INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

ESCUELA DE TELEMÁTICA

AMPLIACIÓN LA RED INTRANET DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO.

POR:

CBOS. SANTAMARÍA PAZMIÑO SHONY LEONEL

Tesis presentada como requisito parcial para la obtención del Título de:

TECNÓLOGO EN TELEMÁTICA

2003

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. CBOS. SANTAMARÍA PAZMIÑO SHONY LEONEL, como requerimiento parcial a la obtención del título de TECNÓLOGO TELEMÁTICO.

Ing. Marco Silva Segovia

DIRECTOR

Latacunga, 05 de marzo del 2003

DEDICATORIA

Quiero dejar testimonio de eterna gratitud a DIOS el infinito creador, a mis PADRES que con su trabajo sacrificado año tras año me han brindado su apoyo en mi anhelo permanente de superación, y, al Instituto por permitirme enriquecerme de conocimientos.

Hoy después de un tiempo de haber aprendido más de la experiencia, entre aciertos y errores ponga a vuestra consideración mi trabajo de investigación, que tiene como propósito principal el de aportar una información veraz y eficiente a las futuras promociones de estudiantes.

CBOS. Santamaría Shony

AGRADECIMIENTO

El más grande agradecimiento a mi MADRE porque ha sido el pilar fundamental para la culminación de mis estudios, por ser la forjadora de mis días y por guiarme hacia el camino del bien y la superación profesional.

Al Instituto Tecnológico Superior Aeronáutico, por haberme abierto sus puertas para formarme como militar y profesional, a todos los MAESTROS que día a día supieron sembrar en mí sus conocimientos, y, en especial al Ing. Marco Silva Segovia quien con su aporte profesional como Director de Tesis me guió para llegar a feliz culminación.

CBOS. Santamaría Shony

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE GRÁFICOS

INTRODUCCIÓN

El Instituto Tecnológico Superior Aeronáutico en su afán de ir a la par con los avances de la tecnología actual, ha creído conveniente implantar en sus instalaciones una red Intranet, que debido al crecimiento vertiginoso de las dependencias de la Institución, se ha visto necesario realizar su ampliación para una mejor cobertura.

La notable tendencia del crecimiento de las intranets es la respuesta espontánea a una necesidad vital para el mundo empresarial contemporáneo: disponer de un eficiente y confiable mecanismo para la comunicación interna. Por ello, e independientemente de lo que se pueda pensar, las motivaciones empresariales que demandan de forma creciente soluciones intranets no están sujetas a una moda, sino que responden a un prolongado proceso evolutivo técnico/organizativo de las redes, en el cual las intranets son sólo una simple parte.

La tecnología internet, a pesar de las limitaciones que aún posee, representa los cambios más importantes en las comunicaciones desde la invención del teléfono. No es casual ni exagerado que los expertos y analistas del sector la traten como sinónimo de telefonía del siglo XXI. Por ello, en tanto que las intranets constituyen la aplicación de dicha tecnología en las funciones internas de las organizaciones, su dominio e implementación significa avanzar por la ruta del progreso de las comunicaciones.

CAPÍTULO I

EL PROBLEMA

1.1. Planteamiento del problema

La tecnología de las intranets está transformando la cultura de las corporaciones internacionales, capacitando a empleados en todo el mundo para entender temas claves que enfrentan en su trabajo, para intercambiar ideas en tiempo real y para colaborar en la aportación de soluciones, sin importar la localización geográfica o la hora.

La parte fundamental es el mejoramiento de las comunicaciones y la creatividad, además del desarrollo o el surgimiento de trabajadores con nociones sobre el pensamiento crítico. Es así, como el Instituto Tecnológico Superior Aeronáutico pretende estimular las ideas sobre la manera de utilizar un concepto de red en evolución, la intranet, para convertir a este Instituto en una organización con una red integrada, global y con inteligencia humana.

1.2. Definición del problema

Ampliación de la Red Intranet del Instituto Tecnológico Superior Aeronáutico.

1.3. Objetivos

1.3.1. General

Ampliar la red Intranet del Instituto Tecnológico Superior Aeronáutico.

1.3.2. Específicos

- Realizar la ampliación de la red Intranet a todas las oficinas del Instituto con implementos de tecnología de punta.
- Dotar a los encargados de las diferentes dependencias del Instituto de un medio eficaz y confiable de flujo de información.
- Implementar la red Intranet con los equipos necesarios que permitan la apertura de la red hacia el exterior.

1.4. Justificación

El Instituto Tecnológico Superior Aeronáutico consciente de que no puede implantar la tecnología por amor a la tecnología, ha creído conveniente coincidir las ideas, la misión y las metas del Instituto para identificar la mejor forma de que éste evolucione y madure, hasta dar forma a una organización propia del siglo XXI, y que aplicando la tecnología lleve a realidad sus planes para el futuro.

No hay necesidad de aplicar la reingeniería a la organización ni de modificar las habilidades de grandes fuerzas de trabajo. Lo principal es acercar la toma de decisiones a la gente que sabe identificar las oportunidades y que posee la capacidad de reaccionar rápida y

eficientemente, para que definan las acciones, se dé solución a los problemas y se asuman las responsabilidades. Cuando un problema necesita una solución de tipo organizacional, los usuarios pueden tener acceso a la experiencia, la capacidad y la riqueza de otros a través de la intranet, con el objetivo de aplicar todos los recursos al problema.

1.5. Alcance

Lo importante de la ampliación de la Intranet del Instituto Tecnológico Superior Aeronáutico es la integración de la mayoría de las dependencias que integran éste, dando cumplimiento al objetivo que persigue las Intranets para beneficio y engrandecimiento del Instituto regentado pro la Fuerza Aérea Ecuatoriana.

CAPÍTULO II

MARCO TEÓRICO

2.1. Redes

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de mas

sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo 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 interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

2.2. Tipos de redes

Las redes se pueden clasificar de acuerdo a diversos criterios, como son:

- De acuerdo a su tecnología
- Según su ámbito de influencia

2.2.1. De acuerdo a su tecnología

De acuerdo a su tecnología de transmisión, las redes se clasifican en:

Redes Broadcast (radiodifusión)

Redes punto a punto

a) Redes Broadcast

En las redes broadcast, el medio de transmisión es compartido por todos los terminales interconectados. Normalmente cada mensaje transmitido es para un solo destinatario, pero para saberlo, cada terminal de la red a de recibir cada uno de los mensajes, analizar la dirección de destino y averiguar si lo tiene que recibir o no.

En una red broadcast el camino a seguir de un terminal a otro es único, no existen terminales intermedios y el grado de ocupación es el mismo para todos ellos.

Si en una red tipo broadcast lo que se quiere es precisamente enviar un mensaje a todos los terminales conectados a él, esta acción se denomina hacer un envío broadcast. Asimismo es posible enviar un mensaje dirigido a un subgrupo de algunos de los terminales de la red (subgrupo que ha de estar definido previamente); a este se conoce como hacer un envío multicast (y el anterior grupo de terminales se denomina grupo multicast). Ejemplos de redes broadcast pueden ser casi todas las tecnologías de red local: Ethernet (en sus diversos tipos), Token Ring, FDDI, las basadas en transmisión vía satélite, etc. En una red broadcast la capacidad o velocidad de transmisión hace

referencia a la conjunta de toda las máquinas conectadas a la red; por ejemplo, la red conocida como Ethernet tiene una velocidad de 10 mbps, lo cual significa que la cantidad máxima de tráfico conjunto de todos los terminales conectados no puede superar los 10 mbps.

b) Redes Punto a Punto

Las redes punto a punto se construyen por medio de conexiones entre pares de terminales. La gran mayoría de los enlaces en línea punto a punto son dúplex simétricos. Así, cuando se hablan de un enlace de 64 kbps sin especificar más, se quiere decir una capacidad de 64 kbps en cada sentido, por lo que la capacidad total del enlace sería de 128 kbps.

Al unir múltiples terminales con líneas punto a punto es posible llegar a formar redes de topologías complejas en las que es difícil averiguar cuál es la ruta óptima a seguir para ir de un punto a otro, ya que puede haber muchísimos caminos posibles. Cada uno de los terminales que participa en una red de enlaces punto a punto es un nodo de la red. Si el nodo tiene un único enlace se dice que es un nodo terminal o «end node», de lo contrario se dice que es un nodo intermedio, de encaminamiento o «routing node». Cada nodo intermedio ha decidir por donde debe dirigir los paquetes que reciba, con lo que tambi{en se les

llama nodos de conmutación de paquetes, nodos de conmutación, conmutadores o encaminadores.

El conjunto de líneas de comunicación y encaminadores que comunican los nodos terminales forman lo que se conoce como la subred de comunicaciones, o simplemente subred. Obsérvese que los host o nodos terminales no forman parte de la subred. Una analogía con la subred telefónica que la subred es el conjunto de líneas y centralitas telefónicas, incluida la roseta donde conectamos el teléfono, pero no formaría parte de la subred el terminal telefónico que conectamos a la roseta.

Cuando un paquete se envía de un nodo al siguiente, normalmente el paquete es transmitido en su totalidad y almacenado; sólo entonces el nodo receptor intenta enviar el paquete al siguiente nodo de la red. Esto es lo que se conoce como una red de conmutación de paquetes.

2.2.2. Según su ámbito de influencia

a) Redes LAN

Su desarrollo fue en los años ochenta son redes de propiedad privada que funciona dentro de una oficina, edificio o terreno hasta unos cuantos kilómetros general mente son usados para conectar computadores personales y estaciones de trabajo en una compañía y su objetivo es compartir recursos e intercambio

de información. Las redes de área local se distingue de otro tipo de redes por su tamaño cableado y tecnología de transmisión. Generalmente una red LAN es de tamaño restringido, limitando el tiempo de transmisión, lo cual hace factible que el diseño de la red simplifique las administración. Las redes LAN generalmente usan una tecnología de trasmisión que consiste en un cable sencillo, al cual se encuentra conectados todos los computadores, la velocidad de transmisión de las redes de área local oscila entre los 10 / 100 Mbps (megabit por segundos, un mega bits son 1000000 de bits). En los últimos años se han mejorado los estándares de cableado para incrementar la velocidad de transferencias sobre cables de cobre par trenzado, esto facilita la decisión del cable ha utilizar ya que el cable de par trenzado es mas barato que el cable coaxial y ofrece una velocidad superior de transmisión. Para ayuda de los instaladores de cableado a tomar las decisiones, la EIA/TIA (Electronic Industries Association / Telecomunication Industries Association) desarrollo un estándar de cableado denominado EIA/ TIA 568 comercial Building Wiring Estándar, que es un conjunto de especificaciones para el sistema de cableado de comunicaciones.

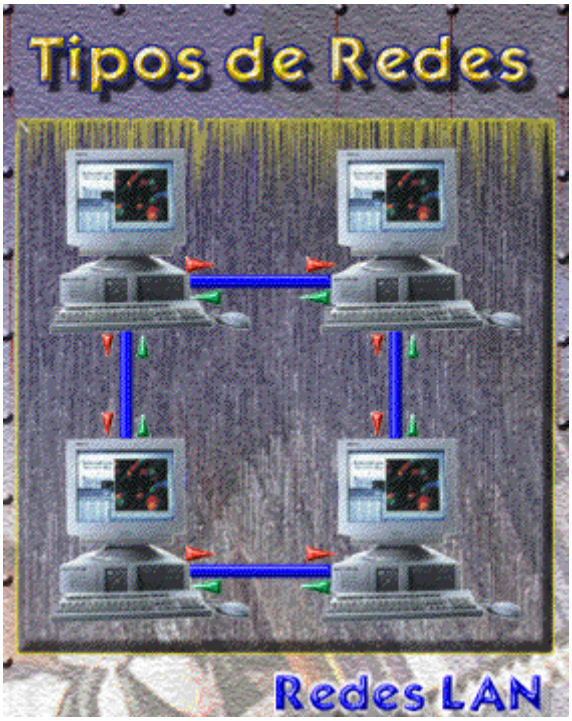


Fig. 2.1. Red LAN

b) Redes MAN

Es básicamente una versión más grande de las redes de área local con una tecnología bastante similar. Una rede de área metropolitana puede manejarse voz y datos e incluso podría estar relacionada con la red de televisión local por cable. Este estándar define un protocolo de gran velocidad, en donde los computadores conectados comparten un bus doble de fibra óptica utilizando el método de acceso llamado bus de cola distribuido. El distinguir las redes MAN en una categoría especial indica que se ha adoptado un estándar especial por ello se a demoninado DQDB (DISTRIBUITED QUEUE DUAL BUS o BUS DUAL DE COLA DISTRIBUIDO), que consiste en

dos cable ópticos unidireccionales donde están conectados los computadores.

Fig. 2.2. Red MAN

c) Redes WAN

Es una red de gran alcance con un sistema de comunicaciones que interconectan redes geográficamente remotas utilizando servicios proporcionados por las empresas de servicio público como comunicación vía telefónica o en ocasiones instalados por una misma organización. Una rede que se extiende por una área geográfica extensa (Ciudades Pises Continentes)mantiene computadores con el propósito de ejecutar ampliaciones a estos computadores se denominan HOSTS. Los Hosts se encuentran conectados a subredes de comunicación, cuya función es conducir mensajes de un Hosts a otro, a diferencia del sistema

telefónico que conduce voz, los Host conducen datos utilizando los misma vía (Red Telefónica).

Una red WAN también tiene la posibilidad de comunicarse mediante un satélite o radio utilizando antenas las cuales efectúan la transmisión y la recepción. Por lo general las redes satelitales son de difusión.

Fig. 2.3. Red WAN

d) Redes INALAMBRICAS

Los computadores portátiles son el segmento más rápido de crecimiento del industria de la computación los usuarios móviles de estos pequeños computadores quieren estar conectados en línea a su base de operaciones y necesitan obtener datos para su aplicación sin estar atados a las comunicaciones terrestres en algunos casos el obtener una conexión para cable es imposible en por ejemplo automóviles, por lo tanto se concentra su interés en las redes inalámbricas.

Las redes inalámbricas se basan en el principio de conectar una antena a un circuito electrónico en donde las ondas electromagnéticas se difunden para captarse en un receptor a cierta distancia. Las redes inalámbricas son de gran importancia para los transportadores de carga pesada y pasajero, vehículos de servicio público, personas que afectan reparaciones en sitios de difícil acceso y para los militares la instalación de redes inalámbricas es relativamente fácil, presentan algunas desventajas como su velocidad de transmisión y recepción que puede alcanzar de uno a dos Mbps lo cual es mucho mas lento que en redes de área local y redes de largo enlace en algunas ocasiones las redes inalámbricas presentan interferencias de comunicación.

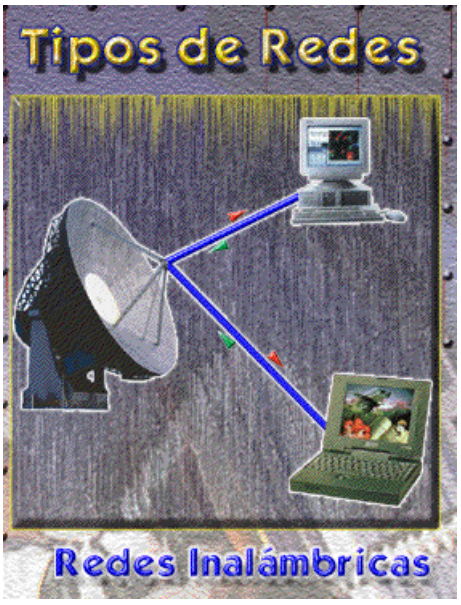


Fig. 2.4. Redes Inalámbricas

e) Red INTERNET

Internet o red de redes es la mayor de las redes de computadores existentes en el mundo compuestas por millares de computadores conectados entre si.

Uno de los aspectos más importante de Internet es que utiliza una base tecnológica y protocolos de comunicación que son abiertos (No tiene un propietario exclusivo) permite la comunicación integrada entre computadores de distintos fabricantes.

Sorprendentemente Internet no tiene dueño y ha surgido gracias a la colaboración entre académicos, investigadores y empresas de todo el mundo.

Fig. 2.5. Red Internet

2.3. Topologías de red

Los nodos de la red necesitan estar conectados para comunicarse. A la forma en que están conectados los nodos se le llama topología. Una red tiene dos diferentes topologías: una física y una lógica. Una topología física es la disposición física actual de la red, la manera en que los nodos están conectados unos con otros. La topología lógica es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la red. Las topologías física y lógica pueden ser iguales o diferentes.

2.3.1. Topología de bus

En esta topología hay un cable que recorre todas las máquinas sin formar caminos cerrados ni tener bifurcaciones. Eléctricamente, un bus equivale a un nodo pues los transceptores de todas las máquinas quedan conectados en paralelo. A los efectos de mantener la impedancia constante en el cableado de la red, se deben conectar dos "terminadores" en ambos extremos del cableado de la misma.

VENTAJAS

- Es fácil controlar el flujo de tráfico entre los distintos computadores.
- Un estación puede difundir la información a todas las demás.
- Permite conectar conmutadores para conectar un nodo en caso de que falle.

DESVENTAJAS

- Existe un solo canal de comunicaciones.
- Si el canal de comunicaciones falla el canal deja de funcionar.

- Dificultad de aislar las averías de los componentes individuales conectados al bus.

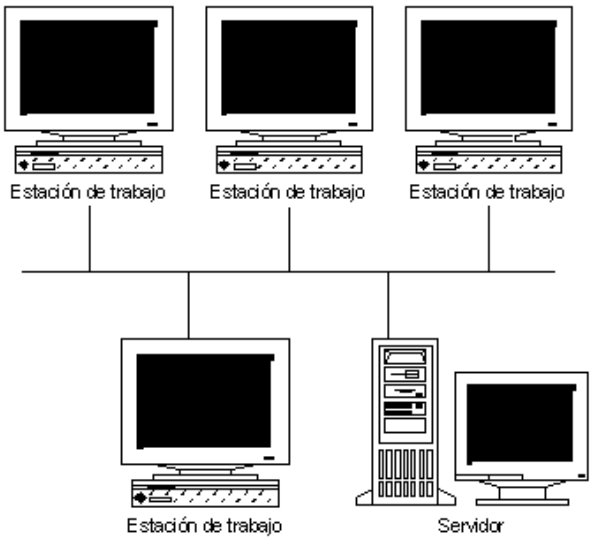


Fig. 2.6. Topología en Bus

2.3.2. Topología de anillo

En este caso, las líneas de comunicación forman un camino cerrado. La información generalmente recorre el anillo en forma unidireccional, cada máquina recibe la información de la máquina previa, la analiza, y si no es para ella, la retransmite a la siguiente.

