF DUPLEX: Permite enviar información en ambos sentidos pero no a la misma vez.
FULL DUPLEX: Permite enviar información en ambos sentidos simultáneamente.

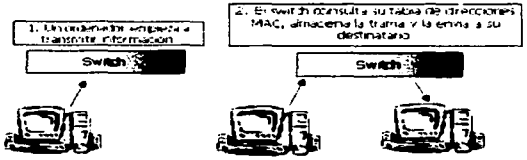
III.2.2 SWITCH



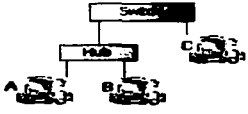
switch hp 101360

switch NP-CNSH1600

Cuando se habla de un Conmutador (*"Switch"*) se hará refiriéndose a uno de nivel 2, es decir, perteneciente a la capa "Enlace de datos". Normalmente un switch de este tipo no tiene ningún tipo de gestión, es decir, no se puede acceder a él. Sólo algunos switch tienen algún tipo de gestión pero suele ser algo muy simple.



1 - El "switch" conoce los ordenadores que tiene conectados a cada uno de sus puertos (enchufes). Cuando en la especificación del un "switch" leemos algo como "8k MAC address table" se refiere a la memoria que el "switch" destina a almacenar las direcciones.
Un "switch" cuando se enchufa no conoce las direcciones de los ordenadores de sus puertos, las aprende a medida que circula información a través de él. Con 8k hay más que suficiente. Por cierto, cuando un "switch" no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un HUB ("Flooding", inundación). Cuando hay más de un ordenador conectado a un puerto de un "switch" este aprende sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama filtrado.



El tráfico entre A y B no llega a C. Como decía, esto es el filtrado. Las colisiones que se producen entre A y B tampoco afectan a C. A cada parte de una red separada por un "switch" se le llama segmento.

2 - El "switch" almacena la trama antes de reenviarla. A este método se llama "store & forward", es decir "almacenar y enviar". Hay otros métodos como por ejemplo "Cut-through" que consiste en recibir los 6 primeros bytes de una trama que contienen la dirección MAC y a partir de aquí ya empezar a enviar al destinatario. "Cut-through" no permite descartar paquetes defectuosos. Un "switch" de tipo "store & forward" controla el CRC de las tramas para comprobar que no tengan error, en caso de ser una trama defectuosa la descarta y ahorra tráfico innecesario. El "store & forward" también permite adaptar velocidades de distintos dispositivos de una forma más cómoda, ya que la memoria interna del "switch" sirve de "**buffer**". Obviamente si se envía mucha información de un dispositivo rápido a otro lento otra capa superior se encargará de reducir la velocidad.

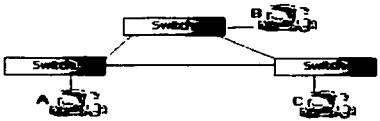
Finalmente comentar que hay otro método llamado "Fragment-free" que consiste en recibir los primeros 64 bytes de una trama porque es en estos donde se producen la mayoría de colisiones y errores. Así pues cuando vemos que un "switch" tiene 512KB de RAM es para realizar el "store & forward". Esta RAM suele estar compartida entre todos los puertos, aunque hay modelos que dedican un trozo a cada puerto.

3 - Un "switch" moderno también suele tener lo que se llama "Auto-Negotation", es decir, negocia con los dispositivos que se conectan a él la velocidad de funcionamiento de 10 Mbps ó 100 Mbps, así como si se funcionara en modo "full-duplex" o "half-duplex". "Full-duplex" se refiere a que el dispositivo es capaz de enviar y recibir información de forma simultánea, "half-duplex" por otro lado sólo permite enviar o recibir información, pero no a la vez.

4 - Velocidad de proceso: todo lo anterior explicado requiere que el "switch" tenga un procesador y claro, debe ser lo más rápido posible. También hay un parámetro conocido como "back-plane" o plano trasero que define el ancho de banda máximo que soporta un "switch". El "back plane" dependerá del procesador, del número de tramas que sea capaz de procesar. Si hacemos números vemos lo siguiente: 100megabits x 2 (cada puerto puede enviar 100 Mb y enviar 100 más en modo "full-duplex") x 8 puertos = 1,6 Gb. Así pues, un "switch" de 8 puertos debe tener un "back-plane" de 1,6 Gb para enviar sin problemas.

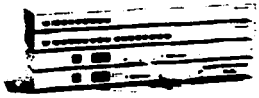
5 - Si un nodo puede tener varias rutas alternativas para llegar a otro un "switch" tiene problemas para aprender su dirección ya que aparecerá en dos de sus entradas. A esto se le llama "loop" y suele haber una lucecita destinada a eso delante de los "switch". El protocolo de Spanning Tree Protocol IEEE 802.1d

se encarga de solucionar este problema, aunque los "switch" domésticos no suelen tenerlo.



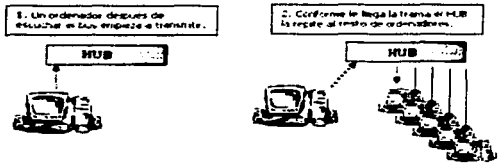
Existen "switch" de nivel 3, se diferencian de los routers en que su hardware es más especifico y diseñado especialmente para llevar a cabo esa función.

III.2.3 HUB



Hub ampliable 100 Mbps
Series SP682/SP685

Un HUB tal como dice su nombre es un concentrador. Simplemente une conexiones y no altera las tramas que le llegan.



1 - El HUB envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el HUB envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

2 - Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea que otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

3 - Un HUB funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el HUB no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mb le trasmitiera a otro de 10 Mb algo se perdería el mensaje.
En el caso del ADSL los routers suelen funcionar a 10 Mb, si lo conectamos a nuestra red casera, toda la red funcionará a 10, aunque nuestras tarjetas sean 10/100.

4 - Un HUB es un dispositivo simple, esto influye en dos características. El precio es accesible, un HUB casi no añade ningún retardo a los mensajes.

Por lo tanto un Hub es un integrador para diversos tipos de cables y de arquitectura que permite estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etcétera.

La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos. Generalmente te indican la actividad de la red, velocidad y puertos involucrados. Su funcionamiento es simple, se lleva hasta el un cable con la señal a transmitir y desde el se ramifican mas señales hacia otros nodos o puertos. Entre los fabricantes que producen gran variedad de estos equipos se encuentran las empresas 3COM y Cisco

III.2.4 REPETIDORES.

"Los Repetidores extienden, típicamente, un segmento físico de una Red de Área Local (LAN) más allá de la distancia máxima normal. Ethernet y Token-Ring contienen en su Topología especificaciones para Repetidores.

El estándar para el Repetidor es un dispositivo "no inteligente"; esto indica que su función solamente es repetir el tráfico que recibe. Trabaja como un dispositivo transparente para el enlace de información y los niveles más altos del Modelo OSI". (Frank, 1991).

Ethernet con cable telefónico o par trenzado, es un ejemplo de Repetidores que actúan con un Repetidor multipuerto que trata a cada UTP como un segmento de Red distinto. Hay un número de medidas de Repetidores que se pueden tomar para centralizar un equipo, como el concentrador, que tiene conexiones inteligentes únicas a cada conexión de Usuario.

Son Dispositivos Electrónicos que solamente regeneran o repiten Paquetes de Datos (señales eléctricas, en realidad) entre segmentos de cable. Su función principal es la de incrementar la extensión física de la Red. A los Repetidores se les puede ubicar en el Nivel 1 ó Capa Física de el Modelo OSI.

Los Repetidores cuentan además con un nivel de tolerancia de errores de las señales eléctricas recibidas, regenerando o repitiendo la señal nuevamente, pero sin las fallas de recepción, por lo que los problemas en un segmento del cable no afectan a los demás segmentos. Sin embargo, una gran desventaja de los Repetidores, es que regeneran todas las señales que llegan sin saber si son o no necesarias en el otro segmento del cable.

III.2.5 BRIDGES.

Los "Bridges" o Puentes según González (1999), están diseñados para la interco-nexión de Redes en la Capa de Información (la cual incluye el Control de Acceso a Medios (MAC) y el Control de Enlace Lógico (LLC)).

Bridge Ethernet de secuencia directa de la serie Cisco Aironet 340

Principalmente, la Capa de Enlace de Información ó nivel 2 está incorporada en la Arquitectura de un NIC específico. Esto es, que el Programa que controla a los Controles de Acceso a Medios (MAC (y el Control de Enlace Lógico (LLC))), es de una "tarjeta" y no están en los manejadores de dispositivos de la Estación de Trabajo. Son transparentes para IPX/SPX, NetBios y otras capas de Redes y Protocolos más altos.

Es un aparato necesario si queremos conectar varias redes locales dentro de un edificio porque nos interese, administralas por separado, o porque en algún momento se quiere aislar una red de otra. Además, si se cuenta con una red Ethernet cuya longitud de cableado va a superar los 2.5Km entre cliente y servidor, podemos poner un puente y conseguiremos hasta 5Km de distancia.

Los Puentes ("Bridges") conectan a las Redes de Área Local a Topologías y Protocolos similares; ejemplo, Ethernet con Ethernet, Token-Ring con Token-Ring. Pueden también ser utilizados para eslabonar tipos de cables diferentes, como el caso del Cable Coaxial de Ethernet con UTP de Ethernet, ó con Token-Ring de Fibra Óptica.

Estos equipos se utilizan asimismo para interconectar segmentos de red, (amplia una red que ha llegado a su máximo, ya sea por distancia o por el número de equipos) y se utilizan cuando el tráfico no es excesivamente alto en las redes pero interesa aislar las colisiones que se produzcan en los segmentos interconectados entre sí.

Hay tres tipos de Puentes: ***Buffered, Filtering y Learning.***

1.- Puente Buffered.

Este Puente aísla segmentos de Redes de Área Local (LAN) conectadas entre sí. Las colisiones no se propagan a través de segmentos.

2.- **Puente Filtering.**

Este tipo de Puente puede filtrar tipos de paquetes mientras que TCP/IP transmite información.

3.- **Puente Learning**

Este Puente escucha a todas las transmisiones en segmentos. Todas las direcciones de la información están cuidadosamente almacenadas, para posteriormente ser mandadas a su lugar de origen.

Los Puentes son "inteligentes". Aprenden las direcciones de destino del tráfico que pasa por ellos y lo dirigen a su destino, es decir que cuando un segmento físico de Red tiene tráfico en exceso y su rendimiento está comenzando a degradarse, se le puede dividir en dos segmentos físicos con un Puente.

Éste dirige el tránsito a su destino final y limita el que no debe pasar por un determinado segmento. Los Puentes usan un proceso de aprendizaje, filtrado y envío para mantener el tráfico dentro del segmento físico al que pertenece. No filtra los broadcasts, que son paquetes genéricos que lanzan los equipos a la red para que algún otro les responda, aunque puede impedir el paso de determinados tipos de broadcast.
Esto es típico para solicitar las cargas de software, por ejemplo. Por tanto, al interconectar segmentos de red con bridges, puede tener problemas de tormentas de broadcasts, de saturación del puente por sobrecarga de tráfico, etc. El bridge generalmente aísla las colisiones, **pero no filtran protocolos.**

Debido a que los Puentes aprenden direcciones, examinan Paquetes y toman decisiones de envío, con frecuencia, su funcionamiento se degrada conforme el tráfico aumenta, de hecho, esta posibilidad debe considerarse si se plantea la utilización de Puentes. Sin embargo, en general, en ambiente de Protocolos mixtos, los Puentes son muy útiles.

Cuando de quiere conectar una Red de Área Local (LAN) con otra Red de Área Local (LAN) para formar Inter-Redes, se recurre a equipos de comunicación conocidos como *"Bridges"*, que hacen la función de puente entre las dos Redes. La mayoría de estos equipos operan entre Redes de Topología distinta (una ARCNET con una Ethernet por ejemplo), pero también pueden usarse en Redes de la misma Tecnología y Topología.

Los "Bridges", regulan el tráfico de información en la Red, filtrando los Paquetes de Datos de acuerdo a la información contenida en el campo de dirección del paquete. Cuando el paquete de datos va dirigido a una de las Estaciones de Trabajo locales, el "Bridge" lo deja continuar con su trayectoria.