VENTAJAS

- Es raro los embotellamientos
- Capacitad de conectar conmutadores para redirigir los datos, saltándose el nodo averiado.
- El montaje de la red es relativamente simple

DESVENTAJAS

- Los nodos están unidos por un mismo canal

- Si falla el canal entre dos nodos toda la red se interrumpe
- Los datos fluyen en una sola dirección

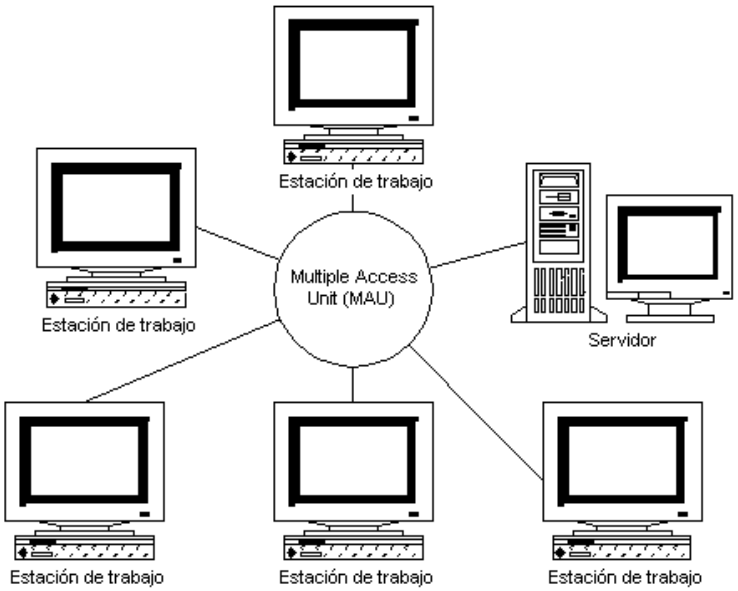


Fig. 2.7. Topología en Anillo

2.3.3. Topología de estrella

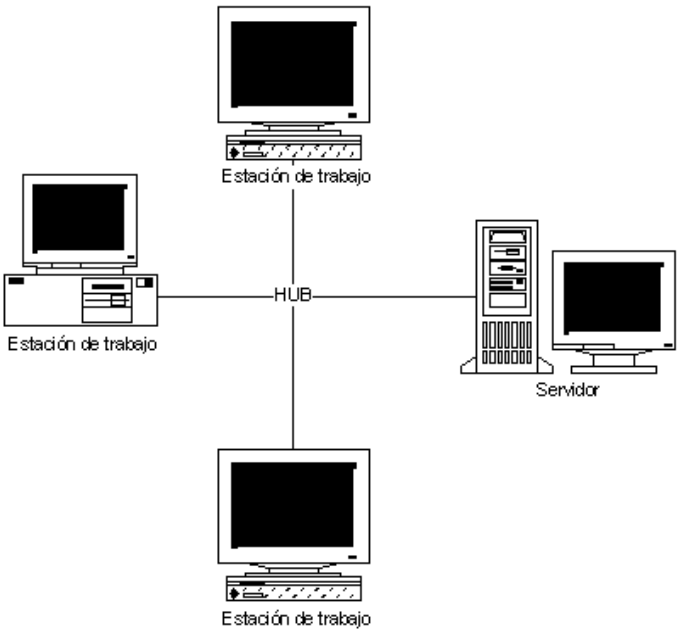
Se la llama así pues hay un centro denominado hub hacia el cual convergen todas las líneas de comunicación. Cada máquina tiene un enlace exclusivo con el hub. Los sistemas host- terminales también usan una topología estrella, con el host en el centro, pero se diferencian por la forma de comunicación. En las LANs, el hub es un dispositivo que, sea activo o pasivo, permite que todas las estaciones reciban la transmisión de una; en los sistemas con host, sólo el host recibe. En una red, la comunicación entre dos estaciones es directa; en un sistema con host, una terminal se comunica con el host y el host con la otra.

VENTAJAS

- El software no es complicado
- El flujo de tráfico es sencillo
- Puede aislar un nodo en caso de averías

DESVENTAJAS

- Serios problemas de fiabilidad
- Capacidad de procesamiento distribuido limitado
- Puede sufrir saturaciones y saturaciones en caso de avería del nodo central.



2.8. Topología en Estrella

2.4. Modelos de referencia

2.4.1. El modelo OSI

En 1984 la Organización de Estándares Internacionales (ISO: Internacional Standards Organization), junto con el CCITT (Consultative Committee on internacional Telegraphy and Telephony) desarrollaron el modelo OSI (Open Systems Interconnection), que consiste en un conjunto de niveles funcionales, en los que cada nivel tiene sus propios protocolos de

comunicaciones para facilitar la comunicación entre las redes de computadoras.

El modelo OSI considera siete niveles funcionales con los que se diseña el software de comunicaciones. La instauración de dicho modelo, aparte de los beneficios que trae consigo, facilita el reemplazo de piezas, la escalabilidad de los equipos y la administración de los recursos que conforman a las redes de área local (LAN).

OSI fue conceptualizado como el software que maneja la transmisión de los mensajes de una terminal o programa aplicativo, con otra terminal o programa aplicativo, separados e interconectados en una red.

Está basado en el concepto de aplicaciones distribuidas cooperativas. En este modelo un sistema se compone de una computadora, todo su software y cualquier periférico conectado a ella, incluyendo terminales tontas. Una aplicación distribuida es cualquier actividad que involucre el intercambio de información entre dos sistemas abiertos.

Este modelo está dirigido al intercambio de información entre dos sistemas abiertos, como se dijo anteriormente, más que al funcionamiento interno de los mismos. La visión para el futuro del modelo OSI es poder conectar cualquier equipo de comunicación de datos y cualquier tipo de software con otros equipos y software, sin importar qué compañía los fabricó, y así poder minimizar el trabajo del usuario final y la complejidad al momento de la interoperabilidad de las redes y de los sistemas actuales.

Fig. 2.9. El modelo OSI

Nivel Físico (Physical Layer)

El nivel físico es la capa más baja y también la más antigua, se encarga de proporcionar los medios físicos y de procedimiento para crear y desactivar las conexiones físicas para la transmisión de bits entre entidades.

Esta capa transmite los bits entre dos entidades directamente conectadas. Regula aspectos de la comunicación, como el tipo de señal, el esquema de codificación, el modo de comunicación (dúplex, semidúplex o símplex). Si la información se transmite por señales eléctricas, se especifican los voltajes permitidos y su significado (1 ó 0) y de una manera análoga en el caso de la fibra óptica. Se especifican las características mecánicas del conector, la señalización básica, etc.

Es fundamental recordar que el nivel 1 es la base de la conexión, la más importante y por donde la información se transmite proveniente de y hacia todos los niveles. El nivel 1 está relacionado únicamente con hardware, mientras que los niveles del 2 al 7 están relacionados sólo con software.

El nivel físico define la forma en la que el cable se conecta a la tarjeta de red; por ejemplo, cuántos pines debe tener el conector y la función de cada uno de ellos. También define la técnica de transmisión que se usará para enviar la información a través del medio de transmisión de la red.

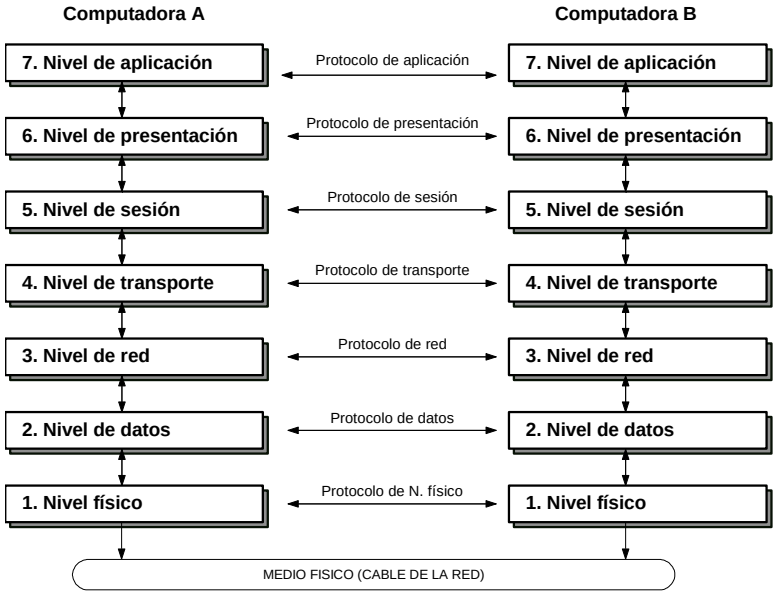


Fig. 2.10. Relación del modelo OSI

Nivel de datos (Data Link Layer)

El nivel de datos es donde los bits tienen algún significado en la red y puede equipararse con el departamento de recepción y envío de una compañía manufacturera, el cual debe tomar los paquetes que recibe del nivel de red y prepararlos en la forma correcta (tramas) para poder enviarlos (transmitirlos) por el nivel físico.

De igual forma sucede cuando recibe paquetes (bits) del nivel físico y tiene que ponerlos correctamente (tramas) para verificar si la información que está recibiendo está libre de errores, si los paquetes vienen en orden, si no faltan algunos de ellos, etc., para poder entregarlos al nivel de red sin ningún error.

Dentro de sus funciones se incluyen la de notificar al emisor (la computadora remota) si algún paquete (tramas) se recibió en mal estado (basura), o si se omitieron algunas de las tramas y se requiere que sean enviadas nuevamente (retransmisión); de igual manera se debe notificar si una trama está duplicada o si llegó sin problemas. Es responsable de saber en dónde comienza la transmisión de la trama y dónde termina, asó como de garantizar hasta qué punto tanto la computadora emisora como la receptora están sincronizadas y si emplean el mismo sistema de codificación y decodificación.

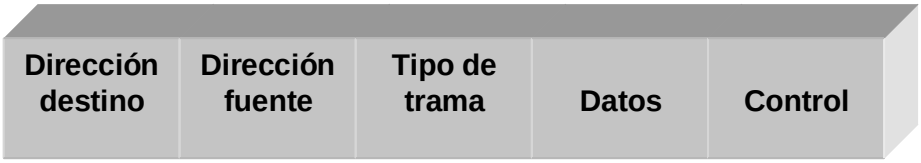


Fig. 2.11. Ejemplo de tramas de datos

Cuando el nivel de datos envía una trama siempre espera una respuesta (acknowledgment) de la computadora receptora. Si ésta encuentra problemas en alguna trama durante la transmisión, solamente se retransmiten las tramas que no fueron reconocidas.

Nivel de red (Network Layer)

Este nivel determina la ruta del mensaje desde la computadora emisora hasta la computadora, dependiendo de las condiciones de la red.

Dentro de las funciones de enrutamiento de mensajes evalúa el mejor camino que debe seguir el paquete dependiendo del tráfico en la red, el nivel de servicios, etc. Los problemas de tráfico que controla tienen que ver con el enrutamiento (routing), intercambio (Switching) y congestionamiento de paquetes en la red.

El nivel de red maneja pequeños paquetes de datos juntos para su transmisión a través de la red, así como la reestructuración de grandes tramas de datos. En paquetes pequeños. En la computadora receptora se reensamblan los paquetes en su estructura de datos original (trama).

A la información proveniente de nivel de transporte (Transport Layer) se le añaden componentes apropiados para su enrutamiento en la red y para mantener un cierto nivel en el control de errores. La información se presenta según el método de comunicaciones utilizado para acceder a la red de área local, la red de área extendida como los enlaces T1, la conmutación de paquetes (packet switching) como X.25, etc. Por ejemplo el protocolo IP (Internet Protocol) es uno de los protocolos que usa en este nivel de red.

Nivel de transporte (Transport Layer)

Este nivel es llamado ocasionalmente nivel de host–to–host o nivel end–to–end. En particular los niveles 4 a 7 son conocidos como niveles end–to–end y los niveles 1 a 3 son conocidos como niveles de protocolos.

El nivel de transporte provee un mecanismo de intercambio de información muy confiable entre las computadoras debido a que es el responsable del manejo de la detección y corrección de errores.

El nivel de transporte se relaciona en mayor medida con los beneficios de end-to-end, como son el manejo de las direcciones de la red, el establecimiento de circuitos virtuales y los procedimientos de entrada y salida de ésta. Solamente al alcanzar el nivel superior de transporte (sesión) se podrán observar los beneficios notorios para el usuario final.

Este nivel puede incluir las especificaciones de los mensajes de Broadcast (difusión), los tipos de datagramas, los servicios de correo electrónico las prioridades de los mensajes, la recolección de la información y su administración, la seguridad, los tiempos de respuesta, las estrategias de recuperación en casos de falla y la segmentación cuando el paquete excede su tamaño máximo según el protocolo.

Cuando recibe información del nivel de red, el nivel de transporte verifica que la información este en el orden adecuado y revisa si existe información duplicada o extraviada.

Si la información recibida esta en desorden lo cual es posible cuando se enlutan las tramas en redes grandes el nivel de transporte corrige el problema y transfiere la información a nivel de sesión, en donde se le dará un proceso adicional. Por ejemplo, el protocolo TCP (Transmisión Control Prorocol) usa este nivel del modelo OSI.

Nivel de Sesión (Session Layer)

Este nivel es el que permite que dos aplicaciones en diferentes computadoras establezcan, usen y finalicen la conexión llamada sesión. El nivel de sesión maneja en dialogo que se requiere la comunicación de dos dispositivos. Establece reglas para poder iniciar y finalizar la comunicación entre dispositivos y puede brindar el servicio de recuperación de errores; es decir, si la comunicación falla y esto es detectado el nivel de sesión retransmitir la información para completar el proceso en la comunicación.

Para poder entender este nivel se hará una comparación con el sistema telefónico. Cuando uno levanta el teléfono espera el tono y marca un número, en ese momento se esta creando una conexión

física que va desde el nivel 1 (físico) como un protocolo de persona a red. Al momento de hablar con la persona en el otro extremo del teléfono uno se encuentra en una sesión persona a persona en otras palabras la sesión es el dialogo de las dos personas que se transporta por el circuito del teléfono. En este nivel se ejecutan funciones de reconocimiento de nombres para el caso de seguridad relacionado con aplicaciones que requieren comunicarse a través de la red.

Nivel de Presentación (Presentation Layer)

En este nivel se traduce o se transfiere la información recibida en el formato de nivel de aplicación a un formato intermediario reconocido. En la computadora receptora la información se traduce o transfiere del formato intermediario al formato usado en su propio nivel de aplicación.

El nivel de presentación maneja beneficios como la administración de la seguridad en la red; por ejemplo, la codificación y decodificación, el encriptado, la comprensión y descomprensión, el cifrado y descifrado. También brinda las normas para la transferencia de información (data transfer) y comprime datos para reducir en número de bites que necesitan ser transmitidos.

Nivel de Aplicación (Application Layer)

Este nivel es el nivel más alto y sirve como una ventana para los procesos de la misma índole al acceder a los servicios de la red.

Entre estas aplicaciones se encuentra el Software para transferencia de archivos (file Transfer), accesos a bases de datos y correo electrónico.

2.4.2. El modelo TCP/IP

Nace en el año 1974 cuando la red ARPAnet se fusiona con otras redes creando la denominada Internet. ARPAnetnace de la agencia ARPA (Advanced Research Proyects Agency), perteneciente al Departamento de Defensa de los Estados Unidos. Esta arquitectura recibe en nombre de sus dos protocolos más importantes: TCP(Transmisión Control Potrocol)el IP (Internet Protocol).

La creación de esta arquitectura fue a la inversa de modelo OSI. En este caso se definieron y se desarrollaron los protocolos, y seguidamente se creó el modelo adaptado a estos protocolos.

Este modelo se compone únicamente de cuatro capas que son las siguientes:

- **La capa host-red.** Es la equivalente a las capas físicas y de enlace en el modelo OSI. Se encarga de conectar el host a la red por medio de un protocolo que permita enviar paquetes IP.

- **La capa Internet.** Es la equivalente a la capa de red en el modelo OSI. Su función es la del encaminamiento de los paquetes que recibe y evitar que se congestionen los nodos intermedios de la red. Esta capa de servicios de conmutación de paquetes no orientados a conexión, por lo que ,los paquetes pueden llegar desordenados a su destino y las capas correspondientes del terminal receptor serán las encargadas de reorganizar los paquetes recibidos. El protocolo de esta capa es el conocido protocolo IP.

- **La capa de transporte.** Realiza la misma función que la capa del mismo nombre del modelo OSI. Permite la conexión terminal a terminal en una red. En esta capa se establece dos protocolos: El TCP (Transmisión Control Protocol) y e UDP (User Datagram Protocol).

    - El primero ofrece un servicio orientado a la conexión fiable y se ocupa del control de flujo en la transmisión para evitar congestiones en distintos nodos. Protocolos de aplicación que utiliza el TCP pueden ser el SMTP, utilizado para el correo electrónico o el FTP un protocolo de transferencia de ficheros entre terminales, muy utilizado en Internet.

    - El segundo, el UDP ofrece un servicio no orientado a la conexión que no es fiable. Tampoco realiza control de flujo ni

de errores, pero es mucho más rápido, como cosa imprescindible en algunos servicios y aplicaciones, como puede ser la transmisión de voz en tiempo real, en el que el retardado sería más problemático que el error en la transmisión de algún paquete.

- **La capa de aplicación.** Esta capa equivale a las de sesión, aplicación y presentación del OSI. Esta concentración de funciones respecto al anterior modelo tiene su explicación práctica, ya que las capas de sesión y aplicación tienen relativamente poca entidad para estar definidas independientemente. En esta capa están implementados todos los protocolos de alto nivel usados en los servicios al usuario.

  Ejemplos de protocolos existentes en esta capa pueden ser los DNS, SNMP, TNP, HTTP.

2.5. Protocolos, interfaces, servicios y tipos de servicios

2.5.1. Protocolos de comunicación

Es un conjunto de reglas que indican como se debe llevar a cabo un intercambio de datos o información. Para que dos o más nodos de una red puedan intercambiar información es necesario que manejen el mismo conjunto de reglas, es decir, un mismo protocolo de comunicaciones.

2.5.2. Interfaz

Corresponde a la separación o división entre dos capas de un modelo de comunicación, y es la encargada de definir las operaciones básicas y los servicios que el nivel inferior ofrece a la capa superior del modelo.

2.5.3. Entidades

Son los elementos activos en cada nivel del modelo. Una entidad puede ser un software (un proceso) o un hardware (un chip).

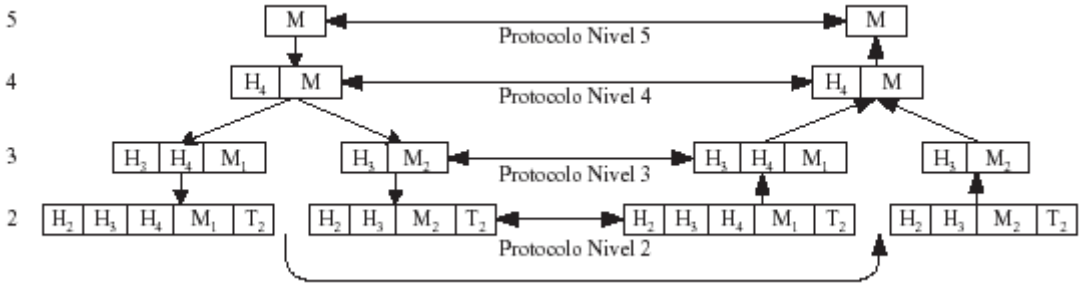


Fig. 2.12. Flujo de información en una comunicación

2.5.4. Servicios

Son un conjunto de operaciones que un nivel provee al nivel superior. En otras palabras, define que operaciones puede ejecutar la capa, pero no especificar como son implementadas estas operaciones.

Cada capa tiene un conjunto de operaciones que realizar y un conjunto de servicios que usa de otra capa. De esta manera, se identifica como usuario de servicio a la capa que solicita un servicio y como proveedor a quien le da. Cuando una entidad se comunica con otra ubicada en la misma capa pero en diferentes nodos se dice que se establece comunicación entre entidades pares.

Cada capa tiene un conjunto de servicios que ofrecer, el punto exacto donde se puede pedir el servicio se llama punto de acceso al servicio o SAP. En cada capa, la entidad activa recibe un bloque de datos consistente de un encabezado que tiene significado para el protocolo de esa capa y un cuerpo que contiene datos para ser procesados por esa entidad o que van dirigidos a otra capa.

Las capas ofrecen servicios de dos tipos: orientados a la conexión y no orientados a la conexión. Además, cada uno de estos servicios puede ser caracterizado por la cierta calidad de servicio que ofrecen. Así, se pueden tener servicios confiables y no confiables.

- **Servicios orientados a la conexión.** Es un tipo de servicio en el que obligatoriamente debe establecerse una conexión o camino, entre el origen y el destino antes de que cualquier dato pueda transmitirse. Los servicios orientados a conexión se caracterizan porque cumplen tres etapas en su tiempo de vida: negociación del establecimiento de la conexión (etapa 1), sesión

de intercambio de datos (etapa 2) y negociación del fin de la conexión (etapa 3). Los servicios orientados a la conexión pueden ser considerados como “alambrados”, es decir, que existe una conexión alambrada entre los dos interlocutores durante el tiempo de vida de la conexión.

- **Servicios no orientados a conexión.** Los servicios no orientados a conexión carecen de las tres etapas antes descritas y en este caso, los interlocutores envían todos paquetes de datos que componen una parte del diálogo, por separado, pudiendo éstos llegar a su destino en desorden y por diferentes rutas. Es responsabilidad del destinatario ensamblar los paquetes, pedir retransmisiones de paquetes que se dañaron y darle coherencia al flujo recibido.

- **Servicio confiable.** Un servicio es confiable si ofrece una transmisión de datos libre de errores. Para cumplir este requisito, el protocolo debe incluir mecanismos para detectar y/o corregir errores. La corrección de errores puede hacerse con información que está incluida en un paquete dañado o pidiendo su retransmisión al interlocutor. También es común que incluya mecanismos para enviar acuses de recibo cuando los paquetes llegan correctamente.

- **Servicio no confiable.** Un servicio es no confiable si el protocolo no asegura que la transmisión está libre de errores y es responsabilidad del protocolo de una capa superior (o de la aplicación) la detección y corrección de errores si esto es pertinente o estadísticamente justificable.

  A un servicio que es a la vez no orientado a la conexión y no confiable se le conoce como *servicio de datagramas*. Un servicio que es no orientado a la conexión pero que incluye acuse de recibo se conoce como *servicio de datagramas con acuse de recibo*. Un tercer tipo de servicio se le llama con *solicitud de respuesta* si consiste de un servicio no orientado a conexión y por cada envío de datos se espera una respuesta inmediata antes de enviar el siguiente bloque de datos.

2.6. El medio físico

2.6.1. Cable coaxial

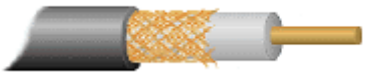


Fig. 2.13. Cable coaxial

El cable coaxial para banda base y el cable coaxial para banda ancha son muy parecido en su construcción, pero sus principales diferencias son: la cubierta del cable, los diámetros y la impedancia.

El cable coaxial para banda base es de 3/8 de pulgada y utiliza una cubierta de plástico, mientras que el cable coaxial para banda ancha es de 1/2 pulgada y está cubierta de una malla o tela de aluminio y una funda protectora de plástico.

Ethernet por ejemplo, puede trabajar con ambos cables, pero lo más común es con banda base.

Tabla 2.1. Tabla comparativa entre banda base (baseband) y banda ancha (broadband)

	Banda base	**Banda ancha**
Tipo de cable	**RG–58 A/U**	**RG–59 o RG–6**
Velocidad máxima de transferencia	10 Mbps	6 Mhz
Impedancia	50 Ω	75 Ω
Distancia máxima de segmento	185 – 500 m	3600 m
Costo	Bajo	Alto
Inducción de ruido	Baja	Alta

- **Thick Ethernet (Ethernet Gruesa)**

  Es un tipo especial de cable coaxial rodeado por un aislante dieléctrico.

Las reglas para la instalación y configuración de segmentos de cable son:

- La longitud máxima de segmento de red es de 500 metros.
- Cada segmento de red debe tener una terminación de 50 ohms en cada extremo.
- No pueden conectarse en serie más de cinco segmentos de red y solo tres de éstos pueden estar ocupados.
- La cantidad máxima de transceptores por segmento es de 100.
- La cantidad máxima de nodos en una red es de 1.024.
- Los transceptores no pueden instalarse a menos de 2.5 mts.
- Los cables de bajada no pueden ser más largos de 50 mts.
- La distancia máxima entre dos estaciones es de 3.000 mts.

- **Thin Ethernet (Ethernet delgado)**

  Un tipo de cable coaxial RG58 cosiste en un conductor interno rodeado por un aislante dieléctrico.

  Reglas para la instalación:

  - La longitud máxima de segmento debe ser de 185 metros.
  - Cada segmento de red debe tener una terminación de 50 ohms en cada extremo.
  - No pueden conectarse en serie más de cinco segmentos de red y solo tres de éstos pueden estar ocupados.

- La distancia mínima de cable entre adaptadores de red es 0.5 metros.
- La cantidad máxima de nodos en una red es de 1.024.
- La distancia máxima entre dos nodos es 1.425 metros.

Se usan conectores de tipo BNC.

2.6.2. Par trenzado

Este es el medio de transmisión más común de todos. Es un medio guiado y consiste en un par de cables de cobre aislados, de aproximadamente 1 mm de espesor cada uno, que se disponen en forma de espiral para evitar la diafonía con otros cables en su proximidad. Esto es así ya que si fueran en paralelo constituirían una antena, mientras que trenzados no.

Este tipo de medio de transmisión es muy utilizado en la telefonía, sobretodo para bucles de abonado; es relativamente barato y no requiere de amplificación de señal hasta distancias superiores a 2 km.

Sirve para transmitir señales tanto analógicas como digitales, y si la sección es suficiente, permite anchos de banda superiores a varios megabits/s.

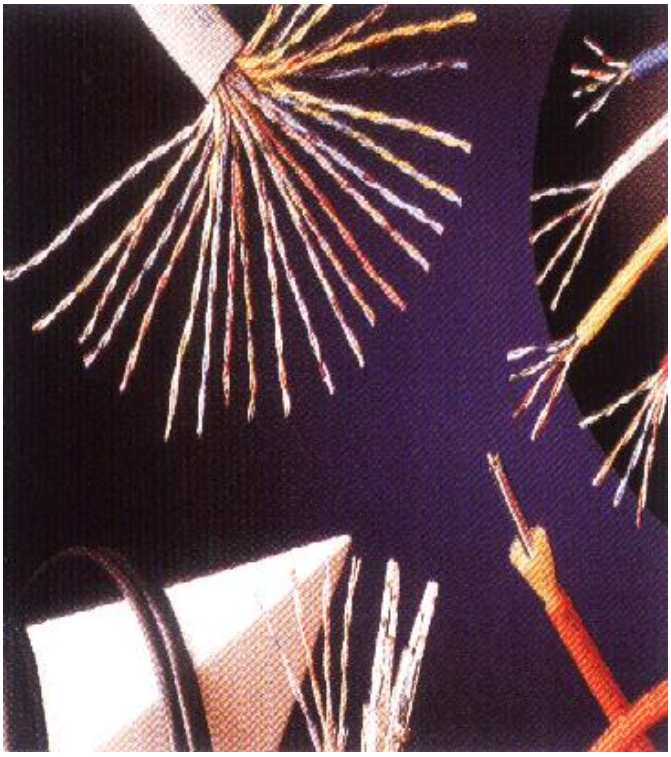


Fig. 2.14. Cable de par trenzado

La principal limitación de este tipo de medio es que si se necesitan altas velocidades de transmisión, y por lo tanto la frecuencia de la señal transmitida, la resistencia de los conductores aumenta para estas señales de alta frecuencia, por lo que también lo hace la atenuación de dichas señales, perdiéndose la potencia de la señal por efecto de radiación. Los dos tipos más importantes son los siguientes:

- Cable UTP (Unshielded Twisted Pair). Es un cable de pares trenzados sin ningún tipo de protección externa, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de

los pares, ya que de lo contrario la transmisión no sería efectiva. Es un cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios.

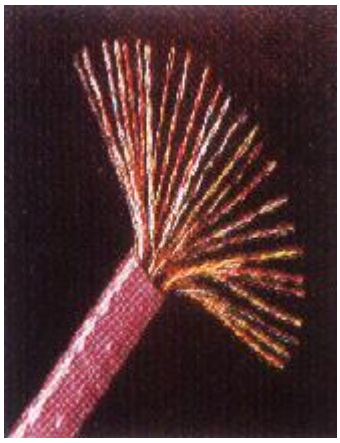


Fig. 2.15. Cable UTP

- Cable STP (Shielded Twisted Pair). Este cable es semejante al UTP, pero se le añade un recubrimiento metálico para evitar las interferencias externas. Por tanto, es un cable más protegido, pero menos flexible que el primero. El sistema de trenzado es idéntico al del cable UTP. La resistencia de un cable STP es de 150 ohmios.

Estos cables de pares tienen aplicación en muchos campos. El cable de cuatro pares está siendo utilizado como la forma de cableado general en muchas empresas, como conductores para la transmisión telefónica de voz, transporte de datos, etc.

Fig. 2.16. Cable STP

En los cables de pares hay que distinguir dos clasificaciones:

- La categoría: cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.
- Las clases: cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características.

Tabla 2.2. Características de longitudes y anchos de banda para las clases y categorías de pares trenzados

Clases	Clase A	Clase B	Clase C	Clase D
Ancho de banda	100 Khz	1 Mhz	20 Mhz	100 Mhz
En categoría 3	2 km	500 m	100 m	no existe
En categoría 4	3 km	600 m	150 m	no existe
En categoría 5	3 km	700 m	160 m	100 m

2.6.3. Fibra óptica

Es también un medio guiado. La composición de un cable de fibra óptica es la siguiente: consta de un núcleo consistente en una o más fibras hechas de cristal o plástico (preferiblemente silicio, aunque es más caro) entre 1 y 10 µm de diámetro, un revestimiento de propiedades físicas distintas al núcleo, de unos 125 µm y una cubierta externa protectora. El núcleo es el conductor de la señal luminosa y la atenuación de señal es despreciable. La señal es conducida por el interior de este núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterior como la interferencia de nuevas señales externas.

Actualmente se utilizan dos tipos distintos de fibra óptiça para la transmisión de datos:

Fibra monomodo.- Cuando el diámetro del núcleo de la fibra es similar a la longitud de onda de la señal transmitida, de tal manera que un solo rayo puede viajar a través de ella. Proporciona un gran ancho de banda, pero está sujeto a una mayor atenuación. Permite la transmisión de señales con ancho de banda hasta 2 GHz. Se suele utilizar para conectar enlaces de larga distancia o que necesiten una gran velocidad de flujo.

Fibra multimodo.- Cuando el diámetro del núcleo de la fibra (entre 50 y 60 µm) es bastante superior que la longitud de onda del rayo

transmitido, la cual se refracta en su camino, llegando a su destino con diferentes fases. Se emplean como enlaces entre centrales telefónicas urbanas que no requieran excesiva capacidad del medio, ni utilización de repetidores.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda (se ha llegado a alcanzar un sistema de 2,5 Gbit/s por cada fibra, lo que supone unos 30.720 circuitos telefónicos).

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas. La luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente para ser utilizada en la transmisión de datos. Son necesarias fuentes especializadas:

a) **Fuentes láser.**- A partir de la década de los sesenta se descubre el láser, una fuente luminosa de alta coherencia, es decir, que produce luz de una única frecuencia y toda la emisión se produce en fase.

b) **Diodos láser.**- Es una fuente semiconductora de emisión de láser de bajo precio.

c) **Diodos LED.-** Son semiconductores que producen luz cuando son excitados eléctricamente.

Otra ventaja es su gran fiabilidad, la tasa de errores es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales. Normalmente se encuentra instalada en grupos, en forma de mangueras (hasta aproximadamente 128 elementos), con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas.

Su principal inconveniente es la dificultad de realizar una buena conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como por su fragilidad y su mayor costo respecto de otros tipos de medios de transmisión.

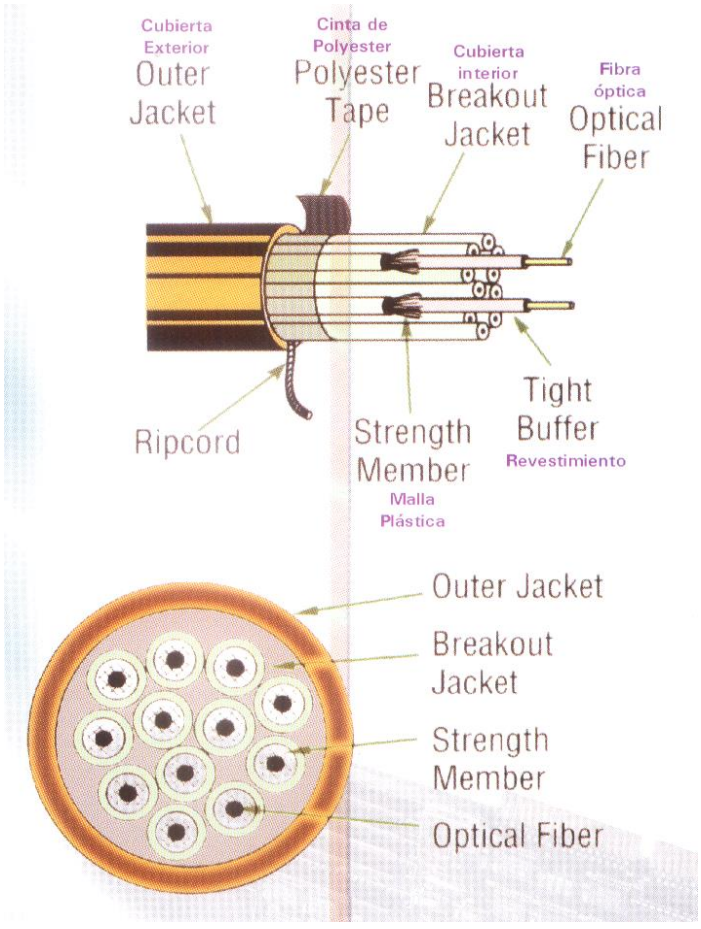


Fig. 2.17. Componentes de la fibra óptica

2.6.4. Enlaces de radio

Las ondas de radio tienen como principales características que son fáciles generar, pueden viajar distancias largas, y penetran edificios fácilmente. Además, son onmidireccionales, lo que significa que ellas viajan en todas las direcciones desde la fuente, para que el transmisor y receptor no tengan que estar físicamente alineados con cuidado.

Las propiedades de ondas son dependientes de la frecuencia. A frecuencias bajas, atraviesan bien obstáculos, pero el poder baja grandemente cuando se aleja de la fuente. A frecuencias altas, las ondas tienden a viajar en líneas rectas y rebotar cuando consiguen obstáculos.

Ellas también son absorbidas por la lluvia. A cualquier frecuencia, las ondas están sujetas a interferencia de los motores y otros equipos eléctricos. El problema principal que se presenta al usar estas bandas para comunicación de datos es el ancho de banda relativamente bajo que ellas ofrecen.

Debido a la habilidad de radio de viajar grandes distancias,, la interferencia entre los usuarios es un problema. Por esta razón, todos los gobiernos licencian al usuario de transmisores de radio.

2.6.5. Enlaces de microondas

Por encima de los 100 MHz, las ondas viajan en líneas rectas y pueden por consiguiente enfocarse estrechamente. Concentrando toda la energía en una haz pequeño usando una antena parabólica se obtiene una razón señal a ruido bastante alta, permitiendo la comunicación, pero las antenas transmisoras y receptoras deben alinearse con precisión entre sí. Además, esta direccionalidad permite que múltiples transmisores sean alineados seguidamente para comunicarse con múltiples receptores seguidos sin interferencia.

Puesto que las microondas viajan en una línea recta, si las torres están demasiado separadas, la Tierra estará en el camino (recordar la curvatura del planeta). Por consiguiente, se necesitan repetidoras periódicamente. Mientras más altas sean las torres, más distantes pueden estar. Las distancias entre las repetidoras suben muy bruscamente con la raíz cuadrada de la altura de la torre. Para torres; con altura de 100 metros, las repetidoras pueden estar separadas entre sí unos 80 kms. Este hecho las hace ser relativamente baratas.

A diferencia de las ondas a bajas frecuencias, las microondas no atraviesan bien edificios.

Más aunque el haz pueda enfocarse bien al transmisor, hay todavía alguna divergencia en el espacio. Algunas ondas pueden refractarse por capas atmosféricas bajas y pueden tomar ligeramente mas tiempo en llenar que las ondas directas. Las ondas retrasadas pueden llegar fuera de fase con la onda directa y por lo tanto cancelar la señal.

La comunicación por microondas se usa ampliamente para la comunicación del teléfono a larga distancia, teléfonos celulares y distribución de la televisión.

2.6.6. Enlaces satelitales

Un satélite de comunicación puede ser pensado como un repetidor de microondas en el cielo. Contiene diversos transponders, cada uno de los cuales escucha alguna porción del espectro, amplifica la señal entrante, y hace una difusión de vuelta en otra frecuencia para evitar interferencia con la señal que entra. Los rayos que bajan son anchos o angostos, pudiendo cubrir grandes o pequeñas superficies de la tierra, respectivamente.

Los enlaces satelitales se diferencian de los enlaces punto a punto terrestres en que los retardos producto de las distancias involucradas son considerables, típicamente 270 mseg. Esto es bastante en comparación con los 3 μseg/km de los enlaces de

microondas y los 5 μseg/km del coaxial o la fibra. Otra diferencia es que los satélites son por naturaleza elementos de difusión, lo que es útil en algunos casos, pero en otros, como la seguridad, no lo es. Otras características son que el costo de una transmisión es independiente de la distancia y que tienen una tasa de error bajísima.

2.7. Características de la red

Las características más representativas de una red son:

- **Alcance.** El área de conexión puede cubrir grandes extensiones geográficas, dependiendo de la tecnología que se utilice.
- **Velocidad de Transmisión.** Hoy en día debido al avance de la tecnología, la velocidad de transmisión es significativamente grande, ya que las comunicaciones se realizan en línea y en tiempo real.
- **Conectividad.** Existen muchos dispositivos que actualmente se encuentran en el mercado que se pueden conectar entre sí sin importar el fabricante.
- **Fiabilidad.** Todas las redes presentan una baja tasa de error en las transmisiones de datos.
- **Compartición de recursos.** Permiten la integración en la misma red de una gran diversidad de dispositivos. Os recursos de almacenamiento, las impresoras y los elementos de comunicación pueden ser utilizados por todas las estaciones de trabajo.

CAPÍTULO III

INTRANETS

3.1. Definición

Una Intranet es un ambiente de computación heterogéneo que conecta diferentes plataformas de hardware, ambientes de sistema operativo e interfaces de usuario con el fin de permitir comunicación ininterrumpida, colaboración, transacciones e innovación.