Sin embargo, cuando el destinatario es un usuario de la otra Red, el "Bridge" toma el Paquete y lo envía optimizando así el tráfico local de información. Algunos "Bridges" más complejos toman en cuenta, no sólo la dirección del Paquete, sino también su tamaño y su Protocolo. Los "Bridges", funcionan independientemente del Protocolo de Transporte usado por la Red: TCP/IP ó IPX.

III.2.6 GATEWAYS.

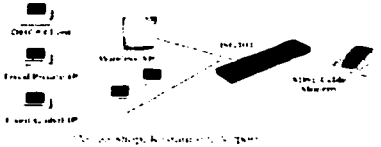
Internet Subscriber Gateway
Está desarrollado para ofrecer los servicios de banda ancha que ofrecen acceso de alta velocidad a Internet, a cualquier equipo que se conecte a el con cualquier IP. El ISG-101 inmediatamente reconoce los nuevos usuarios en la red, sin importar la IP que estén usando en sus equipos: cualquier IP sea fija o dinámica, y redirecciona la petición de su Browser a la página propietaria Web. Con esto se consigue que ningún usuario tenga que modificar su configuración de red para acceder directamente a Internet, una verdadera solución "plug and play"

Huitema (1995) dice que Los **Gateways** operan en las tres capas superiores de el Modelo OSI (Sesión, Presentación y Aplicación). Ofreciendo el mejor método para conectar segmentos de Red y Redes a **Mainframes**. El **Gateway** es utilizado cuando se tiene que interconectar sistemas que se construyeron totalmente con base en diferentes Arquitecturas de Comunicación; por ejemplo para interconectar TCP/IP a un **Mainframes SNA** (Arquitectura de Sistemas de Redes: **S**ystem **N**etwork **A**rchitecture en ingles). En este caso se designa a una de los Ordenadores de la Red, para colocar la tarjeta que haga la operación de "Gateway", y los demás Ordenadores, se comunicarán a los *"Host"* del *"Mainframe"* a través de este Ordenador. Como las dos Arquitecturas no tienen nada en común el *"Gateway"* debe traducir todos los datos que se transfieren entre los dos sistemas interconectados.

Se utiliza el **Gateway** para conectar un sistema remoto como una Red Pública de Datos con conmutación de Paquetes X.25 (método eficiente de empaquetar datos y enviarlos remotamente).

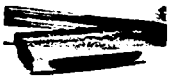
En cada extremo de la Red, el **Gateway** ofrece la conversión del Protocolo de los segmentos de la Red conectados con el otro lado. no proporcionan enrutamiento de paquetes dentro de un segmento de Red, solo entregan sus paquetes de datos de tal forma que los segmentos puedan leerlos. Cuando reciben paquetes del segmento, los traducen y enrutan al **Gateway** en el otro extremo, donde los paquetes vuelven al segmento de Red en el extremo opuesto.

Por lo tanto, los **Gateway**, se utilizan para conectar Ordenadores de diferente Arquitectura, ya que funcionan como convertidores de Protocolos. Dependiendo del nivel de incompatibilidad los "Gateways", se ubican en los Niveles 4 al 7 de el Modelo OSI.



III.2.7 Ruteadores, (Router's).

Router RDSI DI-206



Cyclades-NL1000 VPN Router
Ruteador de Acceso

Ruteador VPN de cable/DSL EtherFast®
con un switch 10/100 de 4 puertos

Encaminadores en español sirven para conectar redes entre sí, enrutan los paquetes de información entre sus distintos puertos. Los Ruteadores son dispositivos de interconexión que operan en la Capa de la Red de nivel 3 dentro del Modelo OSI. Los Ruteadores soportan Protocolos específicos, tales como TCP/IP, IPX/SPX, DECnet y otros.

Este dispositivo es normalmente "ciego" para todos los Protocolos que específicamente no soporten dicho dispositivo. Sin embargo, tienen que estar configurados para soportar diferentes protocolos de red por lo que su rapidez disminuye. Ellos mismos confeccionan una tabla con la topología de la red, que se llama de algoritmos de encaminamiento. Si el router es inteligente los aprende el sólo, y si no, hay que programárselos.

Algunos Ruteadores, como los que ofrece Proteon Inc. y Cisco System Inc. pueden ser Programados de modo que pueden sostener al mismo tiempo Protocolos múltiples. (Huitema, 1995).

conexión a Internet

Algunos Ruteadores como la Serie *Proteon 42XX* y *Schneider & Kock* y los de la Compañía SK-Net; tienen la virtud de encapsular información de un tipo de Protocolo dentro de otro tipo. Esta característica es utilizada por varias Universidades cuya columna de comunicación entre Campus es TCP/IP.

Los router pueden filtrar protocolos y direcciones a la vez. Los equipos de la red saben que existe un router y le envían los paquetes directamente a él cuando se trate de equipos en otro segmento.
Además los routers pueden interconectar redes distintas entre sí; eligen el mejor camino para enviar la información, balancean tráfico entre líneas, etcétera.

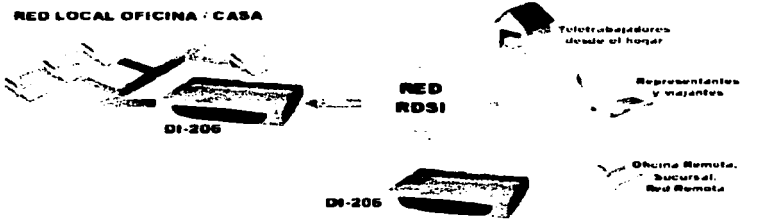
Trabaja con tablas de encaminamiento o enrutado con la información que generan los protocolos, deciden si hay que enviar un paquete o no, deciden cual es la mejor ruta para enviar un paquete y la información de un equipo a otro, pueden contener filtros a distintos niveles, etcétera.

Poseen una entrada con múltiples conexiones a segmentos remotos, garantizan la fiabilidad de los datos y permiten un mayor control del tráfico de la red. Su método de funcionamiento es el encapsulado de paquetes.

Para interconectar un nuevo segmento a nuestra red, sólo hace falta instalar un router que proporcionará los enlaces con todos los elementos conectados.

En conclusión, los Ruteadores, sirven para conectar Redes de Área Local (LAN) con diferentes Topologías ó Protocolos en un segmento real de Red.

conexiones de Redes de Ordenadores Remotas



acceso de Usuarios Remotos

Router RDSI DI-206
caracteristicas

- Acepta de forma simultánea dos usuarios remotos
- Lista de usuarios interna configurable, hasta 8 usuarios máximo
- Protocolo RADIUS para listas y servidores externos
- Acceso de un usuario remoto, bien en modo 64K, 128K o 128K BOD

- Protección de la conexión con nombre de usuario y clave opcional
- Tiempo de conexión máximo configurable para cada usuario
- Tiempo de desconexión por inactividad programable

Funcionamiento individual o simultáneo con las funciones de conexión a Internet y conexión de redes remotas

III.3 El Modelo O. S. I.
(International Organization for Standarization 1987a).

III.3.1 Capa FÍSICA (Physical).

La Capa Física define el mecanismo y las especificaciones eléctricas del medio de la Red y la interfase de la Arquitectura de Sistemas de la Red (Hardware), cómo están conectados a otro y cómo los datos son colocados y retirados del medio de la Red.

Las especificaciones de la Capa Física incluye el número y las funciones de las múltiples terminales en el conector de la Red, como los "1" y los "0" son enviados vía una señal eléctrica ó electromagnética sobre el medio de la Red, qué tipos de cables pueden ser utilizados y otros beneficios.Se establecen las características mecánicas y eléctricas que deben reunir los cables y dispositivos encargados de transportar los bits de información.

Las funciones principales de la Capa Física son:

- Permitir la compatibilidad entre los diferentes tipos de conectores existentes.
- Definir las funciones que van a realizar cada uno de los pines de los conectores.
- Establecer el tipo de cableado que se debe usar en la red.
- Determinar la codificación, el voltaje de las señales y la duración de los pulsos eléctricos.
- Coordinar la modulación de las señales, si es necesario.
- Amplificar y retemporizar las señales en su viaje a través de los medios.

Por lo tanto, incluye todos y cada uno de los elementos de red encargados de transformar los trenes de bits de las tramas en señales aptas de ser transportadas por los medios físicos y viceversa, los medios físicos en sí (cableado de cualquier tipo), los

diferentes conectores de unión entre cables y dispositivos de red y los propios dispositivos que trabajan a nivel de impulsos y señales eléctricas (repetidores, hubs, etcétera).

III.3.2 Capa de ENLACE DE DATOS (Data Link).

La Capa de Enlace de Datos organiza la Capa Física de los datos binarios ("0" y "1" lógicos) en estructuras. Una estructura es una serie continua de datos con un significado lógico independiente. Esto es un sinónimo con el concepto de un telegrama.

Esta capa detecta errores, controla el flujo de datos e identifica Ordenadores particulares sobre la Red. Al igual que las demás Capas, añade su propio control de información al frente del Paquete de Datos. Esta información puede incluir una dirección origen y una destino, información acerca de la longitud de la estructura y una indicación de la capa superior de Protocolo implicada. El intercambio de información entre dos Ordenadores se lleva a cabo mediante grupos pequeños de bits ó Paquetes de Información, estructurados de acuerdo a un formato específico.

El nivel de enlace se encarga de garantizar la transferencia de estos paquetes a la Red de manera confiable así como también, cada Paquete debe cumplir con el formato estándar HDLC *("High Level Data Link Control")* este establece que los paquetes están constituidos por una bandera de inicio, un campo de control, un campo con la dirección del destinatario, un campo para la transmisión transmitida, un campo para la dirección de errores y una bandera que indique el final del paquete.

III.3.3.- Capa DE LA RED (Network).

Su principal objetivo de enrutar la información a través de la Red fingiendo múltiples segmentos de ésta. La Capa de la Red elabora esto examinando la dirección de destino de la Capa de la Red y enviando el paquete al siguiente punto de paso en la Red interna.

El siguiente punto de paso puede ser determinado mediante el cálculo del tiempo real del mejor camino al último destino, ó puede ser simplemente buscado en una tabla estática. En cualquier caso, el paquete se moverá salto por salto a través de entre las Redes del nodo de la tarjeta.

Se encarga de transportar los paquetes de datos a través de la Red e interpretar la información proporcionada por éstas para llevar cada paquete hasta su destinatario y detectar y corregir los errores de transmisión. Prepara la información para su envío en forma de trenes de bits, sucesiones de ceros y unos binarios que contienen los datos a transmitir junto a las cabeceras necesarias para el funcionamiento correcto de los diferentes protocolos

1. **Codificación NRZ**: o de código sin retorno a cero es la codificación más sencilla. Se caracteriza por una señal alta y una señal baja (a menudo +5 o +3,3 V para 1 binario y 0 V para 0 binario). En el caso de las fibras ópticas, el 1 binario puede ser un LED o una luz láser brillante, y el 0 binario oscuro o sin luz. En el caso de las redes inalámbricas, el 1 binario puede significar que hay una onda portadora y el 0 binario que no hay ninguna portadora.

2. **Codificación de Manchester**: los bits se codifican como transiciones así la codificación Manchester da como resultado que los 0 se codifiquen como una transición de baja a alta y que el 1 se codifique como una transición de alta a baja. Dado que tanto los 0 como los 1 dan como resultado una transición en la señal, el reloj se puede recuperar de forma eficaz en el receptor.

III.3.4.- Capa de TRANSPORTE (Transport).

Funcionando en el corazón de el Modelo OSI, la Capa de Transporte asegura la entrega puntual de datos, La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente. En este papel la Capa de Transporte a menudo es remunerada por falta de seguridad en las capas más bajas. El término puntual no implica que todos los datos sean entregados. Si los cables de la Red se rompen, por ejemplo, la Capa de Transporte no podrá entregar los datos puntualmente.

Agrupa el conjunto de procedimientos encargados de llevar a cabo la transferencia transparente de los datos. Esta es a menudo implantada por una parte del Sistema Operativo, mientras que la Capa de Red es implantada por un controlador de Entrada/Salida (I/O).

III.3.5.- Capa DE SESIÓN (Session).

Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado, añade el control de mecanismos a los datos que establece, mantiene, sincroniza y maneja el diálogo entre las aplicaciones de comunicación. También maneja problemas en las Capas más altas, como el inadecuado espacio en disco y la falta de papel en la impresora.