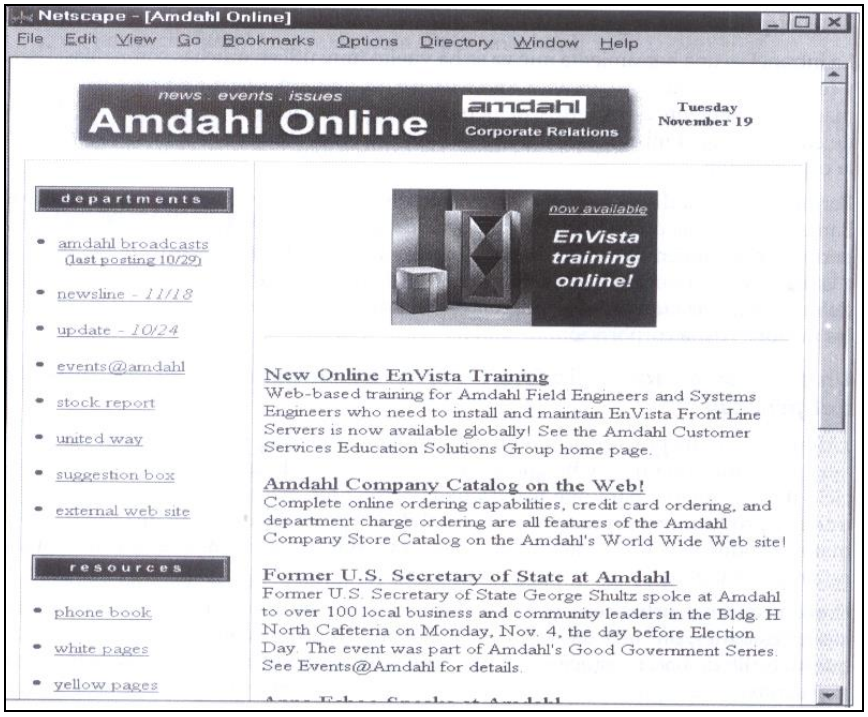


Fig. 3.1. Sitio Central de la intranet de Amdahl

3.2. InternetWorking

En el mundo real existen innumerables redes que no se corresponden con ninguno de los tipos definidos anteriormente. Por ejemplo, una LAN (que

normalmente será una red de tipo broadcast) es muy posible que disponga de un router que la interconecta a una WAN (que generalmente consistirá) en un conjunto de enlaces punto a punto). Esta interconexión de diferentes tipos de redes se conoce como «Internetworking». El router que interconecta redes diferentes tiene que estar físicamente conectado a todas las redes que se desee interconectar.

Cuando una red está formada por la interconexión de varias redes, se le denomina intranet.

La tabla 3.1. muestra los medios de transmisión más importantes, a qué tipos de redes pueden pertenecer y velocidades medias de transmisión.

Tabla 3.1. Resumen de medios de transmisión

MEDIO DE TRANSMISIÓN	TIPO DE RED	VELOCIDAD DE TRANSMISIÓN
Ethernet	LAN	10 a 100 Mbps
Token Ring	LAN	4 a 16 Mbps
Token Bus	LAN	10 Mbps
Appletalk	LAN	10 Mbps
FDDI	LAN/MAN	100 Mbps
X.25	WAN	
Frame Relay	WAN	
VSAT	WAN	
RDSI	WAN	
RTC	WAN	
ATM	WAN	
Punto a Punto	WAN	

3.3. Arquitectura de la Intranet

3.3.1. Estándares Abiertos

Hablar de la arquitectura de una intranet significa hablar de estándares abiertos, que a su vez significa que el software que utiliza para transformar sus datos en información útil para la compañía puede ejecutarse en cualquier software. También significa que cualquier persona puede desarrollar software rápidamente sin tener que asegurarse de que sea compatible con cada sistema operativo de la red. Los días del software y el hardware propietario y de los diferentes sistemas operativos, has terminado con la arquitectura de la red. ¿O no? La interoperatividad depende de la existencia de estándares y de las extensiones que surjan para los protocolos propietarios. Esto significa apertura como las de Windows, Novell, Java y cualquier extensión HTML que se incorpore. Por eso deben existir definiciones de estándares que sean verdaderamente sólidos. Estamos cerca de llegar a tener sistemas abiertos. Lo suficientemente cerca para crear intranets. La figura 3.2. se delinea un esquema claro de los estándares abiertos . Cualquier cliente (PC o estación de trabajo) utiliza TCP/IP (estándares de Internet) para comunicarse con cualquier servidor. No se puede ser más simple.

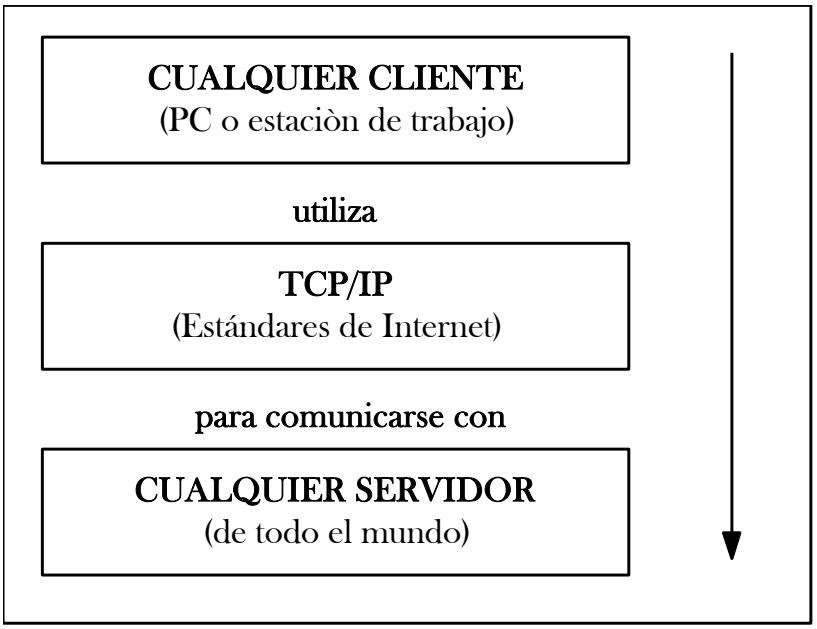


Fig. 3.2. Arquitectura clásica de navegador/servidor Web

3.3.2. Estándares en una Intranet

En realidad no necesita dedicar mucho tiempo a pensar en los estándares de una intranet, porque están basados en los protocolos establecidos por Internet y necesita comprenderlos para construir su marco de trabajo para la intranet. Los estándares de la intranet están conformados por protocolos de Internet, lenguajes de programación y APIs (Interfaces para Programación de Aplicaciones).

En la tabla 3.2. se resumen los estándares clave de Internet que facilitan el flujo de información. Los incluimos aquí porque necesitará tener un poco de información sobre estándares de Internet para ayudarle a colocar sus soluciones para la intranet en el lugar adecuado.

Tabla 3.2. Estándares de Internet

Estándar de Internet	¿Qué hace?	¿Cómo lo hace?
TCP/IP	Actúa como una oficina postal entre redes globales.	Da a cada PC o estación de trabajo su propia dirección, de modo que los paquetes puedan enviarse al lugar correcto.
HTTP	Permite acceso con navegador a las redes globales	Envía y da seguimiento a los paquetes de información entre clientes y servidores. Es como un Federal Express.
HTML (para texto); CSS y DSSL (para hojas de estilo)	Sistema de publicación para documentos, gráficos, videos, audio, etc.	Hace que los archivos tengan los mismos códigos tras bambalinas, de modo que cualquier plataforma con un navegador pueda ver la página Web.
FTP, WebNFS	Mueve cualquier elemento digital (archivos, audio, software) por la red.	Convierte todos los datos imaginables en unos y ceros y asegura su integridad al distribuirse por las líneas telefónicas
SMTP/IMAP4/POP	*Correo electrónico internacional*	Transporta correos electrónicos en la red
Dirección IP	Le proporciona un número único en Internet	Crea un número como 205.124.234.1 que lo representa sólo a usted
SNMP	Superadministración.	SNMP toma varios trabajos específicosde dispositivos como impresoras, routers y puentes; por lo tanto, proporciona un mecanismo estándar de control y monitoreo de red.
NNTP	Proporciona noticias a solicitud en la computadora de escritorio	Delinea datos de noticias para que pueda seguir lo que otros ven en las noticias.
DNS/NIS+	*Proporciona nombres para su sitio Web. Como yahoo.com*	Asigna un nombre como www.hot.company.com a una dirección IP como 205.124.234.1

Tabla 3.1. Estándares de Internet (continuación)

Estándar de Internet	¿Qué hace?	¿Cómo lo hace?
LDAP (Protocolo de acceso a directorio largo)	LDAP proporciona una manera estándar para que clientes, aplicaciones y servidores de Internet tengan acceso a servicios de directorio.	LDAP basa su modelo de directorio en entradas. Las entradas son comunes en todos los directorios, de modo que es más fácil hacer referencia a una entrada sin ambigüedades.
MIME	Permite enviar multimedia por correo electrónico	Utiliza un esquema de traducción cuando el archivo se transfiere o se lanza a una aplicación externa para su observación.

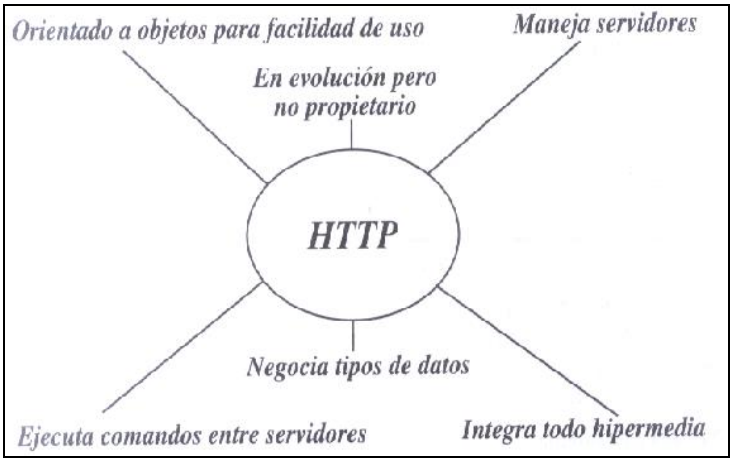


Fig. 3.3. Un panorama de la funcionalidad de HTTP

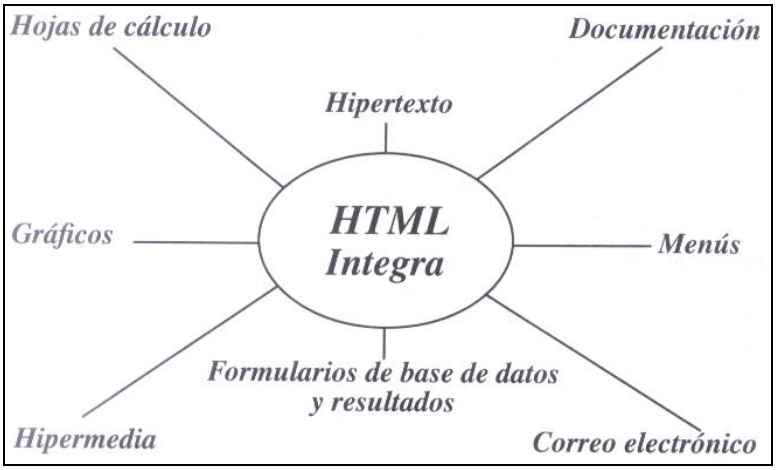


Fig. 3.4. HTML, permite la integración de multimedia

3.4. Infraestructura de la Intranet

La intranet está integrada por una inmensa infraestructura, actualmente de sentido común. Por infraestructura, nos referimos a procesos, personas y políticas. Para comprender políticamente la intranet, debe entender los procesos; al hacerlo, conocerá las habilidades y las personas que se requieren para hacer el trabajo. Una vez que tenga los procesos y la gente en su lugar, deben establecer políticas que definan las posiciones oficiales y legales sobre el uso de intranet.

3.4.1. Procesos

La comprensión de los procesos que debe recorrer para construir una intranet, le beneficiará enormemente al configurar el resto de la infraestructura. En este trabajo la infraestructura está integrada por procesos, personas y procedimientos. Aquí analizaremos los siguientes:

- Proceso de convencimiento de ejecutivos: Una vez que los ejecutivos observan cómo se utiliza la tecnología para su propia superación, entienden un claro análisis beneficio–costo y ven un impacto directo en la percepción y la lealtad del cliente, entonces la intranet se encuentra rumbo a la etapa de planeación.
- Proceso de planeación: La información en la punta de sus dedos es una herramienta importante. Conocer la forma de obtenerla es algo que impulsa una carrera.

- Proceso de diseño: Si se toma el cuidado suficiente para crear un sito de intranet para la organización, debe recordar que el propósito de éste es compartir comunicación e información entre divisiones y departamentos internos. La clave para su sitio es la calidad de comunicación de información entre todos y la manera de manejar la apertura de la información con los demás. Es imperativo comunicar los valores.
- Proceso legal: La parte legal de la organización necesita incluirse desde el principio del proceso de diseño. Por ejemplo, puede poner la información de recursos humanos , de derechos de autor, de contratos y cláusulas especiales para que los empleados tengan acceso a ellas, también puede poner el reglamento interno de la empresa.
- Proceso de biblioteca: Es necesario establecer en línea índices y catálogos para un rápido desarrollo. La biblioteca de elementos comunes, imágenes, fuentes, audio, video, logos, etc., necesitan configuración y mantenimiento. Cualquier script que sea posible volver a utilizar, o cualquier plantilla para diseño de sitios debe estar disponible y debe permitirse su personalización.
- Proceso de desarrollo: Una vez que haya logrado convencer a los ejecutivos, diseñado un elegante plan de intranet, superado el diseño, los procesos legales y de biblioteca, est{a listo para un rápido desarrollo. Si manejó inteligentemente estos procesos utilizando una intranet como un ambiente de administración, seguimiento y supervisión tendrá ya un cúmulo de información

en línea. Si utilizó un sitio Web centralizado para comunicar los procesos a todos los miembros participantes de la intranet, habrá iniciado bien el proceso de desarrollo.

- Proceso de mantenimiento: Los servidores Web necesitan mantenimiento. A medida que surgen problemas o defectos en el software, alguien tiene que responder con rapidez.
- Proceso de análisis de sitio: Es posible mantener fácilmente las estadísticas de procesos en este ambiente. Las estadísticas proporcionan un análisis de la actividad del sitio. Es posible desarrollar estrategas para influir en el comportamiento del sitio.

3.4.2. Gentes

Una vez que se han definido claramente ciertas tareas o procesos, puede empezar a ver cuáles aptitudes y habilidades son necesarias para crear una intranet. En principio, no necesita buscar nuevas habilidades y aptitudes. Lo mejor es elevar el conocimiento actual de los empleados y proporcionar las herramientas de intranet requeridas para permitir a los usuarios publicar y vincularse en línea.

Los empleados necesitar usar intranets para desarrollar tareas existentes, concentrándose primero en el acceso y uso de los datos disponibles. Después, necesitarán la posibilidad de actualizarlos y publicarlos fácilmente. Cada vez se volverá más importante aprender a convertir documentos existentes y publicar páginas Web robustas en la intranet. Los empleados pueden aprender a

desarrollar algunas de las tareas de desarrollo más complejas, o a manejar vendedores que desarrollen las partes técnicas.

3.4.3. Políticas

También debe establecer algunas políticas. Son tratados y verdaderas lecciones de negocios para proteger su organización sobre todo en el aspecto legal. Estos temas han sido confundidos por muchas corporaciones. La distinción se encuentra en la cantidad de empresarios que desean confiar el flujo de la información en sus empleados. El movimiento de la información y la libertad de expresión no es necesariamente una práctica común en todas las culturas del mundo.

3.5. Características, Beneficios y Limitaciones

3.5.1. Características

- Permite la publicación en base a la demanda
- Permite la reducción de costos, se considera como un nuevo paradigma de la información.
- Permite el desarrollo de aplicaciones Cliente–Servidor. Se puede realizar un rápido diseño.
- Es de fácil navegación
- Accesible para la mayoría de plataformas de cómputo
- Integra la estrategia de cómputo distribuido
- Adaptable a los sistemas de información existentes
- Uso de multimedia

3.5.2. Beneficios

Entre los beneficios fundamentales se incluye la disminución de los costos de red, la facilidad de aprendizaje, el desarrollo propio orientado a metas y estándares abiertos que permiten que el software se ejecute sin depender de un sistema operativo. Comunicar los objetivos y dar seguimiento a la misión de la empresa o las metas de cada departamento hace que la intranet resulte una gran opción.

El acceso a almacenes de datos hace que la intranet valga su peso en oro. Otros beneficios claves son los modelos de negocios mejorados, el mejoramiento de la organización, comunicación mejorada, el ambiente de grupo de trabajo colaborativo, con principios de mejoramiento continuo de los procesos sustentados por la infraestructura de la intranet.

En resumen:

- Requiere poca inversión para su inicio
- Ahorra tiempo y costos en comparación de la distribución de información tradicional (oficios, papel, solicitudes).
- Su estrategia de cómputo distribuido utiliza los recursos de cómputo más efectivamente.
- Tiene una interfaz sencilla y flexible (vínculos) y es independiente de la plataforma.

3.5.3. Limitaciones

Las limitaciones son importantes en una estrategia de desarrollo de una intranet. Estas limitaciones tal vez tengan soluciones inmediatas en su organización; sin embargo, si las identifica de antemano, puede ahorrar mucho tiempo de desarrollo. De modo que, al planear, debe hacer una valoración cuidadosa.

Rand Lindsley, ingeniero Señor de Sun Microsystems, dice:
"Antes de que pueda dirigirse a los temas de mejoramiento de los procesos del negocio, tiene que considerar los grandes problemas. Lo que es más importante, debe revisar detenidamente la arquitectura y la infraestructura. ¿Cómo va a configurar los sistemas de todos (de modo que tengan posibilidades de utilizar TCP/IP y un navegador cliente)? ¿Qué tipo de máquina de búsqueda va a incorporar? ¿Y cuáles son los procesos y las políticas para llevar sus mensajes al sitio de la intranet?

Esto no debe resultar desalentador. En cambio, debe llevar a planes de acción.

Otra limitación es la determinación de la confiabilidad y la actualidad del contenido. Cuesta trabajo decidir quienes son los expertos en esta área, a menos de que sean bien reconocidos. Las corporaciones determinan quienes son los expertos en Internet.

3.6. Intranets desde la perspectiva tecnológica

La definición más simple y difundida de intranets, es la que las caracteriza como la forma de utilizar las tecnologías de internet en la organización interna de las empresas. Esto es totalmente cierto y, técnicamente hablando, exacto. Pero, ¿con esta definición somos conscientes del alcance de las intranets en el futuro de la informática y, por lo tanto, en la actividad del desarrollador de software?. En realidad creo que no, pues cautivados por la maravilla de la respuesta simple, esta definición tiende a que limitemos nuestra visión sobre las intranets a su vínculo tecnológico con Internet. Es posible que por este motivo las intranets sean apreciadas en una especie de oposición con internet. También es posible que gracias a esta apreciación sobre las intranets, que eficientemente difundió el sensacionalismo informático, también se deban parte de los temores, rechazos y, por lo tanto, la cautela que aún existe para la implementación de este tipo de soluciones. Tampoco es descartable que una parte de los desarrolladores, sobre todo gracias a la "juventud" de esta tecnología y el relativo poco dominio que existe sobre la misma, también contribuyen a la relativa lentitud de su difusión en el resto del mundo.