El Nivel de Sesión es el responsable de establecer, controlar y sincronizar los procesos del Nivel de Aplicación Permitiendo a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).

Una conexión entre usuario es llamada una *"Sesión"*. Para establecer una Sesión, el usuario debe indicar la dirección del dispositivo al que se quiere conectar. Las direcciones de Sesión son proporcionadas por el usuario ó por el Programa de Aplicación, mientras que las direcciones de Transporte son proporcionadas por los Ordenadores de la Red.

III.3.6.- Capa DE PRESENTACIÓN (Presentation).

La Capa de Presentación convierte entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes a un formato de acuerdo mutuo que puede ser entendido por cada Aplicación y por los Ordenadores que ellas corren. La Capa de Presentación puede en determinado momento comprimir, expandir, encriptar y desencriptar datos.

Su objetivo principal es representar los datos recibidos por las Capas de Aplicación y también puede ser diseñada para aceptar cadenas de caracteres en Código ASCII como entrada y producir patrones de bits comprimidos como salida. Se ocupa también del encriptamiento de los datos para que sólo puedan ser interpretados por los destinatarios, incrementando la seguridad de la información que ha sido enviada.

III.3.7.- Capa DE APLICACIÓN (Aplication).

Este nivel especifica la interfase de comunicación el usuario- comunicación de Aplicaciones del Ordenador, proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero), incluyen acceso a Archivos, Transferencia, Transferencia de Información Virtual, Manejo de Red, Servicios de Directorio y Servicios de Transferencia de Correo.

La Capa de Aplicación abarca el conjunto de Programas y Procesos a los que tiene acceso directo el usuario. Entre los principales Servicios que se ofrecen en esta Capa se encuentran el Correo y la Mensajería Electrónica.

En resumen:

Nivel y Nombre	Función	Dispositivos y Protocolos
1 Físico	Este nivel define la forma de los cables, su tamaño, voltajes en los que operan, etc...	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2 Enlace de datos	Aquí encontramos el estándar Ethernet, define el formato de las tramas, sus cabeceras, etc. A este nivel hablamos de direcciones MAC (Media Access Control) que son las que identifican a las tarjetas de red de forma única.	Puentes (bridges). HDLC y LLC.
3 Red	En esta capa encontramos el protocolo IP. Esta capa es la encargada del enrutamiento y de dirigir los paquetes IP de una red a otra. Normalmente los "routers" se encuentran en esta capa. El protocolo ARP (Address Resolution Protocol) es el que utiliza para mapear direcciones IP a direcciones MAC.	Encaminador (router). IP, IPX.

4 Transporte	En esta capa encontramos 2 protocolos, el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). Se encargan de dividir la información que envia el usuario en paquetes de tamaño aceptable por la capa inferior. La diferencia entre ambos es sencilla, el TCP esta orientado a conexión, es decir la conexión se establece y se libera, mientras dura una conexión hay un control de lo que se envia y por lo tanto se puede garantizar que los paquetes llegan y están ordenados. El UDP no hace nada de lo anterior, los paquetes se envían y punto, el protocolo se despreocupa si llegan en buen estado etc. El UDP se usa para enviar datos pequeños, rápidamente, mientras que el TCP añade una sobrecarga al tener que controlar los aspectos de la conexión pero "garantiza" la transmisión libre de errores.	Pasarela (gateway). UDP, TCP, SPX.
5 Sesión	El protocolo de sesión define el formato de los datos que se envían mediante los protocolos de nivel inferior.	Pasarela.
6 Presentación	External Data Representation (XDR), se trata de ordenar los datos de una forma estándar ya que por ejemplo los Macintosh no usan el mismo formato de datos que los PCs. Este estándar define una forma común para todos de tal forma que dos ordenadores de distinto tipo se entiendan.	Pasarela. Compresión, encriptado, VT100.
7 Aplicación	Da servicio a los usuarios finales, Mail, FTP, Telnet, DNS, NIS, NFS son distintas aplicaciones que encontramos en esta capa.	X.400

III.4.- Justificación de el Modelo O.S.I. (International Organization for Standarization, 1987b).

El Modelo OSI se diseño específicamente para Redes de Área Extensa y aunque muchos de los conceptos son compatibles para las Redes de Ordenadores de Área Local (LAN), fue necesario crear nuevas Normas para estandarizarla

El IEEE (Instituto de Ingeniería Eléctrica y Electrónica), ha establecido las principales Normas de Colectividad para Redes Locales a través de sus recomendaciones basándose en el Nivel Físico y el Nivel de Enlace de el Modelo OSI.

Con estas Normas se logrará suficiente Conectividad para que las *"Mainframes", minis y micros*, independientes se conviertan en una cosa del pasado, excepto en las Tiendas, Hogares ó Almacenes Pequeños, y para aplicaciones muy específicas y críticas para la Misión.

Para que el Sistema de Información dé Servicio a toda la Organización, las cajas deben enlazarse entre sí para formar un Sistema de Información, de manera que a los usuarios finales les da impresión de ser un sólo recurso y una extensión natural de sus Estaciones de Trabajo. Sin embargo, la Conectividad va más allá de un mero enlace *"micros-minis-maiframes"*.

Requiere un Procesamiento cooperativo y una interconexión lógica de los componentes estructurales de los Sistemas de Información. Cualquier usuario tiene la capacidad para acceder a la información e interactuar con otros usuarios en una relación de *"igual-a- igual"* a lo largo de toda la Organización.

La conectividad supone capacidades totales de Redes que les permitan a los usuarios navegar fácilmente a través del Sistema, hacer uso de una cartera de recursos y servicios, y extraer datos de cualquier fuente bajo una base de necesidad de conocimiento.

Obviamente, la Cultura Corporativa y las altas Gerencias deben dar apoyo a la Conectividad lógica y de Sistemas. El Soporte para la Conectividad física proviene de estándares de Arquitectura y Comunicaciones, como la Interconexión de Sistemas Abiertos (OSI), el Protocolo de Control de Transmisiones, el Protocolo Internet (TCP/IP), la Red Digital de Servicios Integrados (ISDN), la Arquitectura de Redes de Sistemas de IBM (SNA) y la inclusión de Protocolos de igual-a-igual de IBM.

Así mismo, el X.25, que es el Estándar Internacional para conmutación de Paquetes, es el modo dominante de transmisión para la Red de Área Amplia (WAN). El método principal para la Conectividad de transacciones entre las Compañías e intercambio electrónico de datos.

Las compuertas y los puentes continúan sirviendo como aglutinante entre las costuras de las Redes. Debido a que ningún proveedor único, incluyendo a *AT&T, DEC* o *IBM*, pueden entregar un complemento completo de Aplicaciones de Sistemas y una Conectividad total, los proveedores deberán trabajar conjuntamente para lograr la interconexión e interoperabilidad entre los productos para obtener una Conectividad sin costuras, (Deening, 1989).

Pero hasta que lo hagan, las compuertas, los puentes y otros esquemas de interfase serán necesarios para enlazar los diferentes productos.

¿Cuál es el valor de la Conectividad para los Sistemas de Información y para la Compañía a la que se sirve? En primer lugar, sin Redes y Protocolos viables no se puede tener Conectividad. En segundo lugar, sin Conectividad no se puede lograr integración.

Sin integración no se puede gozar de una Comunicación sin obstáculos y el flujo libre de la información. Mientras las Compañías necesiten un buen flujo de información para operar en forma eficaz y eficiente, existir la necesidad de la Conectividad.

Este es un concepto fundamental en el campo de las Redes de Área Local (LAN) y significa que cualquier dispositivo conectado a la Red de Área Local (LAN) puede ser direccionado como una conexión individual, por ejemplo un Ordenador grande con muchos puertos, cada puerto es una conexión; en tanto que una Terminal ú Ordenador uniusuario es así mismo una conexión.

Se llevan a cabo Sesiones cuando se establece un circuito entre dos o más conexiones. Algunas Redes de Área Local (LAN), tienen la capacidad de aceptar Sesiones de multidifusión o de Transmisión (transmisiones a un subconjunto de todas las conexiones o bien a todas las conexiones).

Los nodos de la Red, son dispositivos inteligentes y pueden soportar una ó más conexiones. Las Redes de características similares o diferentes pueden conectarse entre sí, a través de vías de acceso las cuales, en principio, permiten que un Usuario-Conexión en una Red se comunique con un Usuario-Conexión en otra Red.

En los próximos años, muchos de los dispositivos de comunicaciones más nuevos, como el Fax, Servicios de Transmisión de Voz y Vídeo, Distribución de Imágenes y quizá, Teléfonos Celulares; se convertirán en ingredientes importantes de las Redes de Área Local.

También será cada vez más importante que los fabricantes de Redes de Área Local (LAN) ofrezcan interfases adecuadas a *The Integrated Services Digital Networks (ISDN)*, o de Redes Digitales de Servicios Integrados (RDSI), ya que esta Tecnología permitirá en breve, a los Sistemas Telefónicos, Transportar Voz en Paquetes, Vídeo en Tiempo Real pleno de movimiento comprimido y otras transferencias de información que requieren alta velocidad y Ancho de Banda amplio, (De Prycker, 1993).

Aunque la implantación inicial de las Redes ISDN, pueden soportar estándares de velocidad inferior, esas velocidades son sustancialmente mayores que las Tecnologías anteriores que se utilizan en las Redes Telefónicas. Además, están en Proceso estándares de muy alta velocidad para mejorar las Redes ISDN.

Es probable que los servicios de las ISDN se conviertan en una de las Tecnologías principales para enlazar entre sí Redes de Área Local, distantes a medida que los servicios de ISDN estén ampliamente disponibles.

CAPÍTULO IV.

SEGURIDAD EN REDES DE ORDENADORES.

IV.1.- Introducción.

Los ordenadores son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso de este siglo el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y derecho.

Imagínese que, por una u otra razón, el Centro de Cómputo o las librerías son destruidos o usados inapropiadamente, ¿cuánto tiempo pasaría para que esta Organización estuviese nuevamente en operación? El centro de cómputo puede ser el activo más valioso y al mismo tiempo, el más vulnerable. En la situación actual de criminología, en los delitos de "cuello blanco" se incluye la modalidad de los delitos hechos mediante el ordenador o los sistemas de información, de los cuales el 95% de los detectados han sido descubiertos por accidente, y la gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como el Ordenador ha modificado las circunstancias tradicionales del crimen. Muestra de ello son los fraudes, falsificaciones y venta de información hechos a los Ordenadores o por medio de éstas, (Almela, 2002).

Existen diferentes estimaciones sobre el costo de los delitos de "cuello blanco", las cuales dependerán de la fuente que haga estas estimaciones, pero en todos los casos se considera que los delitos de "cuello blanco" en los Estados Unidos de América superan los miles de millones de dólares.

Durante mucho tiempo se consideró que los procedimientos de auditoria y seguridad eran responsabilidad de la persona que elabora los sistemas, in considerar que son responsabilidad del área de Informática en cuanto a la elaboración de los sistemas del usuario en cuanto a la utilización que se le dé a la información y a la forma de acceder a ella, y del Departamento de Auditoria Interna en cuanto a la supervisión y diseño de los controles necesarios. La seguridad del área de Informática tiene como objetivos:

Proteger la integridad, exactitud y confidencialidad de la información.
Proteger los activos ante desastres provocados por la mano del hombre y de actos hostiles.

Proteger a la Organización contra situaciones externas como desastres naturales y sabotajes
En caso de desastre, contar con los planes y políticas de contingencias para lograr una pronta recuperación.
Contar con los seguros necesarios que cubran las pérdidas económicas en caso de desastre.

Los motivos de los delitos por ordenador normalmente son por:

Beneficio personal. Obtener un beneficio, ya sea económico, político, social o de poder, dentro de la Organización.
Beneficios para la Organización. Se considera que al cometer algún delito en otro ordenador se ayudará al desempeño de la Organización en la cual se trabaja, sin evaluar sus repercusiones.
Síndrome de "Robin Hood" (por beneficiar a otras personas). Se están haciendo copias ilegales por considerar que al infectar a los ordenadores, o bien al alterar la información, se ayudará a otras personas.
Jugando a jugar.
Fácil de desfalcar.
El individuo tiene problemas financieros.
El Ordenador no tiene sentimientos. El Ordenador es una herramienta que es fácil de desfalcar, y es un reto poder hacerlo.
El Departamento es deshonesto
Odio a la Organización (revancha). Se considera que el Departamento o la Organización es deshonesta, ya que no ha proporcionado todos los beneficios a los que se tiene derecho
Equivocación de ego (deseo de sobresalir en alguna forma).
Mentalidad turbada. Existen individuos con problemas de personalidad que ven en elaborar un virus un reto y una superación, los cuales llegan a ser tan cínicos que ponen su nombre y dirección e el virus, para lograr ese reconocimiento.