Literalmente hablando, internet/intranet "mueve el piso" técnico/tecnológico de los desarrolladores, pues no sólo "todo" es nuevo en este entorno, sino tan notoriamente diferente a las técnicas "tradicionales" de programación, que incluso varía la filosofía de programación. En esta situación, los programadores que en los últimos dos años no se fueron poniendo a tono con los nuevos paradigmas de

programación (Windows, OOP, cliente/servidor, programación gráfica, programación internet, etc.), chocan repentinamente contra la cruda realidad de que las soluciones intranets reducen o eliminan su competitividad, gracias a lo cual sus posibilidades de trabajo disminuyen o simplemente no existen y, por ello, los ingresos mensuales comienzan a mermar drásticamente. Ante esta situación algunos, reaccionan de la forma histórica más natural: rechazando a priori las posibilidades y validez de la nueva tecnología para su entorno de trabajo o tipo de clientes. Esta actitud contiene una alta dosis de intrepidez pues con ella, más que conservar los clientes, se están autoexcluyéndo del torrente de trabajo que traerá consigo la aplicación masiva de uno de los aportes tecnológicos más relevante de la informática para la comunicación interna de las empresas: las intranets.

3.6.1. Las tecnologías Internet/Intranet

Como si todo ello fuera poco, pensar en intranets (con las herramientas antes destacadas u otras) es pensar en sistemas en línea (que pueden incluir las más diversas formas: aplicaciones comerciales, información para consultas, correo, foros de debate, etc.) que utilicen todas las posibilidades de la tecnología internet, es decir:

- Accesos remotos
- ActiveX (controles ActiveX, ActiveX Scripting, ActiveX Server Framework, ActiveMovie, ActiveMusic, ActiveConferencing)

- Applets
- Arquitectura cliente/servidor flexible
- Audio
- Bases de datos
- Búsquedas
- Conferencias y foros
- Correo electrónico
- Consultas
- Edición de páginas HTML
- Navegadores
- OLE
- Protocolos de comunicación
- Publicación de páginas HTML
- Seguridad
- Software distribuido
- Telefonía
- Vídeo

Estas tecnologías, en la práctica, se traduce en aplicaciones informáticas caracterizadas por:

- Bajos costes de entrenamiento para el uso de las aplicaciones
- Capacidad de comunicación interactiva en línea (foros de debates, etc.)
- Correo electrónico, incorporado incluso a las aplicaciones

- Correr en línea aplicaciones comerciales, en tiempo real
- Desarrollo único para clientes internos y externos
- Envío y recepción de archivos
- Estandarización de la interface de trabajo de las redes locales
- Extensibilidad, conectividad y versatilidad
- Hiperenlaces con documentos locales o remotos
- Integración transparente de las redes locales
- Interface Gráfica de Usuario (GUI) fácil e intuitiva
- Integración de diferentes sistemas operativos en los clientes (Windows NT, OS/2, Windows 95)
- Multimedia
- Plataforma independiente, no propietaria, basada en la arquitectura abierta
- Posibilidad de utilizar los servicios internet Gopher, FTP, WWW
- Rápida visualización en línea de cualquier documento
- Reutilización de documentos y gráficos
- Seguridad, privacidad y actualidad
- Software cliente y servidor relativamente fácil y económico (IE, los Asistentes de Internet para Office, los visualizadores de Office, IIS, IS, MS y otros servidores para NT pueden bajarse gratuitamente de Internet)
- Soporte de consultas SQL
- Soporte de formularios en línea
- Soporte de una amplia variedad de motores de búsquedas

- Soporte de una filosofía de administración de documentos centralizada/descentralizada
- Trabajar eficientemente sobre infraestructuras ya existentes de redes, tanto para funciones locales (LANs), como remotas (WANs)
- Uso de periféricos (impresoras, etc.) de forma remota
- Utilizar todo tipo de plataforma instalada (UNIX, Mac, PC, OS/2, etc.)

Como se puede observar en tan amplia lista de opciones, una intranet goza de las virtudes y posibilidades tecnológicas de Internet, sólo que el uso del web está limitado a fines corporativos internos y, por lo tanto, ese es el único punto importante que los separa. Por lo tanto, la diferencia fundamental internet/intranet estriba en que una intranet es cualquier red interna que soporte la tecnología internet: web servers, TCP/IP, HTTP, FTP, HTML, URL, etc., mientras que Internet explota la misma tecnología en un entorno abierto, hacia afuera. Por ello las intranets no constituyen la competencia de Internet, sino una forma específica, lógica, complementaria y necesaria de su existencia, limitada, por así decirlo, a las LAN o WAN. Dado que asumo que el lector habrá navegado por Internet, no considero necesario extenderme mucho más al respecto. Sin embargo, considero oportuno destacar que la tecnología internet tendrá un efecto renovador en las aplicaciones comerciales para redes locales (lo que tiene muy ocupados y preocupados a los

productores tradicionales de productos para redes), pues esta tecnología a nivel de red significa:

- Elevada performance: corre en cualquier sistema operativo de los equipos cliente, soporte multiplataforma, soporta que se le adicione audio, vídeo, imágenes y todo tipo de recurso multimedia, todo lo cual hace mucho más efectiva la comunicación.
- Seguridad: la tecnología internet tienen varias décadas de existencia y, más allá de las limitaciones que posee (¿quién no?), está probada y ha demostrado en la práctica ser robusta, a la vez que muestra una muy positiva y rápida evolución en los aspectos de seguridad.
- Estandarización: dado que esta tecnología adopta los protocolos y APIs estándares del mercado, garantiza la fácil compatibilidad con herramientas de desarrollo y hardware (independientemente del productor), así como la más plena conectividad (comunicación), tanto internamente como con aplicaciones externas.
- Bajos costes comparativos: sobre todo en relación a los sistemas propietarios de redes, lo que se pone particularmente de manifiesto en los requerimientos de hardware, el software (sobre todo el software cliente), así como en el número de clientes conectados a la red.
- Comunicación universal: cualquier persona, departamento, sección o área de la empresa conectada a la intranet puede

interactuar con el resto de los conectados por mail, chat, newsgroup, "telefónicamente" o por videophone.

La rápida difusión de la tecnología internet a nivel de empresa está "garantizada" no sólo por las virtudes antes detalladas, sino también porque es verdaderamente cautivante para las empresas que la creación del servidor Web interno tenga bajos costes y que, como detallaremos en la próxima entrega, la inversión total sea poco riesgosa. En particular esto se debe que las mismas pueden instalase, en principio, en cualquier red local que soporte TCP/IP y convirtiendo los equipos que posea la empresa en servidores web y PCs clientes (con sus correspondientes software), para acceder a las aplicaciones de la misma manera que lo hacemos por Internet: navegando.

3.7. Intranets desde la perspectiva empresarial

La tecnología internet y su aplicación a nivel interno ha llegado al mundo empresarial en un momento muy particular del desarrollo de la economía, que se ha dado por llamar globalización, donde la información se ha convertido en un recurso sumamente estratégico para el éxito. En este contexto altamente competitivo no basta con disponer de buena información, sino de poder procesarla y difundirla tan rápido como sea posible y, atendiendo a los volúmenes de información que mueve cualquier empresa anualmente, a los menores costes posibles. Sólo así se puede ser eficiente en un entorno organizativo que clama por la calidad

total, la participación colaborativa, el marketing interno, TQM (Total Quality Management), dirección por objetivos, etc., todo lo cual es imposible sin tecnologías que permitan:

- Adaptarse rápidamente a los cambios del mercado
- Adoptar con inmediatez los modelos adecuados de negocios
- Asegurarse de que la información fluya por canales simples y seguros
- Costes razonables para instalar y mantener sistemas que gestionen estas soluciones
- Dar la garantía de que la información que se brinde en cada momento está actualizada
- Disponer de la información a demanda, de forma simple, intuitiva y, de ser posible, gráfica
- Fácil elaboración y actualización de la información
- Facilitar el incremento de la productividad en los distintos niveles del proceso de trabajo
- La reducción de los costes de los ciclos de producción (time-to-market)
- Satisfacer el incremento de la demanda de la calidad a todo nivel, sobre todo en los servicios

Sin embargo, a pesar de que quienes están responsabilizados con la toma de decisiones saben lo que precisan resolver, normalmente no tienen una respuesta técnica acabada sobre cómo y con qué satisfacer sus necesidades. Paradójicamente, esa situación no implica que no sepan cuánto y cómo están dispuestos a invertir para dar a su organización la

solución requerida. Y las intranets, dada su novedad, aún no suelen estar incluidas entre las alternativas a tener en cuenta para una inversión. Esta situación trae consigo que, por ahora, para implementar una intranet no basta con conocer y dominar sus posibilidades tecnológicas. Tan necesario como eso es poseer una adecuada perspectiva empresarial sobre las intranet, lo que incluye dominio sobre costes, técnicas para la comunicación interna, métodos para la organización de empresas, diseño de comunicaciones, diseño de páginas y otras muchas disciplinas propias del mundo empresarial. Por ello, una forma ventajosa de presentar una solución intranet es integrando todos esos elementos en un proyecto capaz de resolver lo que hasta ahora siempre se prometió y no se cumplió: comunicaciones, multimedia, entorno gráfico, aplicaciones de gestión, conexión transparente entre diferentes plataformas, etc. en una misma solución.

Hemos comprobado que para que la propuesta de intranet tenga éxito, debemos detectar cual es el área o actividad más adecuada para comenzar, proponiendo que la misma tome carácter de "prueba piloto". Puedo asegurar que la experiencia de la prueba piloto no sólo permitirá al cliente comprobar las bondades, potencialidades y perspectivas de la intranet, sino que la misma le facilitará tomar gradualmente las medidas que la nueva forma de organizar la comunicación demandará, lo que también nos ayudará a ajustar el proyecto total. Esto es así porque en dicho período no sólo conoceremos mejor las actividades del cliente

(incluso hasta en sus sutilezas), sino que de entre sus implicados surgirán los protagonistas más activos quienes, al "descubrir" las bondades de la nueva tecnología, trasmitirán al proveedor lo que consideran no debería faltar a la misma.

Una buena estrategia de trabajo al respecto es crear con dichos protagonistas un "grupo especial intranet" (o el nombre que se desee dar a ese grupo). La importancia de estos "grupos" es incalculable tanto para el proveedor como para el cliente, pues ellos no sólo canalizarán las necesidades e intereses de la empresa, sino que también se encargarán de promover el entusiasmo necesario para que la nueva tecnología no sea rechazada. Además, pueden realizar las funciones de testers de la aplicación, evaluar las posibilidades y prioridades intranets en cada área, aportar vías innovadoras para incorporar diferentes actividades al web, entrenar a empleados en el uso de las aplicaciones intranets, aportar los individuos que deberán colaborar en la administración del web, etc. Es evidente que con estas funciones el "grupo especial" no sólo puede contribuir a una mayor calidad de la solución intranet, sino que en muchos aspectos significará para el cliente la posibilidad de realizar economías, pues podría cumplir algunas tareas con su propia infraestructura.

Pero con ello no es suficiente. Mientras que las intranets no sean el pan nuestro de cada día en las redes corporativas, al realizar una propuesta de solución basada en intranets debemos incluir y destacar en el proyecto las ventajas básicas que estas brindan, es decir:

- Economía de la inversión gracias a la posibilidad de utilizar la infraestructura instalada (PCs, redes, sistemas operativos, etc.)
- Economía en la edición y publicación de información interna al sustituirse las impresiones
- Escalabilidad que permite crecer de acuerdo a un proyecto y abordar todo lo que se precise
- Incorporación de recursos multimedia: audio, vídeo, aplicaciones interactivas, etc.
- Inversión en el servidor similar a otras soluciones (si ya se tiene el servidor, la solución puede significar costes mínimos, limitados a la configuración de la tecnología Internet)
- Inversión mínima, por una única vez, para la configuración de cada máquina cliente (si ya disponen de Windows 95 o Windows NT Workstation, tan sólo deberá instalarse el browser)
- Posibilidades de establecer una estrategia distribuida de los recursos informáticos, capaz de integrar de forma flexible y eficiente a la más amplia gama de equipos y autores de información
- Posibilidades ilimitadas de uso del servidor intranet con otros fines informáticos e, incluso, la posibilidad de reutilizar una parte importante de las páginas para internet
- Rápida incorporación de nuevos documentos a la intranet
- Rápido proceso de aprendizaje para los usuarios (generalmente limitado a algunas horas), gracias a la interface gráfica e intuitiva que caracteriza a este tipo de aplicaciones

- Software a precios económico para la edición de documentos HTML: FrontPage está sobre los 100 dólares, Office97 está diseñado para que los documentos Word, Excel, PowerPoint, etc., se conviertan en archivos .html con tan sólo pulsar un botón de la barra de herramientas y, como si ello fuera poco, Internet Explorer soporta, instalando los correspondientes visualizadores en caso de no estar instalado el software original, el formato de los documentos de Office)
- Software gratuito para publicar los documentos (browsers y visualizadores)
- Tendencias en la difusión de las intranets y su aplicación por parte de la competencia

CAPÍTULO IV

SEGURIDADES

4.1. Seguridad Lógica

4.1.1. Introducción

Anteriormente las áreas de seguridad sólo se ocupaban de la Seguridad Física y contra incendios. Dichas organizaciones vivían en una situación ficticia de seguridad ya que en realidad el nivel de seguridad de las computadoras se encontraba por debajo del estándar aceptable. El compromiso de la gerencia con la efectividad real era bajo.

Actualmente, existen ciertos factores que han modificado el contexto dentro del cual se usan las computadoras y han aumentado el nivel de seguridad que se requiere:

- Concentración del procesamiento y aplicaciones más grandes y de mayor complejidad, las cuales son parte integral de la organización.
- Dependencia en el personal clave.
- Desaparición de los controles tradicionales.
- Terrorismo urbano e inestabilidad social.
- Mayor conciencia de los proveedores de computadoras.
- Mayor conocimiento masivo en temas informáticos.
- Mayor conectividad entre computadoras debido a Internet y a las redes internas.

Hoy en día se requiere un enfoque amplio de seguridad que permita resguardar los datos almacenados mediante métodos que controlen los accesos a ellos. La palabra datos pretende cubrir elementos tales como los archivos maestros y de transacciones, los datos en su estado original.

Los objetivos desde el punto de vista de Seguridad Lógica que se trataran a continuación son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin la supervisión minuciosa y no modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en el procesamiento.

4.1.2. Estándares de seguridad

Dentro de las principales organizaciones de estándares de seguridad en el mundo se encuentra el Centro Nacional de Seguridad Computacional (NCSC: National Computer Security Center) de Estados Unidos, el cual publica lineamientos para el uso de la seguridad dentro de los sistemas computacionales, sistemas operativos y acceso a bases de datos. En lo que respecta a seguridad en sistemas operativos, se han especificado varios niveles o clases.

Nivel C1. Protección de seguridad a discreción (Discretionary Security Protection). La base computacional de confianza (TCB: Trusted Computing Base) de un sistema de red nivel Cl literalmente satisface los requerimientos de seguridad a discreción al proporcionar la separación de datos y de usuarios. Incorpora controles rigurosos para el acceso, limitando a los usuarios con base en sus derechos y privilegios el acceso a los recursos o datos. Así, cada usuario tiene la capacidad de leer y proteger solamente su información, y por ninguna circunstancia otro usuario podrá leer, borrar o modificar dicha información ya sea por accidente o bien intencionalmente, a menos que le sean otorgados los derechos y privilegios para hacerlo.

Nivel C2. Protección de acceso controlado (Controlled Access Protection). Los sistemas de red en este nivel refuerzan los conceptos del nivel C1, llevando registro de las acciones de los usuarios en forma individual, a través de los procedimientos de login, auditando eventos referentes a la seguridad y el aislamiento de recursos.

Nivel B1. Protección de seguridad etiquetada (Labeled Security Protection). Los sistemas de red clase B1 requieren de todas las características necesarias para la clase C2. Adicionalmente, debe estar presente lo siguiente: un reporte informal del modelo de las políticas de seguridad, el etiquetamiento de datos y el control

mandatorio de acceso sobre temas y objetos almacenados. Debe existir la capacidad para un etiquetamiento preciso de la información exportada. Cualquier defecto en estas características identificado durante las pruebas debe ser eliminado.

Nivel B2. Protección estructurada (Structured Protection). En los sistemas de red del nivel B2, la base computacional de confianza (TCB) está estructurada en un modelo de políticas de seguridad formal claramente definido y documentado que requiere del reforzamiento de los controles de acceso a discreción y mandatorio encontrados en los sistemas de red del nivel B1, para ser extendidos hacia todos los temas y objetos en el sistema de red. Además, se direccionan canales de cobertura. El TCB debe ser cuidadosamente estructurado en elementos de protección crítica y de no–protección crítica. La interfaz TCB está bien definida y su diseño e implementación le permite a ésta estar sujeta a pruebas aún más exhaustivas y a una revisión más completa. Los mecanismos de autenticación están fortalecidos y la administración de las facilidades de confianza se da en forma de soporte por las funciones del administrador y operador del sistema; asimismo, se imponen controles estrictos en la administración de las configuraciones. El sistema es relativamente resistente a la penetración.

Nivel B3. Dominios de seguridad (Security Domains). Las TCB de nivel B3 deben satisfacer los requerimientos de monitoreo de referencias, ya que este nivel controla todos los accesos de temas a objetos, es a prueba de interferencias (inviolable) y lo suficientemente pequeño para estar sujeto a análisis y pruebas. Hasta este momento, la TCB está estructurada para excluir códigos no esenciales para el reforzamiento de las políticas de seguridad y está respaldada por una importante ingeniería de sistemas en el diseño e implementación de la misma, todo dirigido a minimizar su complejidad. Debido a ello se requiere un administrador de seguridad, los mecanismos de auditoría son expandidos para señalar eventos que se refieren a la seguridad y se necesitan procedimientos de recuperación de sistema. El sistema es altamente resistente a la penetración.

Nivel A1. Diseño verificado (Verified Design). Los sistemas del nivel A1 son funcionalmente equivalentes a aquellos del nivel B3, en cuanto a que no hay elementos arquitectónicos adicionales ni se añaden requerimientos de políticas. La diferencia de los sistemas en esta clase es el análisis que se obtiene del diseño formal de las técnicas de especificación y verificación, que deriva en un alto grado de seguridad de que la TCB esté correctamente implementada. Esta seguridad es un resultado natural que se obtiene al empezar con un modelo formal de las políticas de seguridad y con una especificación formal de alto nivel de diseño

(FTLS: Formal Top–Level Specification). En continuidad con el diseño extensivo y el análisis de desarrollo de la TCB requerido por los sistemas del nivel Al, se requiere una administración de la configuración más estricta y se establecen procedimientos para distribuir de forma segura el sistema en los sitios. Además se requiere un administrador de la seguridad del sistema.

4.1.3. Seguridad

Existen dos modelos principales de seguridad que otorgan permisos a las estaciones de trabajo para acceder a los recursos compartidos de la red. El primer modelo es a nivel usuario y el segundo es a nivel recurso.

La seguridad a nivel usuario requiere asignar ciertos derechos a cada usuario de la red. El usuario tiene una contraseña personal o password que puede modificar y, según los derechos que le han sido asignados, puede hacer uso de los recursos que estén disponibles para él.