En la actualidad, principalmente en los ordenadores personales, se ha dado otro factor que hay que considerar: el llamado "virus" de los ordenadores, el cual, aunque tiene diferentes intenciones, se encuentra principalmente en paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Se trata de pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición; por ejemplo, haber obtenido una copia de forma ilegal, y puede ejecutarse en una fecha o situación predeterminada.
El virus normalmente es puesto por los diseñadores de algún tipo de programa ("software") para "castigar" a quienes roban o copian sin autorización o bien por alguna actitud de venganza en contra de la Organización. (En la actualidad existen varios productos para detectar virus).

Existen varios tipos de virus, pero casi todos actúan como "Caballos de Troya"; es decir, se encuentran dentro de un programa y actúan con determinada indicación. Un ejemplo es la destrucción de la información de la Compañía USPA & IRA de Forth Worth. Cuando despidieron a un programador en 1985, éste dejó una subrutina que mensualmente destruía la información de las ventas. Este incidente provocó el primer juicio en Estados Unidos de América contra una persona por sabotaje a un Ordenador.

Al auditar los sistemas, se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarse en red con otros ordenadores, no exista la posibilidad de transmisión del virus. También se debe que en ocasiones se toma como pretexto el virus y se producen efectos psicológicos en los usuarios, ya que en el momento de una falla del ordenador o del sistema, lo primero que se piensa es que están infectados, (Bacard, 2002). Se considera que hay cinco factores que han permitido el incremento en los crímenes por ordenador:

El aumento del número de personas que se encuentran estudiando computación.
El aumento del número de empleados que tienen acceso a los equipos.
La facilidad en el uso de los equipos de cómputo.
El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información.
El incremento de redes y de facilidades para utilizar los ordenadores en cualquier lugar y tiempo.

Estos cinco factores, aunque son objetivos de todo Centro de Cómputo, también constituyen una posibilidad de uso con fines delictivos. El uso inadecuado del ordenador comienza desde la utilización de tiempo de máquina para usos ajenos al de la Organización, la copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a Bases de Datos a fin de modificar la información con fines fraudulentos. Estos delitos pueden ser cometidos por personas que no desean causar un mal.

En la actualidad las compañías cuentan con grandes dispositivos para la seguridad física de los ordenadores, y se tiene la idea que los sistemas no pueden ser violados si no se entra al Centro de Cómputo, olvidando que se pueden usar terminales y sistemas remotos de teleproceso. Se piensa (como en el caso de la seguridad ante incendio y robo), que "eso no me puede suceder a mí o es poco probable que suceda aquí".

Algunos gerentes creen que los ordenadores y sus programas son tan complejos que nadie fuera de su Organización los va a entender y no les van a servir. Pero, en la actualidad, existe un gran número de personas que puede captar y usar la información que contiene un sistema y considerar que hacer esto es como un segundo ingreso. También se ha detectado que el mayor número de fraudes, destrucción de

información o uso ilegal de ésta, provienen del personal interno de una Organización. También se debe considerar que gran parte de los fraudes hechos por ordenador o el mal uso de éste son realizados por personal de la misma Organización.

En forma paralela, al aumento de los fraudes hechos a los sistemas computarizados, se han perfeccionado los sistemas de seguridad tanto física lógica; la gran desventaja del aumento en la seguridad lógica es que se requiere consumir un número mayor de recursos de cómputo para lograr tener una idónea seguridad, lo ideal es encontrar un sistema de acceso adecuado al nivel de seguridad requerido por el sistema con el menor costo posible. En los desfalcos por ordenador (desde un punto de vista técnico), hay que tener cuidado con los "Caballos de Troya" que son programas a los que se les encajan rutinas que serán activadas con una señal específica.

IV.2.- Seguridad Lógica y Confidencialidad.

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de un Ordenador, así como de controlar el mal uso de la información. Estos controles reducen el riesgo de caer en situaciones adversas, según Arkin (2000).

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la Organización para perder información, o bien para que ésta sea utilizada en forma inadecuada; así mismo, esto hace que se vea disminuida su defensa ante competidores, el crimen organizado, personal desleal y violaciones accidentales.

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el "software" de desarrollo y por los programas en aplicación; identifica individualmente a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, los programas de uso general, de uso específico, de las redes y terminales. La falta de seguridad lógica o su violación puede traer las siguientes consecuencias ala Organización:

Cambio de los datos antes o cuando se le da entrada al ordenador.
Copias de programas y / o información.
Código oculto en un programa.
Entrada de virus.

La seguridad lógica puede evitar una afectación de pérdida de registros, y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña) hasta los sistemas más complicados, pero se debe evaluar que cuanto

más complicados sean los dispositivos de seguridad más costosos resultan. Por lo tanto, se debe mantener una adecuada relación de seguridad-costo en los sistemas de información.

Los sistemas de seguridad normalmente no consideran la posibilidad de fraude cometida por los empleados en el desarrollo de sus funciones. La introducción de información confidencial al ordenador puede provocar que ésta esté concentrada en manos de unas cuantas personas, por lo que existe una alta dependencia en caso de pérdida de los registros. El más común de estos delitos se presenta en el momento de la programación, en el cual por medio de ciertos algoritmos se manda borrar un archivo. Por ejemplo, al momento de programar un sistema de nómina se puede incluir una rutina que verifique si se tiene dentro del archivo de empleados el Registro Federal de Contribuyentes del programador.

En caso de existir, continúa el proceso normalmente; si no existe significa que el programador que elaboró el sistema renunció o fue despedido y en ese momento pudo borrar todos los archivos. Esta rutina, aunque es fácil de detectar, puede provocar muchos problemas, en caso de que no se tenga los programas fuente o bien que o se encuentren debidamente documentados. También en el caso de programadores honestos, en ocasiones en forma no intencional, se pueden tener fallas o negligencia en los sistemas. La dependencia de ciertos individuos clave, algunos de los cuales tienen un alto nivel técnico, comúnmente pone a la Organización en manos de unas cuantas personas, las cuales suelen ser las únicas que conocen los sistemas debido a que no los documentan.

Un método eficaz para proteger sistemas de computación es el "software" de control de acceso. Dicho de una manera simple, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden al usuario una contraseña antes de permitirle acceso a información confidencial.

Dichos paquetes han sido populares desde hace muchos años en el mundo de los ordenadores grandes, y los principales proveedores ponen a disposición de los clientes alguno(s) de estos paquetes. Sin embargo, los paquetes de control de acceso basados en contraseñas pueden ser eludidos por delincuentes preparados en computación, por lo que no es conveniente depender de esos paquetes por sí solos para tener una adecuada seguridad. El sistema integral de seguridad debe comprender:

Elementos administrativos.
Definición de una política de seguridad.
Organización y división de responsabilidades.

IV.3.- Seguridad Lógica.

Uno de los puntos más importantes a considerar para poder definir la seguridad de un sistema es el grado de actuación que puede tener un usuario dentro de un sistema, ya sea que la información se encuentre en un archivo normal o en una Base de Datos, o bien que posea un miniordenador, o un sistema en red (interna o externa). Para esto se pueden definir los siguientes tipos de usuarios:

Propietario. Es, como su nombre lo indica, el dueño de la información, el responsable de ésta, y puede realizar cualquier función (consultar, modificar, actualizar, dar instrucciones de entrada a otro usuario). Es responsable de la seguridad lógica, en cuanto puede realizar cualquier acción y puede autorizar a otros usuarios de acuerdo con el nivel que desee darles.

Administrador. Sólo puede actualizar o modificar el "software" con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.

Usuario Principal. Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.

Usuario de Consulta. Sólo puede leer la información pero no puede modificarla.

Usuario de Explotación. Puede leer la información y utilizarla para explotación de la misma, principalmente para hacer reportes de diferente índole, los cuales, por ejemplo, pueden ser contables o estadísticos.

Usuario de Auditoria. Puede utilizar la información y rastrearla dentro del sistema para fines de auditoria.

Los usuarios pueden ser múltiples y pueden ser el resultado de la combinación de los antes señalados. Se recomienda que exista sólo un usuario propietario, y que el administrador sea una persona designada por la Gerencia de Informática, (Baker, 2000).

Para conservar la integridad, confidencialidad y disponibilidad de los sistemas de información se debe tomar en cuenta lo siguiente:

La Integridad es responsabilidad de los individuos autorizados para modificar datos o programas (usuario administrador) o de los usuarios a los que se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo (usuario responsable y principal).

La Confidencialidad es responsabilidad de los individuos autorizados para consultar (usuario de consulta) o para bajar archivos importantes para microordenadores (usuario de explotación).

La Disponibilidad es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de Bases de Datos, al monitoreo de teleproceso o al "software" de telecomunicaciones (usuario administrados).

El control implantado para minimizar estos riesgos debe considerar los siguientes factores:

El valor de los datos siendo procesados.
La probabilidad de que ocurra un acceso no autorizado.
Las consecuencias de la Organización si ocurre un acceso no autorizado.
El riesgo y repercusiones en caso de que un usuario no autorizado utilice la información.

La seguridad lógica abarca las siguientes áreas:

Rutas de acceso.
Claves de acceso.
Software de control de acceso.
Encriptamiento.

IV. 3.1. Rutas de Acceso.

El acceso a la computadora no significa tener una entrada sin restricciones. Limitar el acceso sólo a los niveles apropiados puede proporcionar una mayor seguridad. El objetivo de la seguridad de los sistemas de información es controlar las operaciones y su ambiente mediante el monitoreo del acceso a la información y a los programas para poder darle un seguimiento y determinar la causa probable de desviaciones, (Barriuso, 1996). Por ello es conveniente al utilizar algún tipo de "software" dentro de un sistema, contar con una ruta de acceso.

Cada uno de los sistemas de información tiene una ruta de acceso, la cual puede definirse como la trayectoria seguida en el momento de acceso al sistema.

Como se ha señalado, un usuario puede pasar por uno o múltiples niveles de seguridad antes de obtener el acceso a los programas y datos. Los tipos de restricciones son:

Sólo lectura.

Sólo consulta.
Lectura y consulta.
Lectura y escritura, para crear, actualizar, borrar, ejecutar o copiar.

El esquema identifica a los usuarios del sistema, los tipos de dispositivos por los cuales es posible acceder al sistema, el "software" usado para el acceso al sistema, los recursos que pueden ser accedidos y los sistemas donde residen estos recursos. Los sistemas pueden ser en línea, fuera de línea, en "batch", y rutas de telecomunicación.

El esquema de las rutas de acceso sirve para identificar todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El auditor debe conocer las rutas de acceso para la evaluación de los puntos de control apropiados.

IV.3.2.- Claves de Acceso.

Un área importante en la seguridad lógica es el control de las claves de acceso de los usuarios, (Bernal, 1997). Existen diferentes métodos de identificación para el usuario:

Un código o contraseña.
Una credencial con banda magnética.
Algo específico del usuario (características propias).

La identificación es definida como el proceso de distinción de un usuario a otros. La identificación de entrada proporcionará un reconocimiento individual; cada usuario debe tener una identificación de entrada única que debe ser reconocida por el sistema.

Contraseña, código o llaves de acceso. La identificación de los individuos es usualmente conocida y está asociada con un "password" o clave de acceso. Las claves de acceso pueden ser usadas para controlar el acceso a la computadora, a sus recursos, así como definir nivel de acceso o funciones específicas.

Las llaves de acceso deben tener las siguientes características:

El sistema debe verificar primero que el usuario tenga una llave de acceso válida.
La llave de acceso debe ser de una longitud adecuada para ser un secreto.
La llave de acceso no debe ser desplegada cuando es tecleada.
Las llaves de acceso deben ser encriptadas, ya que esto reduce el riesgo de que alguien obtenga la llave de acceso de otras personas.
Las llaves de acceso deben de prohibir el uso de nombres, palabras o cadenas de caracteres difíciles de retener, además el "password" no debe ser cambiado por un valor pasado. Se recomienda la combinación de caracteres alfabéticos y numéricos.