La seguridad a nivel recurso implica asignar una contraseña o password a cada uno de los recursos disponibles en la red; el acceso a éstos es permitido únicamente a los usuarios que tengan autorización para hacerlo o a cualquier persona que conozca la contraseña.

4.1.4. Controles Lógicos de Acceso

Estos controles proveen medidas técnicas para encauzar la información a la que los usuarios pueden acceder, los programas que pueden ejecutar y las modificaciones que pueden realizar sobre los datos computarizados.

La implementación de este tipo de controles permitirá restringir los accesos de acuerdo con los requerimientos de procesamiento de los usuarios de las distintas áreas de la organización (quién puede acceder a qué datos) indicando el tipo de acceso permitido.

Los controles lógicos de acceso pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en otros utilitarios como el administrador de base de datos, o bien podrían estar incluídos en un paquete específico de seguridad, como por ejemplo el Kerberos, Racf y el Tacacs).

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde determinar un permiso de acceso solicitado por un usuario. Al respecto, existen varios criterios que pueden aplicarse:

- **Identificación y Autenticación.-** Para al mayoría de los sistemas, es la primera línea de defensa y permite prevenir el ingreso de personas no autorizadas a un sistema

computarizado. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina identificación al momento en que el usuario se da a conocer en el sistema, y autenticación a la verificación que realiza al sistema sobre esta identificación.

- **Roles.-** El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere el acceso a la información. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

- **Ubicación.-** El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica.

- **Horario.-** Este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

- **Transacciones.-** También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

- **Limitaciones a los servicios.-** Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

- **Modalidad de acceso.-** Se refiere al modo de acceso que se permite al usuario sobre la información. Esta modalidad puede ser:
  - Lectura: el usuario puede leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
  - Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
  - Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
  - Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos).

4.1.5. Control de Acceso Interno

Palabras Claves.- Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y

aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Encriptación.- La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

Listas de Control de Accesos.- Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Límites sobre la Interface de Usuario.- Generalmente son utilizadas en conjunto con las listas de control de accesos, y restringen el acceso de los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menúes, vistas sobre la base de datos y límites físicos sobre la interface de usuario (como por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas).

Etiquetas de Seguridad.- Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

4.1.6. Control de Acceso Externo

Dispositivos de Control de Puertos.- Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluídos en otro dispositivo de comunicaciones, como por ejemplo un módem.

"Firewalls" o Puertas de Seguridad.- Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada como por ejemplo Internet. La firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que prevenir la intromisión de hackers o virus a los sistemas de la organización.

4.1.7. Administración

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de Seguridad Lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos, especificando las consideraciones necesarias para el establecimiento de perfiles (información a la que el usuario necesita acceder para el desarrollo de las tares, criticidad de la información, funciones del puesto, etc.).

Un Programa Específico para la Administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas, y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

4.1.8. Criptografía

La criptografía consiste en modificar los datos de un fichero o los que se transmiten por módem, radio, etc. para evitar que los puedan leer personas no deseadas. Esta técnica ha tenido su principal aplicación en los ejércitos y en la diplomacia. Pero con el auge de los ordenadores, y la gran cantidad e importancia de la información que en ellos se almacena está convirtiéndose en un tema muy importante para la informática, sobre todo en las redes (especialmente en INTERNET) y el comercio a través de ellas.

4.1.9. Claves Simétricas y Asimétricas

Claves simétricas (secretas o únicas).- Se trata del mecanismo clásico. Estas técnicas usan una clave K que es conocida por el remitente de los mensajes y por el receptor, y con la que cifran y descifran respectivamente el mensaje. Para mantener la seguridad del cifrado, deben mantener esta clave en secreto.

Las ventaja del uso de estas claves es la existencia algoritmos muy rápidos y eficientes para su cálculo. Si K es lo bastante larga (típicamente se usan valores de 56 a 128 bits), es imposible reventarlas usando la fuerza bruta.

El principal inconveniente estriba en la necesidad de que todas las partes conozcan K, lo que lleva a problemas en la distribución de las claves. Esta debilidad ha hecho que sea poco utilizada en los mecanismos desarrollados hasta el momento para permitir el pago, a no ser que vaya combinada con otro tipo de técnicas.

Claves asimétricas.- Existen también sistemas asimétricos de cifrado, siendo los más populares los de clave pública. Estas técnicas se basan en la existencia de parejas de claves, una secreta (Ks), conocida únicamente por su propietario, y una pública (Kp), libremente distribuida por su propietario en toda la red. El conocimiento de una de las claves no permite averiguar la otra. Un mensaje es cifrado con una de las claves y descifrado con la otra.

Los algoritmos de cifrado que utilizan estas claves son usualmente muy lentos, por lo que no se suelen utilizar para cifrar datos. Lo más habitual es que las partes elijan una clave simétrica y la compartan mediante mecanismos de clave pública. Una vez compartida la clave, se aplican técnicas simétricas de alta velocidad.

Las claves públicas son más fáciles de romper (averiguar Ks a partir de Kp). 300 bits sólo valen para aficionados; 800 bits son una dimensión habitual para una calidad comercial, y a partir de 1000 bits puede considerarse una calidad aceptable para uso militar.

4.1.10. Firmas Digitales

Una firma digital es un bloque de caracteres que acompaña a un documento (o fichero), acreditando quién es su autor ("autenticación") y que no ha existido ninguna manipulación posterior de los datos ("integridad").

Para firmar un documento digital, su autor utiliza su propia clave secreta, a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría ("no revocación"). De esta forma, el autor queda vinculado al documento que firma.Cualquier persona puede verificar la validez de una firma si dispone de la clave pública del autor.

4.2. Seguridad Física

4.2.1. Diseño y Ubicación

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al equipo de cómputo del mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas, inundaciones.
- Amenazas hechas por el hombre:
- Disturbios, sabotajes internos y externos deliberados.

Ya se trate de actos naturales, errores u omisiones humanos y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

- Minimizando la posibilidad de su ocurrencia.
- Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.

- Diseño de métodos para la más rápida recuperación de los daños experimentados.
- Corrección de las medidas de seguridad en función de la experiencia recogida.

Para ello analizaremos los peligros más importantes que se corren en un centro de procesamiento con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

- Incendios
- Condiciones climatológicas
- Señales de radar
- Instalación eléctrica
- Sistema de aire acondicionado
- Mantenimiento
- Ergonomía

Incendios.- Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

Ubicación física

- El área del computador debe estar en un local que no sea combustible.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes del área del computador deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- El falso piso instalado sobre el piso real, debe construirse con materiales incombustibles o resistentes al fuego y antes de instalar la computadora, el espacio entre ambos pisos debe limpiarse, pintarse y mantenerse limpio permanentemente.
- Debe existir la prohibición absoluta de fumar en el área de proceso.
- Deben emplearse muebles incombustibles, cestos para papeles metálicos.
- Deben evitarse los materiales plásticos o inflamables .
- El piso y el techo en el recinto de ubicación de la computadora y de almacenamiento de los medios magnéticos deben ser impermeables.

Seguridad en el hardware y el software

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal

autorizado, además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta:

- La temperatura, no debe sobrepasar los 65º C,
- El limite de la humedad no debe superar el 85 % para evitar el deterioro,
- La biblioteca no debe situarse próxima a la computadora, debe contar con un área cerrada a prueba de fuego.

Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

Condiciones climatológicas.- Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Una vez más las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran esta documentada. La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Medidas preventivas

- El centro de cómputos no debe estar en una planta baja o subterránea si el edificio esta en una zona de inundación frecuente.
- Sistemas de drenaje adecuados y eficientes.
- Evitar proximidades directas con tuberías de agua.
- Se debe tener cuidado con fugas en los aparatos de aire acondicionado.
- Se debe contar con medidas para detectar la presencia de agua debajo del piso antes de que se vuelvan peligrosas para el equipo.
- Contar con cubiertas plásticas para el equipo de cómputo y detectores de agua e idealmente con bombas para evacuar rápidamente el agua.

Señales de Radar.- La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años.

Para evitar los posibles efectos, la manera más práctica de resolver el problema en instalaciones con ventanas de vidrio, consiste en la colocación de cortinas con hojas de aluminio o algún material metálico similar.

Instalación Eléctrica.- Trabajar con computadoras implica trabajar con electricidad. Por lo tanto es una de las principales áreas de la seguridad física. Además es una problemática que abarca desde el usuario hogareño hasta la gran empresa. Veamos cuáles son los lineamientos básicos de las medidas de seguridad física con respecto a las instalaciones eléctricas, en la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Los tomacorrientes deben tener puesta a tierra real. Una puesta a tierra real significa que el tercer conector del tomacorriente está conectado, por medio de un cable, a una barra de cobre enterrada bajo tierra (este tipo de instalación la debe realizar un electricista especializado). Esta conexión actúa cuando se produce una descarga sobre un aparato eléctrico (por ejemplo, la computadora), derivándola hacia la barra de cobre enterrada, en lugar de hacia la persona que esté tocando el aparato.

Contar con un disyuntor, llaves térmicas o algún otro sistema de protección disminuye los riesgos de electrocución.

La instalación debe estar en buen estado, sin remiendos caseros y se deben evitar los "pulpos" que se forman cuando (triples mediante)

conectamos "todo" al mismo tomacorriente. Invertir algo de dinero en la visita de un electricista responsable no sólo puede prevenir accidentes humanos sino que disminuye el riesgo de pérdidas de información por corte de energía eléctrica.

Si se vive en una zona con muchas variaciones de tensión es conveniente conectar la computadora con un filtro de línea que amortigüe estas fluctuaciones que pueden dañar el equipo. Además todo centro de procesamiento de datos deberá considerar la instalación de equipos que garanticen un suministro eléctrico en todo momento y con las especificaciones adecuadas como los Uninterruptable Power Source (UPS, alimentación ininterrumpida por batería), que dan autonomía suficiente (dos horas) para terminar el trabajo y grabarlo, en caso de corte de suministro. La selección de estos equipos debe decidirse basándose en requerimientos de energía, reserva de electricidad y confiabilidad (determinar en promedio cuántas veces al día se usarán las pilas del UPS). También se pueden instalar generadores de respaldo (que funcionan normalmente con diesel) para proveer electricidad. El suministro de energía debe considerar el consumo del equipo de aire acondicionado, la computadora y sus periféricos así como equipos de redes (especialmente cuando hay cómputo distribuido) y telecomunicaciones.

En toda instalación de equipo de cómputo deberá existir una red de pararrayos que garantice que toda descarga eléctrica atmosférica sea derivada a tierra; con ésto también se disminuirá el riesgo de incendio. Otros riesgos son los cambios de voltaje. Por lo tanto, deben instalarse supresores de picos, reguladores de voltaje, dispositivos de monitoreo y alarmas. Muchos constructores de equipo recomiendan conectar la CPU y los periféricos a diferentes circuitos para mantenerlos aislados eléctricamente.

Sistema de Aire Acondicionado.- Se provee un sistema de calefacción, ventilación y aire acondicionado separado, que se dedica al cuarto de computadoras y equipos de proceso de datos en forma exclusiva. Cualquier sistema de HVAC (Heat Ventilation Aconditionated Air) que preste servicios en otras áreas, puede también ser utilizado en el cuarto de computadoras y equipos de proceso de datos, si se proveen apagadores de fuego / humo en el punto de penetración del límite del cuarto.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, provocados por fugas a través de los ductos, es recomendable instalar redes de protección en todo el sistema de ductos al interior y al exterior, extinguidores, detectores de incendio, monitores y alarmas de sonido efectivas.

Los tubos por los que circula el aire acondicionado central en los falsos techos, no deben tener fibra de vidrio porque es altamente combustible.

Mantenimiento.- La limpieza de la instalación de cómputo es importante desde dos puntos de vista: Primero, refleja una actitud disciplinada. La seguridad es en gran parte una actitud mental y se refleja en el hecho de que los procedimientos adecuados y efectivos estén en uso. Y segundo, el mal mantenimiento crea condiciones para una brecha en la seguridad, o bien propicia incendios, al dejar papeleras o cajas en los rincones de las salas. El buen mantenimiento refleja la actitud general de las personas en una empresa, simboliza una buena administración y aumenta la seguridad en computación.

Las áreas de procesamiento de datos serán evaluadas según las amenazas potenciales del calor, polvo, electricidad estática y humedad. Los excesivos niveles de polvo o filtraciones de aire pobre pueden causar fallas frecuentes en las computadoras, impresoras u otros periféricos.

Los niveles de humedad relativamente altos (80% y más) pueden causar problemas en sistemas de computadoras incluyendo corrosión de contactos eléctricos o la textura del papel, etc. La humedad relativamente baja puede permitir que el papel se pegue

o se atranque. Por eso acondicionar la temperatura es esencial para todo el área de procesamiento de datos.

Las instalaciones de cómputo son muy sensibles a la temperatura, incluso temperaturas de 50 a 60°C pueden tener efectos muy dañinos en equipo y medios de almacenamiento de información. Por lo tanto deben existir sistemas de aire acondicionado con salidas bien distribuidas, también la construcción del centro de cómputo tiene que estar bien diseñada de modo que no haya fugas del aire frío ni entradas de aire caliente o polvo.

Resulta vital mantener limpio el centro de cómputo. También es importante para la estabilidad de la operación, que el aire esté limpio y libre de partículas (se deben instalar filtros). Otras medidas que se pueden poner en práctica para eliminar ciertos tipos de contaminación y para minimizar el impacto de contaminantes que no pueden ser totalmente eliminados, son las siguientes:

- Prohibir comer, fumar y beber dentro del centro de cómputo
- Vaciar los basureros y sacar el papel de desperdicio del centro de cómputo
- Poner las impresoras fuera del cuarto donde están las CPU, unidades de cinta, etc.
- Observar medidas apropiadas de mantenimiento del piso falso, etc.

- Asegurar que todas las computadoras estén equipadas con los mejores filtros que el vendedor puede proveer
- No instalar purificadores de aire generadores de iones y dar un buen mantenimiento al aire acondicionado

Ergometría.- El enfoque ergonómico plantea la adaptación de los métodos, los objetos de trabajo (materias primas), las maquinarias, herramientas e instrumentos o medios de trabajo y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección a los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro. La ergonomía intenta modificar las condiciones de trabajo y, así, las ventajas que ofrece son interesantes, no solo para los trabajadores sino también para los empleadores, desde el momento en que un trabajo más simple determina, en términos generales, un sustancial aumento de productividad. Por lo tanto:

La ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.

CAPÍTULO V

INSTALACIÓN DE UNA RED

5.1. Aspectos Generales de la Instalación

- Representar gráficamente toda la instalación. El instalador original del cableado telefónico existente podría ofrecernos documentación sobre éste. Anotaremos todos los problemas para futuras consultas.
- Conocer los techos y paredes del edificio para evitar sorpresas. Podríamos encontrar muros de hormigón o placas antiincendios en lugares inesperados. Debemos comprobar las placas de doble techo al buscar sitios para pasar el cable, y asegurarnos de evitar equipos eléctricos como acondicionadores de aire, cables de media tensión y fluorescentes.
- Evitar extender el cable en pasillos y otras áreas de paso.
- Asegurarse de que los puntos de conexión de estaciones están cerca de una toma de electricidad.
- Planificar la instalación del cable y asignarle el tiempo suficiente para hacer bien el trabajo.
- Trabajar fuera de horas de oficina cuando no se desee molestar a los empleados.
- Al montar conectores de par trenzado, asegurarse de que los hilos se conectan a los terminales adecuados.

- Al usar cable de par trenzado, comprobar la continuidad entre el cajetín y la estación de trabajo. Hay una serie de herramientas de verificación que se usan para tal efecto.
- Si se utiliza cable coaxial, evitar doblar, arrugar , estirar o forzar el cable, ya que esto podría causar modificaciones en las características eléctricas del conductor y producir errores de transmisión de los paquetes.
- Las bolas y piedras pueden ser las mejores amigas de un instalador. Atando una cuerda a una pelota de tenis, podremos lanzarle a un colega para poder pasar un cable por un espacio cerrado. Una cuerda atada a una piedra puede bajarse por un orificio en la pared. Cuando se necesita introducir un cable por una instalación existente, pueden resultar útiles unas varillas finas de hilo de nylon resistente.
- Los radioteléfonos son útiles cuando se necesita comunicarse con una persona que se encuentra al otro lado de una pared o techo.
- Evitar tender el cable cerca de luces fluorescentes en los dobles techos. Para evitar problemas, debemos planificar los tendidos con cable de sobra.
- Evitar pasar el cable cerca de otros cables eléctricos siempre que sea posible. Aunque el apantallamiento inhibe las interferencias, no está de más ser prevenido.
- Fijar el cable con broches, grapas o abrazaderas y evitar doblarlo demasiado. No estirarlo al pasarlo por los conductores.
- Asegurarse de que todos los tramos de cable son del mismo tipo y preferiblemente del mismo fabricante. El cable puede resultar parecido

pero tener distintas características eléctricas. Un solo tramo de cable inadecuado puede causar problemas de transmisión en todo un segmento de la red.

- La humedad puede deteriorar el cable, así que protegeremos los tendidos de cables externos de la acción de los elementos usando tubos u otras envolturas.
- Los tramos largos de cable son susceptibles a las interferencias. Los cables metálicos tienden a actuar como una antena que capta los campos eléctricos e interferencias de los dispositivos que encuentra a su paso. A medida que se incrementa la longitud del cable, disminuye su capacidad de transmisión de señal. Si los programas de monitorización y análisis informan de un gran número de errores por reenvío de paquetes, esto podría señalar un problema de interferencias en el cable.
- Evitar problemas con las tomas a tierra.
- Los problemas de cableado son relativamente fáciles de detectar en las redes configuradas en estrella. Si una estación no entra en comunicación con la red, verificaremos su tarjeta de red o el cable de conexión. Si fallan varias estaciones conectadas a un concentrador o hub, comprobaremos el concentrador.

5.2. Como instalar una red

En el caso de que necesitemos conectar dos computadores de forma económica podemos usar Windows 95/98 y necesitaremos:

• dos tarjetas de red			
C O A X I A L	• cable • dos conectores BNC para los extremos del cable • dos conectores BNC en forma de T • dos terminales	• cable • dos conectores RJ45 • ponchadora	**U T P**

- Comprobar que tipo de computadores se van a conectar.
- Comprobar que tengan una ranura libre, tipo PCI o tipo ISA, cada computador. Esto se puede hacer mediante un software adecuado o bien abriendo el PC y mirando el número de ranuras que tenga.
- Medir la cantidad de cable que va a ser necesario y adquirirlo.
- Con el computador apagado, abrir cada computador insertar la tarjeta de red.
- Cerrar el computador y encenderlo.
- Utilizar el diskette del fabricante de la tarjeta para configurarla y testearla.
- Reiniciar el computador una vez configurada la tarjeta.
- Comprobar que coinciden las configuraciones de la tarjeta de red y la que le asigna Windows, en caso contrario cambiarlas y volver a reiniciar para que los cambios tengan efecto.
- Instalar las utilidades de Windows para Redes.
  - Panel de Control
  - Red

- Agregar Adaptador
- Microsoft Acceso Telefónico a Redes.
- Protocolo Microsoft TCP/IP.
- Cliente Microsoft

  Cliente para Redes Microsoft.