No debe ser particularmente identificable con el usuario, como su nombre, apellido o fecha de nacimiento.

Credenciales con banda magnética. La banda magnética de las credenciales es frecuentemente usada para la entrada del sistema. Esta credencial es como una bancaria, pero se recomienda que tenga fotografía o firma.

La ventaja más importante de la credencial es prevenir la entrada de impostores al sistema. Una credencial ordinaria es fácil de falsificar, por lo que se debe elaborar de una manera especial, que no permita que sea reproducida.

Validación por características. Es un método para la identificación del usuario, que es implantado con tecnología biométrica. Consiste en la verificación y reconocimiento de la identidad de las personas, basándose en características propias. Algunos de los dispositivos biométricos son:

Las huellas dactilares.
La retina.
La geometría de la mano.
La firma.
La voz.

IV.3.3.- "Software" de Control de Acceso.

Éste puede ser definido como el "software" diseñado para permitir el manejo y control del acceso a los siguientes recursos:

Programas de librerías.
Archivos de datos.
Trabajos ó "Jobs".
Programas en aplicación.
Módulos de funciones.
Utilerías.
Diccionario de datos.
Archivos.
Programas.
Comunicación.

Controla el acceso a la información, grabando e investigando los eventos realizados y el acceso a los recursos, por medio de la identificación del usuario, (Caballero, 1996).

El "software" de control de acceso, tiene las siguientes funciones:

Definición de usuarios.
Definición de las funciones del usuario después de acceder al sistema.
Establecimiento de auditoria a través del uso del sistema.

El "software" de seguridad protege a los recursos mediante la identificación de los usuarios autorizados con las llaves de acceso, que son archivadas y guardadas por este "software".

Esto puede ser efectuado a través de la creación de archivos o tablas de seguridad. Los paquetes de seguridad frecuentemente incluyen facilidades para encriptar estas tablas o archivos.

A cada usuario se le debe asignar un alcance en el acceso y por cada recurso un grado de protección; para que los recursos puedan ser protegidos de un acceso no autorizado.

Algunos paquetes de seguridad pueden ser usados para restringir el acceso a programas, librerías y archivos de datos; otros pueden además limitar el uso de terminales o restringir el acceso a bases de datos, y existen otros más para confirmar y evaluar la autorización de la terminal para utilizar determinada información. Éstos pueden variar en el nivel de la seguridad brindada o los archivos de datos. La seguridad puede estar basada en el tipo de acceso: usuarios autorizados para agregar registros a un archivo o los que únicamente leen registros.

La mayor ventaja del "software" de seguridad es la capacidad para proteger los recursos de accesos no autorizados, incluyendo los siguientes:

Procesos en espera de modificación por un programa de aplicación.
Accesos por los editores en línea.
Accesos por utilerías de "software".
Accesos a archivos de las bases de datos, a través de un manejador de base de datos (DBMS).
Acceso de terminales o estaciones no autorizadas.

Estos paquetes pueden restringir el acceso a los recursos (archivos de datos), reduciendo así el riesgo de los accesos no autorizados.

En el caso de terminales de compra de boletos de pronósticos, se puede restringir la entrada a terminales no autorizadas o en tiempo no autorizado.

Otra característica de estos paquetes es que se pueden detectar las violaciones de seguridad, tomando las siguientes medidas:

Terminaciones de procesos.
Forzar a las terminales a apagarse.
Desplegar mensajes de error.
Escribir los registros para la auditoria.

La bitácora de auditoria es seleccionada mediante la implementación.

La bitácora puede consistir en registrar los accesos no exitosos, solo los intelectos, un registro de todos los accesos válidos y los recursos protegidos.

Algunos paquetes contienen datos específicos para ser incluidos en la bitácora de auditoria.

Cada bitácora debe incluir la identificación del usuario; si el acceso es exitoso, deben consignarse los recursos accedidos, día, hora, terminal y un dato específico de lo que fue modificado durante el acceso; si el acceder no fue exitoso la mayor información posible sobre día, hora, terminal y claves de intento usadas.

IV.3.4.-.Otros Tipos de "Software" de Control de Acceso.

Algunos tipos de software son diseñados con características que pueden ser usadas para proveerles seguridad. Sin embargo, es preferible usar un "software" de control de acceso para asegurar el ambiente total y completar las características de seguridad con un software específico, (Coelli, 2002).

Como existen diferentes tipos de "software", se explicarán las características de seguridad de los siguientes:

Sistemas operativos.
Manejadores de base de datos.
Software de consolas o terminales maestras.
Software de librerias.
Software de utilerías.
Telecomunicaciones.

A) Sistemas Operativos.

Se trata de una serie de programas que se encuentran dentro de los sistemas operativos, los cuales manejan los recursos de las computadoras y sirven como interfase entre el "software" de aplicaciones y el "hardware".

Estos programas proporcionan seguridad ya que, internamente, dentro de los sistemas operativos manejan y controlan la ejecución de programas de aplicación y proveen los servicios que estos programas requieren, dependiendo del usuario y del sistema que se esté trabajando. Cada servicio debe incluir un calendario de trabajo ("Job Schedule"), manejador de equipos periféricos, un contador de trabajo y un compilador de programas, pruebas y "debugs" (depuraciones). El grado de protección sobre estos servicios depende de los sistemas operativos.

Los elementos de seguridad de los sistemas operativos incluyen los siguientes:

Control de salidas de los programas al modificarse códigos. Estos usualmente pueden acceder a los elementos más importantes del sistema, y sus actividades deben ser monitoreadas.
Los sistemas operativos usan claves de acceso ("password", ID) para prevenir usuarios no autorizados a funciones y utilerías del sistema operativo. Muchas veces, estas claves de acceso están definidas en una tabla del sistema que es activada cuando un sistema es utilizado. Las claves de acceso deben ser cambiadas inmediatamente por las nuevas claves de acceso.
Algunos sistemas operativos proveen una característica que puede limitar el número de accesos no autorizados y autorizar usuarios a los recursos protegidos, si este número es excedido, el usuario no autorizado es prevenido para el nuevo acceso a estos recursos.
Los sistemas operativos permiten una instalación para la implementación opcional de características de seguridad cuando es sistema es instalado. Algunos sistemas operativos contienen sus propias características de seguridad y muchas veces éstas no son adecuadas; en este caso es aconsejable integrar al sistema operativo un "software" de seguridad para proteger los recursos. El valor de estos es un factor determinante cuando se decide que tanta protección es necesaria.
Los sistemas operativos tienen un completo control sobre las actividades de todas las aplicaciones que estás corriendo en el sistema. Si un usuario no autorizado puede acceder a los recursos del sistema operativo, puede hacer modificaciones que alteren el proceso normal del flujo del sistema. El sistema operativo tiene autoridad para dar facilidades de seguridad y para acceder a recursos confidenciales. Esto implica que en algunas ocasiones se requerirá del uso de algún producto de seguridad adicional. El "software" de funciones de control del sistema operativo debe proveer una bitácora de auditoria.
Tanto el administrador del sistema o de seguridad de datos establece sus privilegios a través del sistema operativo. Individualmente, con estos privilegios tienen completo control sobre el sistema operativo y su ambiente; ellos pueden otorgar la autoridad para modificar usuarios y acceder a secciones, alterar la generación de procedimientos del sistema y modificar las prioridades de trabajo ("jobs") que corren dentro del control del sistema. Debe existir una bitácora de las actividades del administrador del sistema o del administrador de la seguridad de datos.
Los sistemas operativos permiten la definición de consolas o terminales maestras desde las cuales los operadores puede introducir comandos al sistema operativo. Las consolas no requieren una señal en proceso para la emisión de comandos. Por lo

tanto, el acceso, a áreas físicas en donde están las consolas debe ser restringido. Además, las características del sistema que permiten a una terminal ser asignada con el estatus de consola deben ser guardadas a prueba de accesos no autorizados.

B) "Software" Manejador de Base de Datos.

Es un "software" cuya finalidad es la de controlar, organizar y manipular los datos. Provee múltiples caminos para acceder a los datos, en una base de datos. Maneja la integridad de datos entre operaciones, funciones y tareas de la organización.

Cuando un usuario inicialmente requiere del uso de sistemas de administración de bases de datos ("Data Base Management System", DBMS) se establece un identificador para el usuario y la sesión. Inmediatamente, el usuario puede ser identificado por el ID-terminal, y por una aplicación o función.

En espera del modo de modificaciones, el usuario podrá ser identificado por el trabajo ("job"), por la aplicación o por la función.

El identificador del usuario será usado para rastrear todos loa accesos a los archivos de datos a través del administrador de la base de datos (DBMS).

Las características de seguridad del software DBMS pueden ser usadas para restringir el acceso a un usuario específico, a un cierto archivo o a vistas lógicas, los accesos a procedimientos, funciones o "software" en aplicaciones limitado a usuarios autorizados con el propósito de ejecutar sus tareas asignadas. Las vistas de datos lógicos están colocadas en archivos para usuarios particulares, funciones o aplicaciones, y puede ser representado todo o parte del archivo de datos físicos o una combinación de campos de múltiples archivos de datos físicos. Estas características son usadas para controlar funciones únicas en el administrador de la base de datos (DBMS).

Las utilerías de la base de datos proveen funciones de mantenimiento, como respaldos y restauración de la base de datos, reorganización de datos, reportes estadísticos de la base de datos y sus relaciones. Ésos pueden ser usados además para adicionar o borrar datos y proveer seguridad.

El diccionario de datos (DD) es un "software" que guía y provee un método para documentar elementos de la base de datos, así como un método de seguridad de datos en un administrador de base de datos (DBMS).

Todas las modificaciones al director de datos (DD) deben producir una bitácora de auditoria, como un registro automático de todos los cambios y un medio de recuperación después de alguna interrupción que hubiese ocurrido.

C) "Software" de Consolas o Terminales Maestras.

El "software" de consolas o terminales maestras puede ser definido como varios programas del sistema operativo que proveen soporte y servicio para que las terminales en línea accedan a los programas en aplicación.

Las consolas incluyen funciones de seguridad para restringir el acceso a los datos, vía programas en aplicación.

Estas funciones frecuentemente están basadas en una serie de tablas que definen a los usuarios autorizados, así como los recursos y programas en aplicación que ellos pueden acceder. Generalmente las consolas pueden sólo limitar al acceso al usuario para entrar a un programa en aplicación, no para el uso de funciones específicas de un programa.

La mayor parte de las consolas mantienen un registro de uso de llaves de acceso ("password") diario válidas o no válidas.

D) "Software" de Librerías.

El "software" de librerías consta de datos y programas específicos escritos para ejecutar una función en la organización.

Los programas en aplicación (librerías) pueden ser guardados en archivos en el sistema y acceder a estos programas puede ser controlado por medio del "software" ("software" de control de acceso general) usado para controlar el acceso a estos archivos.

El "software" de manejo de librerías puede ser usado para mantener y proteger los recursos de programas de librerías, la ejecución de "jobs", y en algunas instancias, los archivos de datos pueden ser utilizados por éstas.

Estas librerías deben ser soportadas por un adecuado control de cambios y procedimientos de documentación.

Una importante función del "software" controlador de librerías es controlar y describir los cambios de programas en una bitácora. El "software" de librerías provee diferentes niveles de seguridad, los cuales se reflejan en las bitácoras de auditoria.

Los controles de cambios de emergencia deben estar en algún lugar debido a la naturaleza de estos cambios (frecuentemente son realizados fuera de horas de trabajo normal, son cortos, no se comunican):
Accesos de emergencia. Pueden ser concedidos con el propósito de resolver el problema, y ser inmediatamente revocados después de que el problema es resuelto.
Todas las acciones realizadas durante la emergencia deberán ser automáticamente registradas.

Cuando se instala el software de librerías se definen las librerías y sus respectivos niveles de protección.

Los tipos de acceso a la librería pueden ser registrados durante la instalación. Por ejemplo, un programador deberá ser autorizado para leer o modificar un programa.

E) "Software" de Utilerías.

Existen dos tipos de "software" de utilerías. El primero es usado en los sistemas de desarrollo para proveer productividad. El desarrollo de programas y los editores en línea son los ejemplos de este tipo de "software". El segundo es usado para asistir en el manejo de operaciones del Ordenador. Monitoreos, calendarios de trabajo, sistema manejador de disco y cinta son ejemplos de este tipo de "software".

El "software" de utilerías tiene privilegios para acceder todo el tiempo, algún tiempo o nunca. Los accesos privilegiados se otorgan en programadores o a usuarios que ejecutan funciones que sobrepasan la seguridad normal.

Entre los ejemplos de utilerías de "software" están:

Utilerías de monitores.
Sistemas manejadores de cintas.
Sistemas manejadores de disco.
Calendarios de "jobs".
Editores de línea.
"Debugers".
Verificador de virus.
"Software" de telecomunicaciones.

Ciertos tipos de "software" de telecomunicaciones pueden restringir el acceso a las redes y a aplicaciones específicas localizadas en la red.

El "software" de telecomunicaciones provee la interfase entre las terminales y las redes y tiene la capacidad para:

Controlar la invocación de los programas de aplicación.
Verificar que todas las transacciones estén completas y sean correctamente transmitidas.
Restringir a los usuarios para actuar en funciones seleccionadas.
Restringir al acceso al sistema a ciertos individuos.

IV.4.- Riesgos y Controles a Auditar.

Los controles de "software" de seguridad general y de "software" específico pueden ser implantados para minimizar el riesgo de la seguridad lógica, (Calle, 1997).

Controles del "software" de seguridad general. Los controles del "software" de seguridad general aplican para todos los tipos de "software" y recursos relacionados y sirven para:

El control de acceso a programas y a la información.
Vigilar los cambios realizados.
Las bitácoras de auditoria.
Control de acceso a programas y datos. Este control de acceso se refiere a la manera en que cada "software" del sistema tiene acceso a los datos, programas y funciones. Los controles son usualmente a través del ID (identificador) o del "password" para identificar a usuarios no autorizados y para controlar el acceso inicial al "software".
Cambios realizados. Deben ser probados y revisados para ser autorizados, y una vez autorizados se asignan a los programas en aplicación y datos.

Dependiendo de la aplicación, el ambiente y el potencial del efecto de los cambios, éste puede ser muy informal o extremadamente rígido. Los procedimientos a seguir para los cambios realizados pueden ser los siguientes:

Diseños y código de modificaciones.
Coordinación con otros cambios.
Asignación de responsabilidades.
Revisión de estándares y aprobación.
Requerimientos mínimos de prueba.
Procedimientos del respaldo en el evento de interrupción.

La bitácora de auditoria debe registrar cambios en el "software" antes de la implementación. Los procedimientos de cambios de "software" deben además incluir notificaciones escritas para el departamento apropiado de cada cambio. Los cambios realizados deben incluir independientemente una fase de pruebas realizadas por un grupo fuera del ambiente de desarrollo.

Bitácoras de Auditoria. Las bitácoras de auditoria son usadas para monitorear los accesos permitidos y negados. El "software" debe contener una bitácora de auditoria de uso de las funciones que el "software" ejecuta, particularmente si cambian las funciones o se modifican datos. Esta bitácora de auditoria posiblemente sea mantenida en un archivo separado, y puede ser manejada por las actividades del sistema, o tal vez sea una parte del registro. El tipo de bitácoras de auditoria varía gradualmente de acuerdo al "software" y al vendedor; por ejemplo, un "software" puede guardar antes y después imágenes de los cambios, mientras que otros solamente tienen una técnica de recuperación que puede ser usada para seguridad en casos necesarios.

Las bitácoras de auditoria generalmente están relacionadas con el sistema operativo o con el "software" de control de acceso. Estas bitácoras de auditoria registran las actividades y opcionalmente muestran el registro de los cambios hechos en el archivo o programas. Son importantes para el seguimiento de los cambios.

Controles de "software" específico. A continuación se presentan algunos de los controles usados por los diferentes tipos de "software" específico:

El acceso al sistema debe ser restringido para individuos no autorizados.
Se debe controlar el acceso a los procesos y a las aplicaciones permitiendo a los usuarios autorizados ejecutar sus obligaciones asignadas y evitando que personas no autorizadas logren el acceso.
Las tablas de acceso o descripciones deberán ser establecidas de manera que se restrinja a los usuarios ejecutar funciones incompatibles o más allá de sus responsabilidades.
Se deberá contar con procedimientos para que los programadores de aplicaciones tengan prohibido realizar cambios no autorizados a los programas.
Se limitará tanto a usuarios como a programadores de aplicaciones a un tipo específico de acceso de datos (por ejemplo: lectura y modificación).
Para asegurar las rutas de acceso deberá restringirse el acceso a secciones o tablas de seguridad, mismas que deberán ser encriptadas.
Las bitácoras de auditoria deberán ser protegidas de modificaciones no autorizadas.

Deberán restringirse las modificaciones o cambios al "software" de control de acceso, y éstos deberán ser realizados de acuerdo a procedimientos autorizados:

1.- "Software" de sistemas operativos. Entre los controles se incluyen los siguientes:

Los "password" e identificadores deberán ser confidenciales. Los usuarios no autorizados que logran acceder al sistema pueden causar modificaciones no autorizadas.
El acceso a "software" de sistema operativo deberá ser restringido.
Los administradores de la seguridad deberán ser los únicos con autoridad para modificar funciones del sistema, incluyendo procedimientos y tablas de usuarios.
El acceder a utilerías del sistema operativo será restringido.
Las instalaciones de sistemas y las reinstalaciones deben ser monitoreadas porque la realización no autorizada puede resultar inválida.
El uso de todas las funciones del "software" (editores de línea, consolas) es restringido a individuos autorizados.
Deberán revisarse las bitácoras de auditoria para determinar si ocurre un acceso no autorizado o si se realizan modificaciones.

2.- "Software" manejador de base de datos. Los controles incluyen lo siguiente:

El acceso a los archivos de datos deberá ser restringido en una vista de datos lógica, a nivel de tipo de campo. La seguridad en el campo será dada de acuerdo al contenido del campo (validación de campos).
Deberá controlarse al acceso al diccionario de datos.
La Base de Datos debe ser segura y se usarán las facilidades de control de acceso construidas dentro del "software", DSMS.
La bitácora de auditoria debe reportar los accesos al diccionario de datos.
Las modificaciones de capacidades desde el DBMS para las bases de datos deberán limitarse al personal apropiado.

3.-"Software" de consolas o terminales maestras. Estos controles incluyen lo siguiente:

Los cambios realizados al "software" de consolas o terminales maestras deberán ser protegidos y controlados.

4.- "Software" de librerías. Los controles incluyen lo siguiente:

El "software" de librerías mantiene una bitácora de auditoria de todas las actividades realizadas. La información provista en la bitácora incluye el nombre del programa, el número de la versión, los cambios específicos realizados, la fecha de mantenimiento y la identificación del programador.
El "software" de librerías tiene la facilidad de comparar dos versiones de programas en código fuente y reportar las diferencias.
Debe limitarse al acceso a programas o datos almacenados por el "software" de librerías.
Deberá impedirse al acceso a "password" o códigos de autorización a individuos no autorizados.
Los cambios realizados al "software" de librerías tendrán que ser protegidos y controlados.
Las versiones correctas de los programas de producción deben corresponder a los programas objeto.

5.- "Software" de utilerías. Los controles incluyen lo siguiente:

Deberá restringirse el acceso a archivos de utilerías.
Algunas utilerías establecen niveles de utilización por cada función y verifican cada nivel de autorización del usuario antes de darle acceso, utilizando "password" para proveer accesos no autorizados.
El "software" de utilerías genera una bitácora de auditoria de usos y actividades. Algunas proveen bitácoras detalladas de actividades con datos protegidos, librerías y otros recursos. Estas bitácoras de auditoria proveen información de cada identificador (ID), fecha y hora de acceso, recursos accedidos y tipo de acceso.
Esta bitácora sirve como un registro de eventos, incluyendo violaciones a la seguridad y accesos no autorizados. Cada paquete de "software" puede tener diferentes capacidades de control.

Tomar precauciones para asegurar la manipulación de datos (copiar, borrar, etcétera), los protege de un uso no autorizado.
Asegurar que únicamente personal autorizado tenga acceso a correr aplicaciones.
Las utilerías no deben ser mantenidas en el ambiente de producción y se debe asegurar que únicamente usuarios autorizados tengan acceso a ellas.
Las bitácoras de auditoria producidas por utilerías deben ser cuidadosamente revisadas para identificar alguna violación a la seguridad.

6.- "Software" de telecomunicaciones. Los controles incluyen lo siguiente:

Controlar el acceso a datos sensibles y recursos de la red de la siguiente forma:

Verificación de "login" de aplicaciones.
Control de las conexiones entre sistemas de telecomunicaciones y terminales.
Restricción al uso de aplicaciones de la red.
Protección de datos sensibles durante la transmisión, terminando la sesión automáticamente.

Los comandos del operador que pueden dar "shoutdown" a los componentes de la red sólo pueden ser usados por usuarios autorizados.
El acceso diario al sistema debe ser monitoreado y protegido.
Asegurar que los datos no sean accedidos o modificados por un usuario no autorizado, ya sea durante la transmisión o mientras está en almacenamiento temporal.

IV.4.1.- Consideraciones al Auditar.

Cuando se realiza una revisión de seguridad lógica, el auditor interno deberá evaluar y probar los siguientes tres controles implantados para minimizar riesgos:

Control de acceso a programas y a la información.
Control de cambios.
Bitácoras de auditoria.

La evaluación de todos los tipos de "software" deberá asegurar que los siguientes objetivos sean cumplidos:

El acceso a funciones, datos y programas asociados con el "software" debe estar restringido a individuos autorizados y debe ser consistente con documentos esperados.
Todos los cambios del "software" deben ser realizados de acuerdo con el manejo del plan de trabajo y con la autorización del usuario.
Se debe mantener una bitácora de auditoria de todas las actividades significativas.

La auditoria de seguridad lógica puede ser realizada de diferentes maneras. La auditoria puede enfocarse en áreas de seguridad que son aplicables a todo tipo de "software" y pueden cubrir la instalación, el mantenimiento y la utilización del "software".

También debe tomarse en cuenta las características de seguridad del "software", incluyendo el control de acceso, la identificación del usuario y el proceso de autenticidad del usuario, ejecutado por el "software". Entre las consideraciones específicas al auditar están:

"Software" de control de acceso.
"Software" de telecomunicaciones.
"Software" manejador de librerías.
"Software" manejador de Bases de Datos.
"Software" de utilerías.
"Software" de Sistema Operativo.

Durante el ciclo de vida del "software" deben ser evaluadas su instalación, mantenimiento y operación. Se debe utilizar la auditoria para asegurar que algún cambio hecho al "software" no comprometa la integridad, confidencialidad o aprovechamiento de los datos o recursos del sistema. El "software" de auditoria especializado puede ser usado para revisar todos los cambios y asegurarse que son ejecutados de acuerdo con los procedimientos aprobados por la Gerencia.

Instalación y mantenimiento. Es la primera fase del ciclo de vida del "software", en el cual el auditor debe revisar lo siguiente:

Procedimientos para nuevas pruebas o modificaciones al "software", incluyendo al personal responsable, ejecución de pruebas, respaldo de "software" existente, pruebas de funciones, documentación de cambios, notificación de cambios, revisión y redención de pruebas de salida y aprobación de prioridades para la implantación.
Procedimientos para iniciación, documentación, pruebas y aprobación de modificaciones al "software".
Procedimientos usados para ejecutar "software" y mantenimiento del diccionario de datos para un mayor grado de modificación.
Procedimiento de emergencia usado para dar solución a un problema específico de "software".
Mantenimiento y contenido de las bitácoras de auditoria de todos los DBMS y modificaciones del diccionario de datos.
Bitácoras a los parámetros del "software" y de las sentencias del lenguaje de aplicaciones en ejecución.
Acceso a librerías de programas.