Los dos PC's deben pertenecer al mismo Grupo de Trabajo. Asegúrese de que el nombre de Grupo de Trabajo coincide en ambos computadores. El nombre del PC debe ser distinto naturalmente.

- Reiniciar.
- Hacer click en el icono Entorno de Red y ver si aparecen los dos PC's con el nombre asignado. En caso afirmativo ya tenemos nuestra red.

5.3. Instalación y Configuración de una Red Local

En primer lugar, se necesita tener instalado y configurado el hardware de la red (tarjetas de red, hub, cableado).

5.3.1. Instalación bajo Windows 95/98/NT

Accedemos al “Panel de Control”, en Inicio → Configuración → Panel de Control. Una vez allí, abra el icono Red:

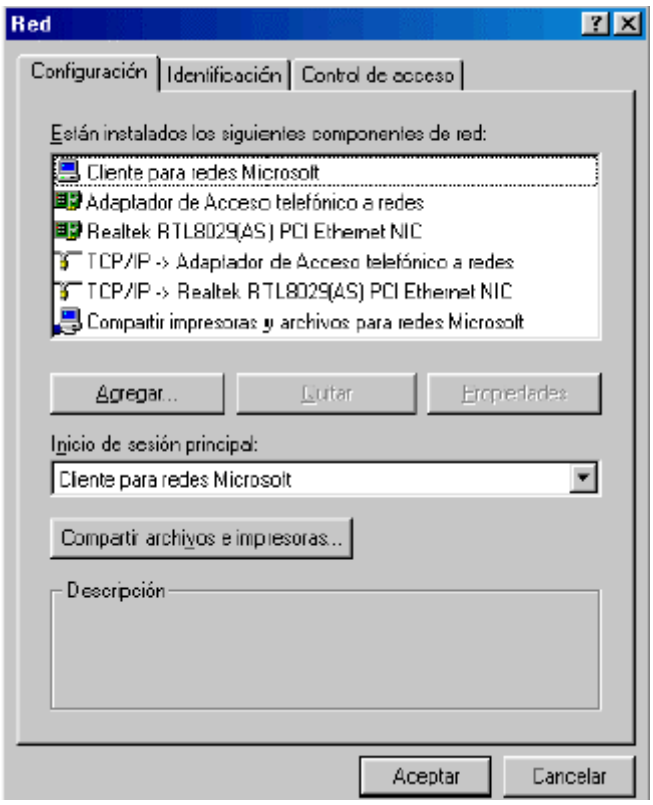


Fig. 5.1. Ventana de diálogo del icono red

Busque el protocolo TCP/IP asociado a la tarjeta de red. Si no lo encuentra, agréguelo (Agregar → Protocolo → Microsoft → TCP/IP)

A continuación, deberá configurarlo. Para ello, debe seleccionarlo y abra las Propiedades:

Fig. 5.2. Propiedades de TCP/IP (Dirección IP)

Debe marcar la casilla “Especificar una dirección IP” y a continuación debe introducirla. Cada computador debe tener su propia dirección, y no pueden estar duplicadas. Se recomienda llamar al servidor 192.168.0.1 y a los clientes 192.168.0.2, 192.168.0.3, 192.168.0.4, etc. La máscara de subred siempre es 255.255.255.0.

A continuación, seleccione la pestaña DNS. Seleccione la opción “Activar DNS”. En el campo Host introduzca el nombre del computador (ej. computador2, servidor, administracion, etc) en

minúsculas y sin acentos. Después, en el campo Orden de búsqueda del servidor DNS introduzca la dirección IP del servidor donde está instalado ABC Proxy y pulse Agregar. Una vez hecho esto, pulse sobre el botón Aceptar.

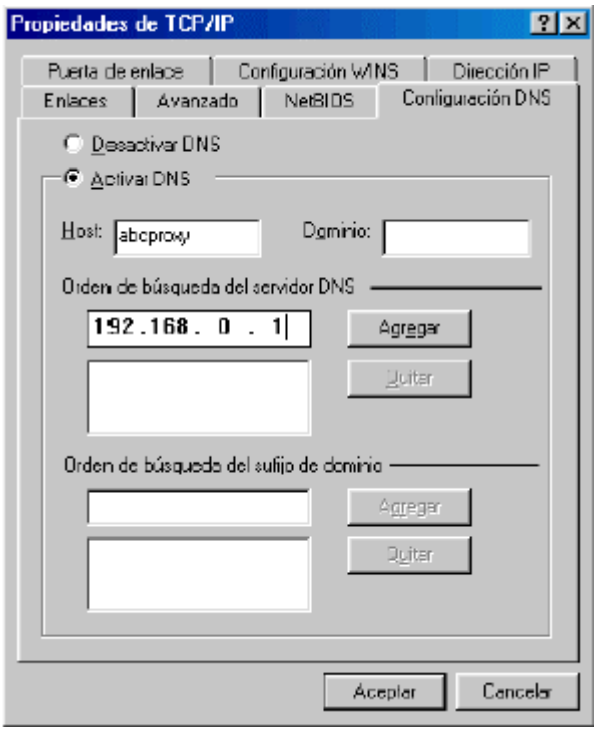


Fig. 5.3. Propiedades de TCP/IP (Configuración DNS)

Windows deberá reiniciar el computador y es posible que necesite el CD-ROM de Windows.

5.3.2. Instalación bajo Windows ME/2000

Haga clic derecho en el icono “Entorno de Red” que está ubicado en el Escritorio, y seleccione la opción “Propiedades”.

Después hacemos clic en “Conexión de Area Local”, apareciendo esta pantalla:

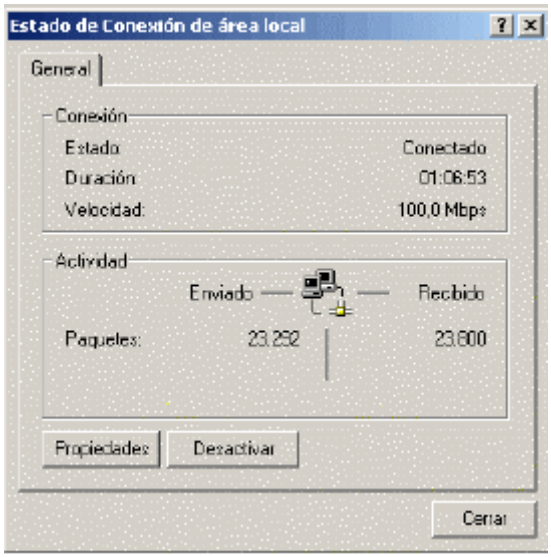


Fig. 5.4. Ventana de diálogo de Conexión de Area Local

Seleccionamos el botón Propiedades y nos aparece esta pantalla:

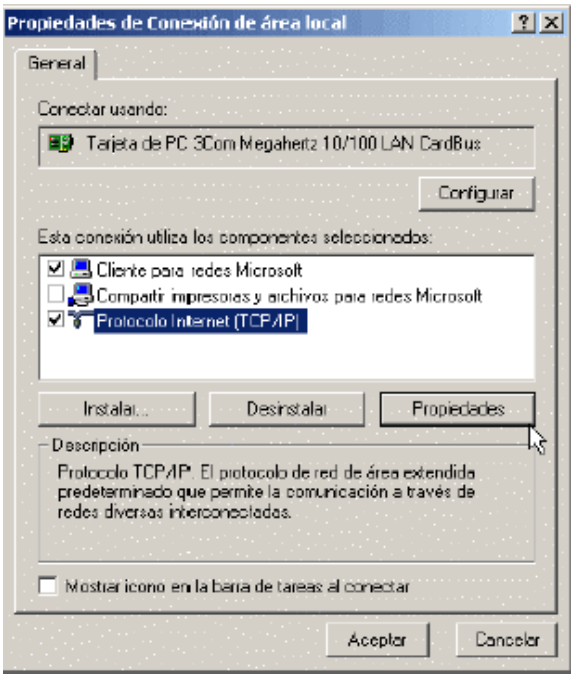


Fig. 5.5. Propiedades de conexión de área local

En esta pantalla, deberá comprobar que aparece el protocolo “Protocolo Internet (TCP/IP)”. Si no aparece, pulse el botón Instalar y agréguelo (Añadir → Protocolo → Microsoft → TCP/IP)

Ahora seleccionamos el protocolo “Protocolo Internet TCP/IP” y pulsamos el botón Propiedades. Aparece una pantalla similar a esta:

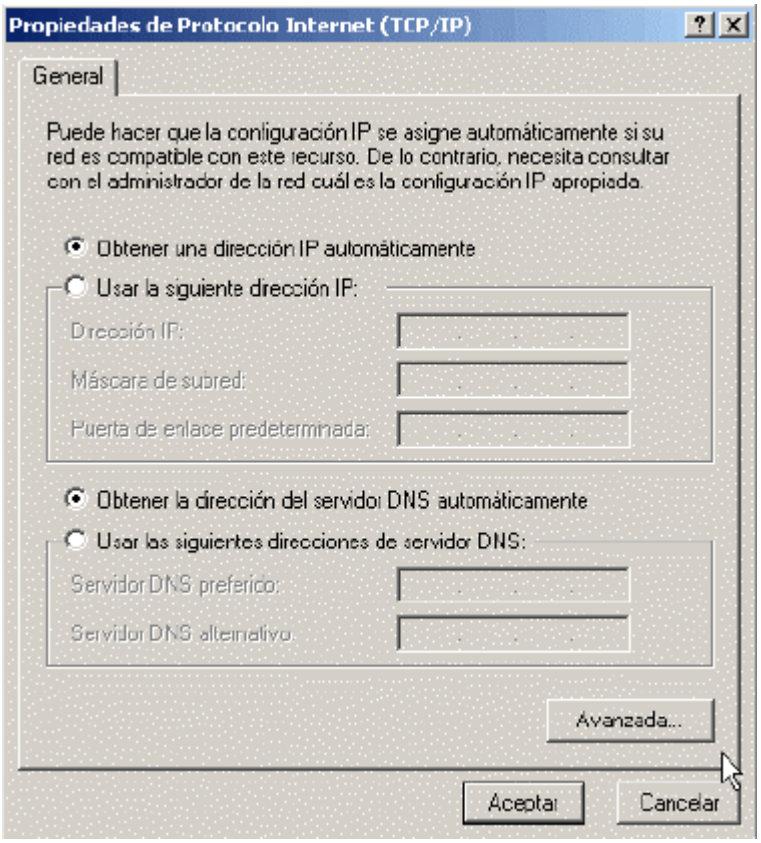


Fig. 5.6. Ventana de Protocolo Internet (TCP/IP)

Debemos marcar la casilla “Usar la siguiente dirección IP” y en el campo Dirección IP introducimos una dirección IP para el computador. Cada computador de la red local debe tener una dirección IP diferente. Es recomendable que introduzca 192.168.0.1

para el computador donde instalamos ABC Proxy (servidor), y para los demás computadores 192.168.0.2, 192.168.0.3, etc.

En el campo Máscara de subred, introduzca 255.255.255.0. Este dato no varía en los equipos. En el campo Puerta de enlace predeterminada los dejamos en blanco.

A continuación, marcamos la casilla “Usar las siguientes direcciones de servidor DNS” y en el campo Servidor DNS preferido, introducimosla dirección IP del computador donde está instalado ABC Proxy, que por defecto es 192.168.0.1. En campo Servidor DNS alternativo lo dejamos en blanco. Pulsamos Aceptar dos veces para guardar los cambios. Windows puede solicitarnos el CD-ROM de instalación.

5.3.3. Instalación bajo Windows XP

Haga clic en Inicio → Panel de Control. Seleccione la categoría “Conexiones de Red”. En el menú izquierdo, haga clic en Crear una conexión nueva para lanzar el Asistente para Conexión Nueva. Pulse Siguiente y en el Tipo de Conexión, seleccione “Conectarse a Internet”. Pulse Siguiente:

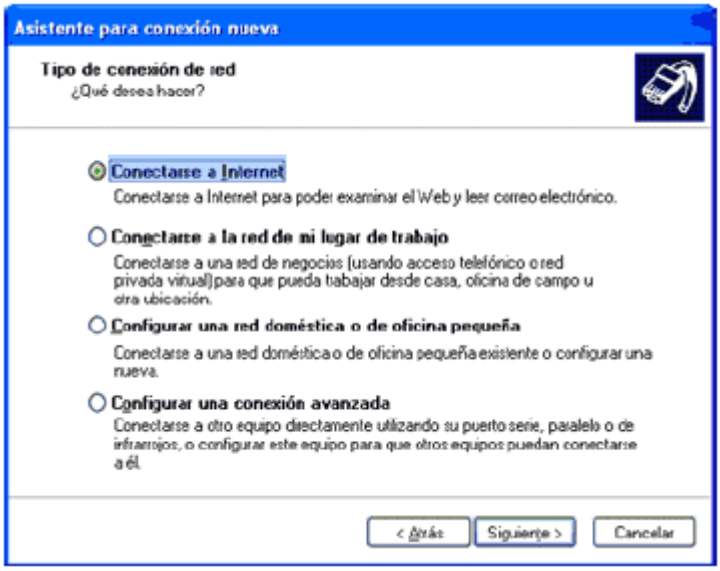


Fig. 5.7. Asistente para conexión nueva (Tipo de conexión de red)

Seleccione “Establecer mi conexión manualmente” y haga clic en Siguiente:

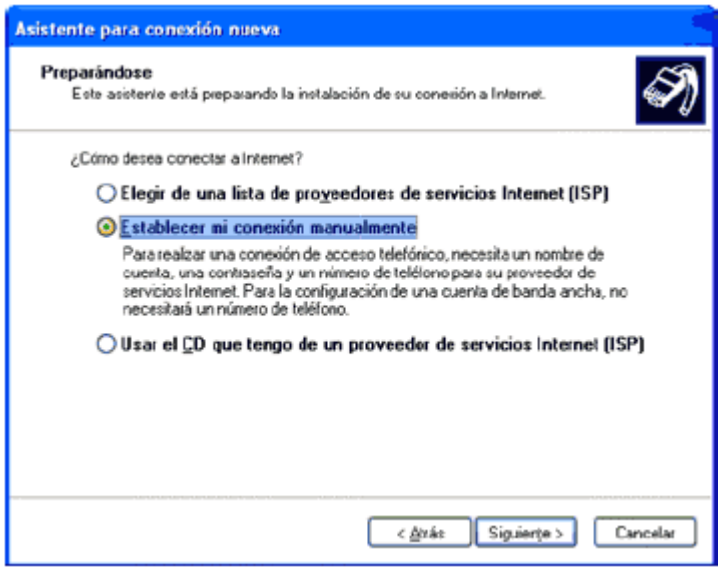


Fig. 5.8. Asistente para conexión nueva (Preparándose)

Ahora seleccione la opción “Conectarse usando una conexión de banda ancha que está siempre activa”. Haga clic en siguiente:

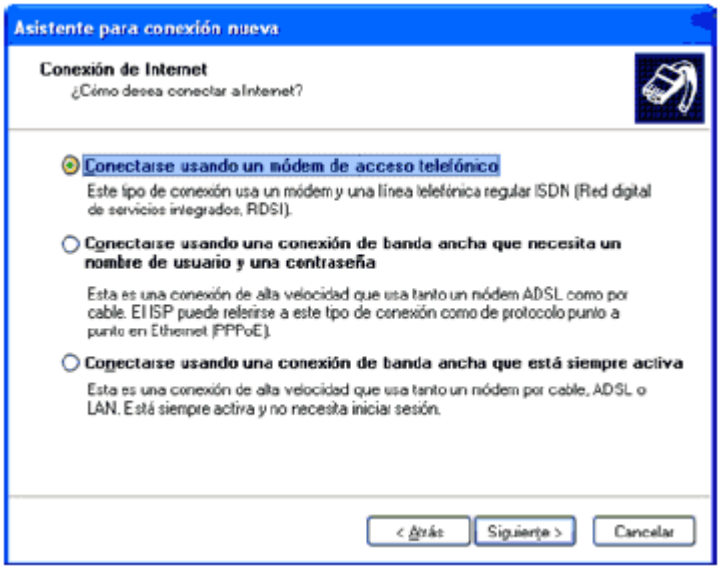
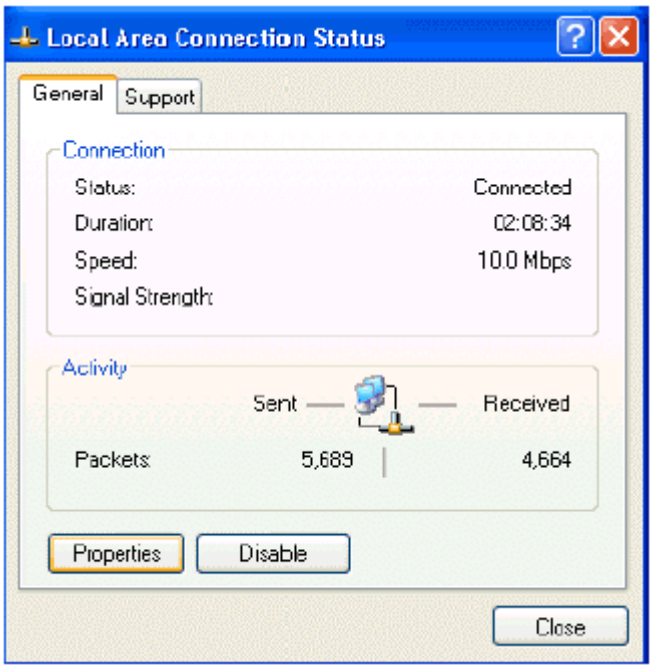


Fig. 5.9. Asistente para conexión nueva (Conexión a Internet)

Pulse el botón Finalizar. En la ventana Conexiones de red, haga doble clic en el icono titulado Conexión de Area Local (LAN). Aparecerá una ventana muy similar a esta, y debe pulsar el botón propiedades:



5.10. Estado de Conexión de Area Local

A continuación, haga clic en la pestaña General, después haga un clic en “Protocolo Internet (TCP/IP)”. Pulse Propiedades. En la pestaña General, debemos marcar la casilla “Usar la siguiente dirección IP” y en el campo Dirección IP introducimos una dirección IP para el computador. Cada computador de la red local debe tener una dirección IP diferente. Recomendamos que introduzca 192.168.0.1 para el computador donde instalamos ABC Proxy (Servidor), y para los demás computadores 192.168.0.2, 192.168.0.3, etc.