Operación. En la segunda fase del ciclo de vida del "software" deberán revisarse:

Controles de acceso para los programas, librerías, parámetros, secciones o archivos de "software" asociados.
Procedimientos diseñados para asegurar que el sistema no es instalado (carga inicial del programa) sin el "software" original, creando así un procedimiento de seguridad.
Disponibilidad y control de acceso a los comandos que pueden ser usados para desactivar el "software".
Áreas de responsabilidad para el control del "software", operación y consistencia de capacidad de acceso.
Horas durante las cuales el "software" está disponible.
Procedimientos para la iniciación y terminación del uso del "software".
Control de acceso sobre consolas y terminales maestras.
Procedimientos para registrar terminación anormal o errores, los cuales pueden indicar problemas en la integridad del "software" y documentar los resultados en programas de seguridad.
Controles de acceso sobre escritura de programas y lenguajes de librerías y de aplicaciones en ejecución.
Bitácoras de auditoria sobre las actividades del "software".
Dependencia de otro "software" para continuar la operación, operaciones automatizadas o dependencia del calendario de actividades.

"Software" de control de acceso. Entre las consideraciones de auditoria para el "software" de control de acceso están:

Diseño y administración.
Procedimiento de identificación del usuario.
Procedimientos de autentificación del usuario.
Recursos para controlar el acceso.
Reportes y vigilancia del "software" de control de acceso reportando y vigilando.

El "software" de control de acceso usualmente provee utilerías que pueden ser usadas en la ejecución de una auditoria. Los eventos pueden ser registrados en un archivo de auditoria (cambios en el sistema, así como la ocurrencia de otras numerosas actividades: "login", archivos de acceso, recursos de acceso, violaciones y cambios de acceso). Los reporteadores y otras utilerías pueden ser usadas para presentar esta información continuamente.

Diseño y administración. En estos aspectos los auditores internos deben revisar lo siguiente:

Localización de archivos de seguridad, tablas para asegurar que los archivos del "software" de control de acceso están protegidos.

Uso de recursos o controles de acceso a nivel del usuario para asegurar que el "software" de control de acceso protege datos y recursos en un nivel correcto.
Archivos de seguridad o encriptación de tablas usadas para prohibir la vista de tablas individuales.
Limitaciones de acceso para archivos de seguridad que contienen descripciones y contraseñas.
Limitaciones de acceso a archivos de seguridad a través de la administración de comando de seguridad en línea o utilerías.
Los usuarios encargados de la administración de la seguridad pueden tener gran capacidad para cierto "software".
Métodos y limitaciones sobre archivos de seguridad o modificación de tablas.
Responsabilidades del usuario para la administración de la seguridad, particularmente en un ambiente descentralizado, para asegurar que las capacidades definidas son consistentes con las responsabilidades.
Definición de parámetros de seguridad, como los recursos definidos, reglas de contraseña(s), "default" de niveles de acceso y opciones de "login" con aprobación de la Gerencia, considerando pruebas de protección para acceder recursos protegidos.

Procedimientos de identificación del usuario. Los auditores deberán revisar y aprobar los métodos usados para definir usuarios para el "software". Las siguientes situaciones deberán ser revisadas por un apropiado nivel de dirección:

Las identificaciones del usuario para corroborar que sean individuales y no compartidas.
Probar la revocación de usuarios inactivos.
El despliegue de la última fecha y hora en que algún ID específico fue usado. Esta información podrá ayudar para identificar actividades ilícitas.
Revocación o desconexión de identificaciones del usuario siguiendo un número específico de acceso inválido. Este control puede también limitar actividades ilícitas.
El uso de comienzo y fin de fechas para ID de usuario de empleados contratados.
El uso de grupos de usuarios para el recurso de acceso a los archivos. Los usuarios deberán ser asignados a los grupos apropiados.

Procedimientos de autentificación del usuario. Los auditores internos deberán revisar lo siguiente:

Deberá ser evaluado el uso de contraseñas o información personal durante la sesión.
Deberá ser identificada la disponibilidad de automatizar funciones una vez identificado el usuario, así como la autenticación de procedimientos.
Deberá ser identificado el uso de contraseñas por otro personal que no sean los usuarios autorizados.
Los procedimientos para el uso de contraseñas para asegurarse que éste está protegido cuando es usado por el usuario.
La máscara de la contraseña para asegurarse que el área donde los caracteres son tecleados no se desplieguen.

La sintaxis de la contraseña. Algún "software" de control de acceso puede restringir el uso de ciertas palabras o cadenas de caracteres.
El mantenimiento de la historia de la contraseña. Éste puede ser usado para prevenir a usuarios que reutilizan una contraseña por un período específico.
Procedimientos para suplir identificaciones de usuarios y contraseñas por procesos "batch".

Los recursos para controlar e acceso. Los auditores internos deberán revisar lo siguiente:
Posibles niveles de acceso.
Niveles de acceso por "default", particularmente para usuarios o "jobs" que no tienen un ID de usuario.
El acceso del usuario a archivos de seguridad.
Que la seguridad sea implantada en el nivel correcto.
Procedimientos para asegurar la protección automática.
Procedimientos para la protección de recursos.
Uso de rutas rápidas o funciones aceleradas a través de controles.
Controles de acceso sobre aplicaciones locales o remotas.
Restricciones de acceso sobre recursos críticos del sistema, tales como sistemas, programas y aplicaciones en ejecución, librerías del lenguaje, catálogos del sistema y directorios, diccionarios de datos, "logs" y archivos de contraseñas, tablas de definición de privilegios, algoritmos de encriptación y tablas de datos.

Reportes y vigilancia del "software" de control de accesos. EL auditor interno deberá revisar:

"Login", identificación del acceso autorizado al sistema y el uso de recursos.
Las identificaciones de acceso no autorizado.
La identificación de archivos de seguridad, mantenimiento a tabla y el uso de comando sensibles.
El "login" de usuarios privilegiados y sus actividades.
Las restricciones de acceso a archivos de "log" del sistema. Estos archivos frecuentemente contienen las bitácoras de auditoria del control de acceso.
Sistema Operativo o "software" de control de acceso existente
Las violaciones a la seguridad.
Los archivos de seguridad y la generación de reportes de las actividades del usuario para asegurar que los propietarios de datos y recursos son notificados de los eventos de seguridad en un período determinado.

Sistemas operativos. El auditor deberá revisar, evaluar y probar el uso y procedimientos que gobiernan programas, usuarios y funciones del sistema operativo, especialmente los siguientes:

Las facilidades del Sistema Operativo, como son la supervisión y privilegios para programas y usuarios.

Controles de acceso sobre tablas que definen privilegios de usuarios, programas y funciones.
Controles de acceso sobre consolas o terminales maestras y privilegios asociados.
Bitácoras de auditoria.
Posibilidad y uso del control de acceso sobre los "default" de inicio de ID de usuarios y contraseñas.
Comandos de "software" o funciones que son consideradas importante, como mantenimiento de seguridad al archivo de descripciones.
Diagnóstico de utilerías del Sistema Operativo que pueden ser usados para leer o almacenar áreas que contienen información importante.

"Software" del sistema manejador de Bases de Datos. En relación con las funciones del "software" que restringen el acceso a datos y recursos, y los procedimientos que gobiernan el uso de estas funciones, el auditor deberá revisar, evaluar y probar lo siguiente:

Procedimientos usados por el "software" de control de acceso para restringir el acceso a la Base de Datos y al direccionamiento de datos.
El diseño de una restricción de acceso en los archivos por niveles, incluyendo restricciones sobre archivos físicos y lógicos en el DBMS y en el diccionario de datos.
Seguridad de campos, uso de secciones de usuarios y contraseñas y restricciones de acceso.
Si el "software" ejecuta la función de identificación del usuario y procedimientos de autentificación.
Comandos y funciones del diccionario de datos (utilerías del Administrador de la Base de Datos, comandos para modificar DSMS, archivo o definiciones de archivo).
Accesos de los programadores, acceso a DBMS y comandos o funciones del directorio de datos.
Bitácoras de auditoria.
El "software" de desarrollo que afecta la seguridad del DBMS.

El manejador de la Base de Datos y el diccionario de datos usualmente proveen utilerías para revisar e imprimir las capacidades de acceso, información del usuario y bitácoras de auditorias.

"Software" del manejo de librerías. Las funciones del "software" restringen el acceso a librerías críticas; los procedimientos que gobiernan el uso de esas funciones deberán ser revisados; evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:

Documentación de librerías.
Programas fuente(s) y ejecutables.
"Jobs" en ejecución y lineamientos de control.
Parámetros de corrida.
Uso de "software" para restringir el acceso a librerías.
Restricción del acceso a librerías de producción.

Restricciones de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).
Acceso a librerías en prueba.
Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.
Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de "job").
Si el "software" ejecuta funciones de identificación de usuario y procedimientos de autentificación.
Procedimientos inusuales de las librerías.
Capacidades de la bitácora de auditoria.
Los números de versión del "software".

Los reportes escritos pueden ser usados para organizar las actividades de las librerías de "logs" de acceso al "software" manejador de librerías o bitácoras de auditoria.

"Software" de utilerías. El auditor deberá evaluar, revisar y probar los siguientes procedimientos diseñados para limitar el acceso a comandos de utilerías o funciones:

Funciones o comandos de utilerías.
Los controles de acceso sobre comandos o funciones de utilerías.
Seguridad de acceso a los programadores para la utilización de funciones o comandos de utilerías.
Si el "software" ejecuta las funciones de identificación del usuario y procedimientos de autentificación.
Capacidades de uso de utilería para cada grupo de usuarios.
Bitácoras de auditorias.

El "software" de utilerías no provee bitácoras de auditoria, por ello debe usarse el reporte escrito del "software", para lo cual puede utilizarse el "software" de control de acceso, si éste está integrado al "software". Deberán usarse reportes para monitorear el control de acceso.

"Software" de telecomunicaciones. El auditor deberá revisar, evaluar y probar si es posible usar las funciones del "software" que restringe el acceso en las redes de telecomunicaciones y los procedimientos que gobiernan su uso, especialmente los siguientes:

Restricciones al acceso de la red basados en tiempo, día, usuario, lugar y terminal.
Apagado automático de terminales inactivas en un tiempo específico (terminales que pueden ser usadas).
Facilidad de acceso no autorizado basado en protocolos de transmisión y líneas para la conexión rápida.
Números de seguridad de entrada (revisar la posibilidad de este número para acceso local o tableros de boletín nacional).

"Autorrespuesta", facilidad de uso sobre módem.
Horas durante las cuales la línea está disponible.
Recursos y funciones posibles a través del acceso de entrada.
Uso de identificación de la terminal físicamente.
Controles de acceso sobre los recursos de la red.
Controles de acceso sobre tablas de configuración de red.
Controles de acceso a funciones de la red.
Seguridad física sobre líneas telefónicas y telecomunicaciones.
El uso de red de área local (LAN) y la conectividad para otras redes de área local (LAN), redes de área amplia (WAN) o redes en otro lugar.
Si el "software" ejecuta las funciones de la identificación del usuario y procedimientos de autentificación.
Procedimientos para la protección de comunicaciones (desde las conexiones hasta la recepción no autorizada).
Posibilidad y uso de encriptación de datos o mensajes técnicos de identificación.

Los reportes escritos pueden ser usados para reportar las actividades de la red, de "logs" de acceso a "software" de telecomunicaciones o bitácoras de auditoria. Éstos pueden además hacerlo con el "software" de control de acceso. Los reportes especiales de auditoria deberán contener lo siguiente:

Personal registrado por el sistema en el que no corresponde la contraseña con su identificador, o el que ha intentado más de dos veces entrar al sistema sin una contraseña autorizada.

Identificaciones de usuarios no usados hace seis meses.
Identificaciones de usuarios con privilegios especiales.
Un reporte de referencias cruzadas que debe mostrar a los ID usuarios con cada acceso a las aplicaciones.
Listar todos los ID usuarios por grupos.

IV. 5.- Encriptamiento.

Encriptar es el arte de proteger la información transformándola con un determinado algoritmo dentro de un formato para que no pueda ser leída normalmente, (Derrien, 1994). Sólo aquellos usuarios que posean la clave de acceso podrán "desencriptar" un texto para que pueda ser leído. Las tecnologías modernas de encriptamiento hacen casi imposible que una persona no autorizada utilice la información.

Encriptar (Fisher, 2002), es la transformación de los datos a una forma en que no sea posible leerla por cualquier persona, a menos que cuente con la llave de

descripción. Su propósito es asegurar la privacidad y mantener la información alejada de personal no autorizado, aun de aquellos que la puedan ver en forma encriptada.

Debido a que Internet y otras formas de comunicación electrónica se han convertido en algo normal y rutinario, la seguridad se ha convertido en un factor muy importante. El encriptamiento se usa para proteger mensajes de correo electrónico, firmas electrónicas, llaves de acceso, información de tipo financiero e información confidencial. Existen en el mercado diferentes paquetes y formas para encriptar la información.

Los sistemas de encriptamiento pueden ser clasificados en sistemas de llave simétrica, los cuales usan una llave común para el que envía información y para el que la recibe, y sistemas de llave pública, el cual utiliza dos llaves, una que es pública, conocida por todos, y otra que solamente conoce el receptor.

Para generar una firma digital, se usan algunos algoritmos públicos. La firma digital es un conjunto de datos que son creados usando una llave secreta, aunque existe una llave pública que es usada para verificar que la firma fue realmente generada usando la llave privada correspondiente. El algoritmo usado para generar la firma electrónica es de tal naturaleza, que si no se usa la llave secreta no es posible usar la firma electrónica.

La autenticación en sentido digital es el proceso por medio del cual el emisor y / o receptor de un mensaje digital confidencial tiene una identificación válida para enviar o recibir un mensaje. Los protocolos de autentificación pueden estar basados en sistemas convencionales de encriptamiento de llaves secretas, o en sistemas públicos de encriptamiento. En la autenticación de sistemas de llaves públicas se usan las firmas digitales.

La firma digital tiene la misma función que la firma escrita en cualquier documento. La firma digital es un fragmento de información confidencial y propia de cada usuario que asegura a la persona que envía o autoriza un documento. El receptor o terceras personas pueden verificar que el documento y la firma corresponden a la persona que lo firma, y que el documento no ha sido alterado.

La firma digital es usada para verificar que el mensaje realmente viene de la persona que se señala como la que lo envía. También puede ser usada para certificar que una persona envió un documento o una autorización en un tiempo determinado. Existe una serie de firmas digitales que identifican y certifican desde el usuario inicial hasta el último usuario. En el caso de envío de documentos pueden certificar la organización que envía el documento, su departamento y la persona que lo manda o autoriza.

Un sistema seguro de firmas digitales debe comprender dos partes: un método para firmar el documento que sea de tal manera confiable que no pueda ser usado por

otras personas, y otro que verifique que la firma fue realmente generada por el que ella representa, de tal forma que posteriormente no pueda ser cuestionada.

El resultado de un conjunto de datos encriptados es la firma digital. Normalmente, junto con la información, la llave pública que es usada para firmar. Para verificar la información, el receptor primero determina si la llave pertenece a la persona a la cual debe pertenecer, y después de desencriptarla verifica si la información corresponde al mensaje, entonces la firma es aceptada como válida.

Criptoanálisis es el arte de desencriptar comunicaciones sin conocer las llaves apropiadas. Existen muchas técnicas para lograrlo, y entre las más comunes están:

Ataque a textos encriptados. Ésta es una situación en la cual el atacante no conoce nada acerca del contenido del mensaje, y debe trabajar únicamente en el contenido del mensaje. En la práctica es muy posible adivinar el contenido de algún texto, ya que normalmente tienen encabezados fijos.
Ataque conociendo el texto original. El atacante conoce o puede adivinar el contenido del texto debido a algunas partes del texto encriptado. El objetivo es desencriptar el resto del texto usando esta información. Esto también puede ser hecho al determinar la llave usada para desencriptar
Ataque hecho por medio de escoger un texto encriptado. El atacante tiene el objetivo de determinar la llave con la cual se encriptó el texto.
Atacar en la parte central. Este tipo de ataque es relevante para la comunicación criptografiada y para los protocolos clave de intercambio. La idea es que cuando dos personas están intercambiando llaves de seguridad para lograr la comunicación, el atacante se pone en medio de la línea de comunicación. El atacante realiza un intercambio separado de laves. Posteriormente, el atacante, con las llaves de acceso, puede realizar cualquier función. Una forma de prever este tipo de ataques es encriptar la llave de acceso al momento de enviar, así, una vez enviada, el emisor y receptor verifican la firma digital para realizar las operaciones necesarias.
Ataque en el tiempo. Éste es un nuevo tipo de ataque y está basado en la medición repetitiva de los tiempos exactos de ejecución.

Aunque existen diversas formas para atacar la información encriptada, es conveniente que el programador conozca las formas de encriptamiento, sus ventajas y desventajas, así como su costo, para determinar la mejor para cada uno de los sistemas, y que el auditor verifique la forma de encriptamiento y su seguridad de acuerdo con los requerimientos de seguridad de cada sistema. Existen diferentes protocolos y estándares para la criptografía, entre los cuales están:

DNSSEC (Domain Name Server Security). Éste es un Protocolo para servicio seguro de distribución de nombres.
GSSAPI (Generic Security Services, API). Provee una autentificación genérica, llaves de intercambio e interfases de encriptamiento para diferentes temas y métodos de autentificación.

SSL (Secure Socket Layer). Es uno de los dos protocolos para una conexión segura a la web.
SHTTP (Secure Hypertext Transfer Protocol). Protocolo para dar más seguridad a las transacciones de web.
E-Mail (Security and Related Services).
MSP (Message Security Protocol).
PKCS (Public Key Encryption Standards).
SSH2 (Protocol).
Algoritmos de Encriptamiento.
DIFFIE HELLMAN.
DSS (Digital Signature Standard).
ELGAMAL.
LUC.
Simétricos.
DES
BLOWFISH.
IDEA (International Data Encryption Algorith).
RC4.

Varios algoritmos de llave pública, algunos con promisorio futuro; sin embargo, el más popular es el RSA (Rivest Shamir Adelman). En algoritmos simétricos el más famoso es el denominado DES y su variante DES-CBC, pero el más reciente es RC4.

CONCLUSIÓN.

La Seguridad Informática es un paradigma que en el gobierno se ha manejado desde hace mucho tiempo, pero que es emergente en la Industria e Instituciones Educativas.

La Seguridad Informática no es crear un sistema y ya se resolvió el problema; sino que es un sistema que debe estar en constante transformación, y así como evolucionan los ataques informativos también este Sistema debe estar teniendo siempre nuevas modificaciones, estando prevenidos y adaptándose a los nuevos ataques de virus que surjan. Es por eso que se habla de la consecución e implantación de procesos de Seguridad Informática. Este nuevo enfoque hace que los líderes de este tipo de proyecto dependan más del avance tecnológico y de cómo se vincula la solución de distintos procesos como: los temas de Control de Acceso, Telecomunicaciones y la Seguridad de la Red, Administración de la Seguridad, en Aplicaciones y Desarrollo, Recuperación de Desastres, Criptografía, Investigación y ética, así como de los Modelos y Arquitecturas de Seguridad; etcétera.

Por consiguiente, hay que administrar los proyectos de acuerdo al tamaño y al lugar que tiene asignado cada integrante para desempeñarse en proyectos pequeños o en proyectos de gran alcance donde estén en juego compañías, personas, distribuidores, fabricante, proveedores, etcétera.

Teniendo en cuenta todos estos procesos y llevándolos a cabo como debe de ser una Red de Ordenadores, no se tendrán tantos problemas, que de otra manera sí podrían afectar al entorno de red tal y como se mencionó en los párrafos anteriores.

FUENTES DE CONSULTA

Banke, A. y Badrinath, B. (1995).
I-TCP: Indirect TCP for Mobile Hosts.
New York: Prentice- Hall.

Barlow, J. P. (1995).
Property and Speech: Who Owns Whay You Say in Cyberspace.
USA: Commun of the ACM, vol. 38.

Beltrao, A. (1998).
Redes de Computadoras. Protocolos y Prestaciones.
México: Mc Graw-Hill. Primera Edición.

Black, U. D. (1994).
Emerging Communication Technologies.
New Jersey: Prentice-Hall, Englewood Cliffs.

Black, U. D. (1995).
TCP/IP and Related Protocols.
New York: Mc Graw-Hill.

Black, Ulysees. (1999).
Redes de Computadoras: Protocolos, Normas e Interfases.
México: Mc Graw-Hill.

Carl-Mitchell, S. y Quarterman, J. S. (2001).
Practical Internetworking with TCP/IP and UNIX.
New Jersey: Addisson Wesley.

Clark, D. (1998).
Window and Acknowledgement Strategy in TCP.
New Jersey: Prentice Hall, Englewood Cliffs.

Comer D. E. (1995).
Internetworking with TCP/IP.
New Jersey: Prentice-Hall, Englewood Cliffs.

Deening, P. J. (1989).
The Science of Computing: Worldnet.
USA: In American Scientist, 432-434.

Frank, H. y Frish, J. (1991).
Communicion, Transmission and Transportation Networks.
Massachusetts: Addison-Wesley.

Giozza, W.; De Araújo, J. y Moura, J. (1996).
Redes Locales de Computadores: Aplicaciones y Tecnologías.
México: Mc Graw-Hill.

González, Néstor. (1999).
Comunicaciones y Redes de Procesamiento de Datos.
México: Mc Graw-Hill.

Green, Paul. (1992).
Computer Network Architectures and Protocols.
New York: Plenum Press, Second Edition.

International Organization for Standarization. (1987a). Information Processing Systems –Open Systems Interconnection-
Specification of Basic Specification of Abstract Syntax Notation One (ASN.1). International Standar number 8824, ISO, Switzerland.

International Organization for Standarization. (1987b). Information Processing Systems –Open Systems Interconnection –
Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). International Standard number 8825, ISO, Switzerland.

International Organization for Standarization. (1988a). Information Processing Systems –Open Systems Interconnection- **Management Information Protocol Definition, Part 2: Common Management Information Protocol.** Draft International Standard number 9596-2.

Latif, A., Rowlance, E. J. y Adams, R. H. (1992).
The IBM LAN Bridge.
IEEE Network Magazine.

Madrón, A. (1997).
Redes de Computadoras. México: Mc Graw-Hill.

Menascé, D. A. y Schwabe, D. (1994).
Redes de Computadoras. Buenos Aires: Ed. Campus.
Milenkovic, Anton. (1998). **Sistemas Operativos**. México: Mc Graw-Hill.

. Novel, Inc. (1995).
Introducción a Novel: Manual de Referencia.
México: Novel Incorporation.

Perlman, R. (1992).
Interconnections: Bridges and Routers.
New Jersey: Addisson Wesley.

Rosenthal, R. (Ed.).
The Selection of Local Area Computer Networks.
USA: National Bureau of Standards Special Publications.

Schwartz, M. y Stern, T. (1999).
IEEE Transactions on Communications. USA: COM-28 (4), 539-552.

SNA, (1995). **IBM System Network Architecture – General Information.**
North Carolina: IBM System Development Division, Publications Center Department.

Tabembaum, Andrews. (1997).
Redes de Computadoras.
México:Pearson/Prentice-Hall. Tercera Edición.

Tanenbaum, A. (1981).
Computer Networks: Toward Distributed Processing Systems.
New Jersey: Prentice-Hall, Englewood Cliffs.

Tanenbaum, A. S. (1991).
Computer Networks.
New Jersey: Prentice Hall, Ebglewood Cliffs.

Villamizan, C. y Song, C. (1995). **High Performance TCP in ANSNET.** USA: Mc Graw-Hill.

Summers, Rita C
Secure Computing Threads and Safeguards;
McGraw Hill; (1997).

Denning, Dorothy; *Information Warfare and Security*; Adison Wesley; (2000).

Security Fundamentals
EDS University

Malware Fundamentals
EDS University

Simson Garfinkel and Gene Spafford
Practical Unix & Internet Security
O'Reilly

Stuart McClure-Joel Scambray-George Kurtz
Hacking Exposed
McGraw-Hill

Denning, Dorothy
Information Warfare and Security
Adison Wesley; (2000).

Krause, Micki; Tipton, Harold F
Information Security Management Handbook, Fourth Edition
;CRC Press - Auerbach Publications; (2000).

Denning, Dorothy;
Information Warfare and Security
Adison Wesley; (2000)

Davis, Duane
Business Research for Decision Making Fith Edition
Duxbury Thomson Learning; (1999).

Redja, George, E.
Principles of Risk Management and Insurance Seventh Edition
Addison Wesley; (2000)..