En el campo Máscara de subred, introduzca 255.255.255.0. Este dato no varía en los equipos. El campo Puerta de enlace predeterminada lo dejamos en blanco:

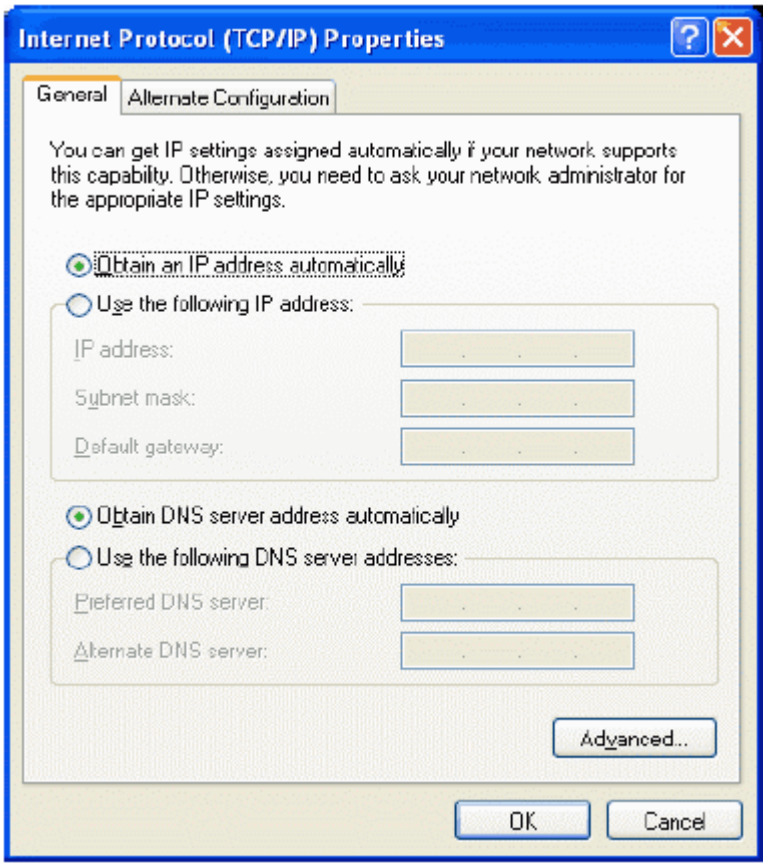


Fig. 5.11. Propiedades del Protocolo Internet

A continuación, marcamos la casilla “Usar las siguientes direcciones de servidor DNS” y en el campo Servidor DNS preferido, introducimos la dirección IP del computador donde está instalado ABC Proxy, que por defecto es 192.168.0.1. En el campo Servidor DNS alternativo lo dejamos en blanco. Pulsamos Aceptar dos veces para guardar los cambios. Windows puede solicitarnos el CD-ROM de instalación.

CAPÍTULO VI

MARCO ADMINISTRATIVO

6.1. Cronograma

MESES / ACTIVIDADES	NOVIEMBRE				DICIEMBRE				ENERO				FEBRERO			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Entrega Perfil de Proyecto				X												
Aprobación Perfil de Proyecto					X											
Capítulo I						X										
Capítulo II						X	X									
Capítulo III							X	X								
Capítulo IV								X								
Entrega del Primer Avance										X						
Capítulo V											X					
Capítulo VI											X	X				
Capítulo VII												X	X			
Revisión Final por el Director														X		
Entrega Final del Proyecto															X	

6.2. Presupuesto

CANT	DESCRIPCIÓN	V. UNIT.	V. TOTAL
1	Switch	60.00	60.00
1	Hub	35.00	35.00
2	Rollos de manguera flexible	11.00	22.00
12	Canaletas blancas	2.00	24.00
200 m	Cable UTP	0.55	110.00
	Accesorios	20.00	20.00
	Tacos Fisher	5.00	5.00
	Tornillos	5.00	5.00
	Tapas, cajetines, conectores	70.00	70.00
	Canaletas planas	20.00	20.00
	Grapas	3.00	3.00
		TOTAL →	**374.00**

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

- El presente trabajo demuestra que las potencialidades de la tecnología Internet coloca a las soluciones intranets en un lugar muy particular a la hora de competir con las soluciones tradicionales, pues aplicarlas significa además de acceder a una magnífica y fácil interface gráfica de trabajo, soluciones a bajo costo basadas en la explotación de las infraestructuras básicas existentes.

- La notable tendencia del crecimiento de las intranets es la respuesta espontánea a una necesidad vital para el mundo empresarial contemporáneo para disponer de un eficiente y confiable mecanismo para la comunicación interna de la institución o empresa.

- La tecnología Internet, a pesar de las limitaciones que aún posee representa los cambios más importantes en las comunicaciones desde la invención del teléfono. Por esta razón no es casual ni exagerado que los expertos y analistas del sector lo traten como sinónimo de telefonía del siglo XXI.

7.2. Recomendaciones

- Es necesario evitar los llamados cuellos de botella, ya que constituyen un verdadero obstáculo para que las intranets cumplan con eficiencia su acometido, pues los cuellos de botellas suelen crear las condiciones ideales para que la información sea incorporada a la red con atrasos.

- Para que las intranets satisfagan las expectativas del mundo empresarial deberá garantizarse la fácil incorporación de la documentación que cada organización genera a su torrente digital, lo cual será posible con la generación directa de documentos para la red.

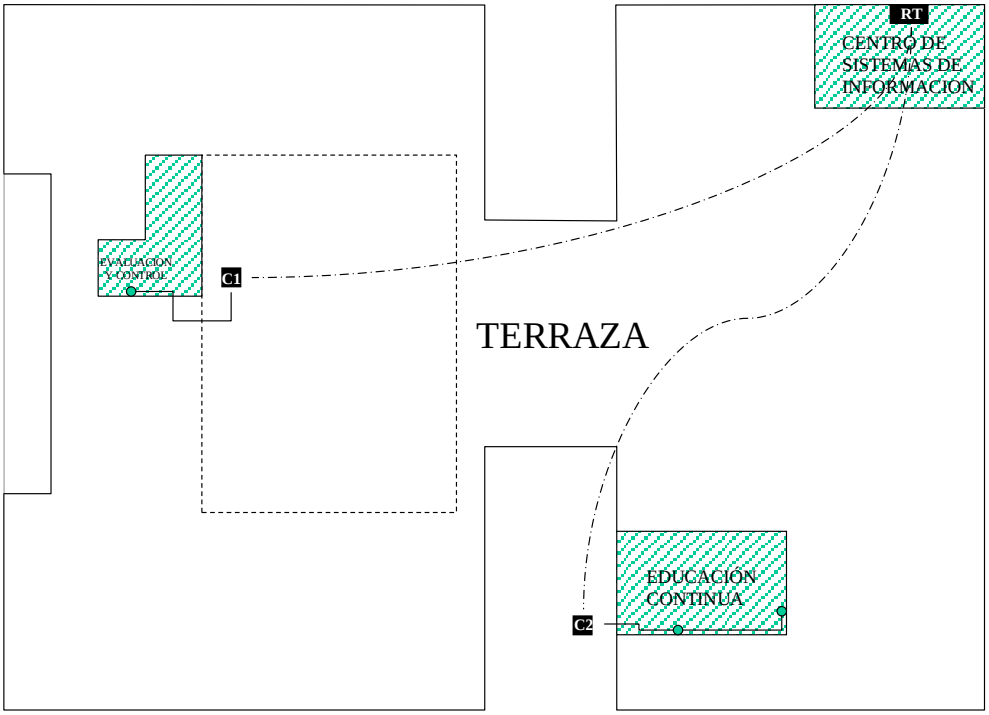
- Se debe tener muy en cuenta la seguridad, ya que es un punto neurálgico en los temores de los clientes, para lo cual se debe establecer una adecuada política de seguridad digital tomando en cuenta aspectos como: tecnología a implementar, niveles de acceso a la información, frecuencia de cambio de claves para acceder a determinados webs, etc.

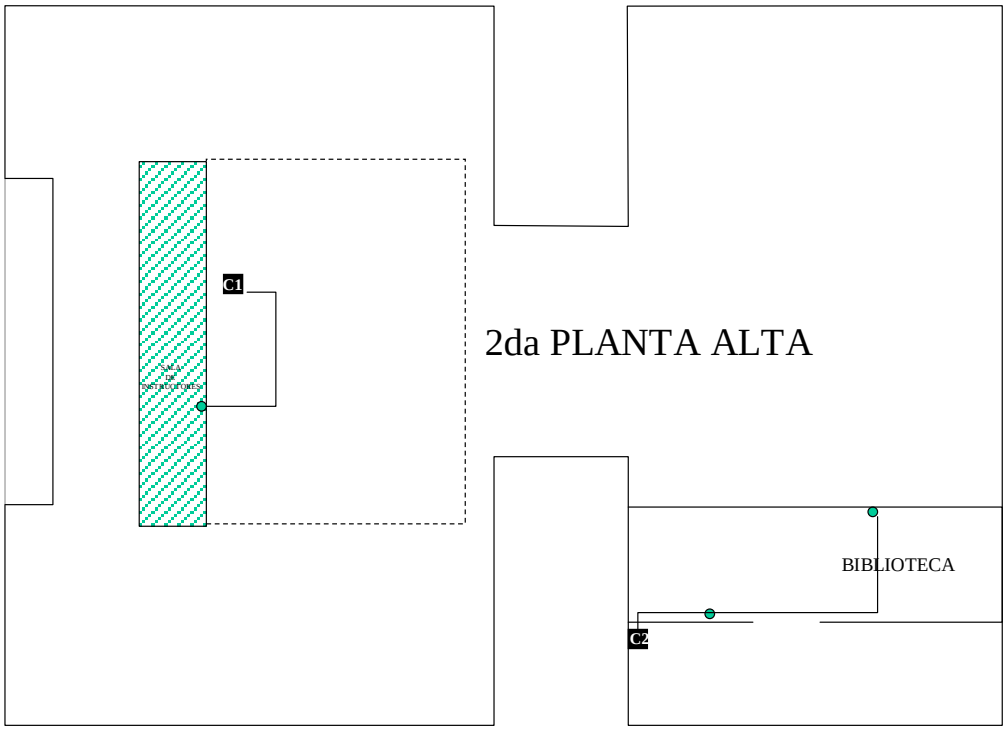
BIBLIOGRAFÍA

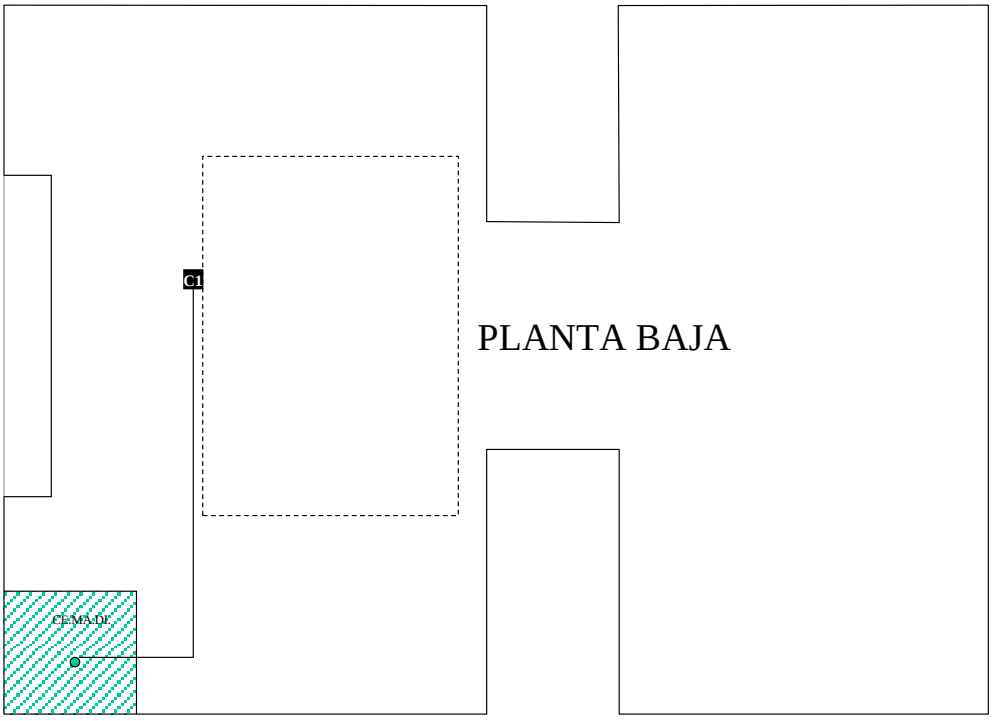
- Computer Networks. Andrew Tanenbaum. Prentice Hall PTR, Third Edition. 1996.
- Tecnologías de Interconectividad de Redes. Merilee Ford, H. Kim Lew, Steve Spanier, Tim Stevenson. Prentice Hall, Primera Edición. 1998.
- Internetworking LANs and WANs. Gilbert Held. Wiley Communications Technology, First Edition. 1995.
- Comunicaciones y Redes de Computadores. William Stalling. Prentice Hall, Sexta Edición. 2000.
- Tecnologías Emergentes Para Redes de Computadores. Uyless Black. Prentice–Hall. 2000.
- MundoPC.NET - http://www.ciudadfutura.com/mundopc/redes/indred.htm
- Técnico en Telecomunicaciones Tomo 1, 2 y 3. Julián Espinosa de los Monteros, Oscar López Gómez, Santiago García, Editorial Cultural S.A., Madrid–España, 2002.
- Introducción a las Redes de Area Local. Jorge E. Rodríguez G., Editorial McGraw-Hill Interamericana Editores S.A. México, 1996.
- Técnico en Redes y Comunicaciones para Computadores, CODESIS.
- http://tips.iworld.com
- MundoPC.NET - http://www.ciudadfutura.com/mundopc/intranets

ANEXO A

PLANOS DEL PROYECTO




C1
2da PLANTA ALTA
BIBLIOTECA
C2


C1
PLANTA BAJA

ANEXO B

FOTOGRAFÍAS DEL PROYECTO DESARROLLADO

GLOSARIO DE TÉRMINOS

10BASE–T.- Se trata del estándar IEEE 802.3 para Ethernet con una velocidad de transmisión de 10 Mbps que utiliza un cable UTP.

100BASE–T.- Se trata del estándar IEEE 802.3 para Ethernet con una velocidad de transmisión de 100 Mbps a través de un cable UTP.

ACCESO REMOTO.- Se denomina así a la posibilidad de ejecutar programas en sistemas remotos; al exportar a otros sistemas aquellos procedimientos que requieren mucho tiempo, se libera la estación de trabajo local.

ANCHO DE BANDA.- Es el rango (las frecuencias comprendidas entre dos límites) de las frecuencias que se pueden pasar a través de un canal de comunicación.

ARCNET.- Red disponible de Datapoint Corporation y otros fabricantes, que permite conectar una amplia variedad de PC y estaciones de trabajo por medio de un cable coaxial, par trenzado o fibra óptica.

ATENUACIÓN.- Disminuir la fuerza de una señal al aumentar la distancia. Se mide en decibeles y se incrementa a medida que la fuerza de la señal disminuye.

ATM.- Una tecnología de red, que transfiere paquetes de datos para el posterior reenvío de diferentes tipos de información (video, datos, comunicación oral).

AUTENTICACIÓN.- En un sistema operativo de red o multiusuario, proceso que valida la información de ingreso de un usuario. Por lo general, la autenticación involucra la comparación del nombre y las contraseñas con una lista de usuarios autorizados.

BACKBONE.- Proción de la red que administra el tráfico pesado. Puede ser el punto de conexión de varios edificios o localidades y también tener enlazadas pequeñas redes.

BPS.- Bits por segundo; se refiere a la velocidad a la que la información es enviada sobre una conexión lógica.

BROADBAND.- Se refiere a la técnica de cable coaxial en la cual varias señales moduladas sobre varias portadoras se transmiten sobre un solo cable coaxial.

BYTE.- Se llama así a un grupo de bits que tiene un significado singular.

CABLE COAXIAL.- Es un tipo de cable donde el conductor (alambre) que lleva la señal está completamente rodeado por el conductor “ground” (llamado escudo o trenza). El cable coaxial provee un ambiente de alta velocidad y mínima distorsión para las señales.

CIRCUITO CONMUTADO.- Ruta DE transmisión dentro de una red conmutada (por ejemplo la red telefónica o un conmutador telefónico de una empresa) en la

que se crea una ruta cuando una estación origen especifica una de destino y esa ruta se mantiene por la duración de la llamada.

EIA.- Asociación de Industrias Electrónicas, es una asociación de manufactureros de equipo electrónico en los Estados Unidos que crea estándares.

FAST ETHERNET.- Una tecnología de redes con un amplio ancho de banda y que se basa en el estándar 802.3 Ethernet (100BASE–T); de 100 Mbps, diez veces más rápido que el Ethernet (10BASE–T).

FDDI.- Siglas de Fiber Distributed Dat Interface; un estándar de cables de fibra óptica.

FIBRA OPTICA.- un cable que utiliza frecuencias de luz como transmisor de datos; uno de los cables más rápidos y menos sensibles a interferencias electromagnéticas, pero también uno de los más caros.

HUB.- Dispositivo que ejerce de nodo central en redes en estrella; se puede utilizar en caso de administración central. Los nodos pueden aislarse contra colapsos.

IEEE.- The Institute of Electrical and Electronic Engineers: Una asociación profesional que define estándares y especificaciones.

IEEE802.- Estos son los estándares para la conexión física y eléctrica de LAN's desarrollado por IEEE.

IEEE802.3 10BASE2.- Esta especificación de la IEEE iguala el cableado estrecho de Ethernet. Este designa un rate de señal de 10 mbps, técnica de base de banda, y un máximo de distancia de 185 mteros.

LAN.- Red de área local. Se refiere a una red de computadoras conectadas bajo un mismo protocolo y tipo de conexión física, sin modulación de la señal y en distancias cortas (menores generalmente a los 10 Km.)

MAN.- Red de área metropolitana.

MODULACIÓN.- Proceso mediante el cual se sobreimpone una señal de datos a una señal portadora de manera que la información pueda ser transportada sobre un medio que normalmente es incompatible con la señal de datos. Por ejemplo, un módem convencional se usa para transmitir señales de datos sobre una línea telefónica que normalmente se usa para la transmisión de voz.

PAR TRENZADO.- Un cable popular y barato, que normalmente se utiliza en el cableado de teléfonos; utiliza un par de hilos trenzados el uno sobre el otro, que minimizan las interferencias eléctricas.

PROTOCOLO.- Este es el procedimiento (conjunto de pasos, mensajes y secuencias) que se utiliza para mover la información de una localización a otra sin errores.

STP.- Par trenzado apantallado mediante malla de cobre.

SERVIDOR.- Un dispositivo de red que ofrece servicios a un PC cliente; por ejemplo, acceso a ficheros, cola de impresión, o acceso remoto.

TOPOLOGÍA EN ANILLO.- Una configuración de los cables en una red, en la cual los distribuyen alrededor de un anillo formado por el medio de transmisión.

TOPOLOGÍA EN BUS.- Configuración física de una red, en la cual todos los sistemas están conectados a un cable principal; también se denomina bus lineal.

TOPOLOGÍA EN ESTRELLA.- Una configuración de cables para redes LAN, que normalmente utilizan un dispositivo central, a través del cual pasa toda la comunicación.

UTP.- Par trenzado no apantallado; se trata de un cable fino muy utilizado en la instalación de cables de redes.

WAN.- Red de área extensa.

HOJA DE VIDA

DATOS PERSONALES

APELLIDOS	**:**	Santamaría Pazmiño
NOMBRES	**:**	Shony Leonel
FECHA DE NACIMIENTO	**:**	13 de agosto de 1980
EDAD	**:**	22 años
ESTADO CIVIL	**:**	Soltero

ESTUDIOS REALIZADOS

PRIMARIOS	**:**	Escuela Juan Montalvo
SECUNDARIOS	**:**	Instituto Técnico Superior Guaranda
SUPERIORES	**:**	Instituto Tecnológico Superior Aeronáutico

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

CBOS. SANTAMARÍA PAZMIÑO SHONY LEONEL

_____

DIRECTOR DE LA ESCUELA DE TELEMÁTICA

Ing. Ramiro Yerovi

_____

Latacunga, 07 de marzo de 2003