Universidad Autónoma de Querétaro
Facultad de Informática

CARTA DE ACEPTACIÓN DE TESINA

Por este medio, se otorga constancia de aceptación de la tesina que para obtener el título de Licenciado en Informática, presenta la pasante **NORA CAROLINA MORENO SALAZAR**, con el tema denominado **"REDES LOCALES, RED NEW HOLAN DE MEXICO, S.A."**

Este trabajo fue desarrollado como una investigación derivada del curso de titulación **"REDES LOCALES",** dando cumplimiento a uno de los requisitos contemplados en el artículo 34 del reglamento de titulación vigente, en lo referente a la opción de titulación por realización y aprobación de cursos de actualización.

Se extiende la presente para los fines legales a que haya lugar y para su inclusión en todos los ejemplares impresos de la tesina, a los veinte días del mes de marzo de mil novecientos noventa y siete

A T E N T A M E N T E

Ing. Francisco Javier Martínez Mejía
Responsable de la Revisión y
Coordinador del Curso de Titulación Impartido

UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

FACULTAD DE INFORMÁTICA

REDES LOCALES

DOCUMENTACION DE LA RED DE LA EMPRESA:

TRACTORES NEW HOLAN DE MÉXICO S.A.

PRESENTA:

NORA CAROLINA MORENO SALAZAR

INDICE

INDICE

INTRODUCCIÓN

INTRODUCCION

La Empresa Tractores New Holan de México S. A. existe ya desde tiempos atrás, pero con otras Nombres de Razón Social, como lo han sido Masey Ferguson y FNT, en realidad la Razón Social de New Holan surgió en el año de 1993, cuatro años atrás fue FNT, y la Razón Social Fundadora fue Masey Ferguson.

Actualmente la Empresa se dedica al ensamble de las partes para su maquinaria, ya que las partes las proveen ya sea de Estados Unidos o Italia. Aunque en algunas ocasiones la Empresa realiza adaptaciones de algunas partes para sus Tractores.

Se tiene como objetivo, que en un futuro próximo se desarrollen también sus propias partes.

En cuanto a la Red de Computadoras con la que cuenta la empresa, se trata de Una Red tipo WAN (Red de Gran Alcance), ya que se encuentran conectados vía Routher a Estados Unidos e Italia con sus Proveedores. Pero el documento que se presenta a continuación sólo muestra lo referente a la Red de Área Local.

I. CONCEPTOS

SOBRE

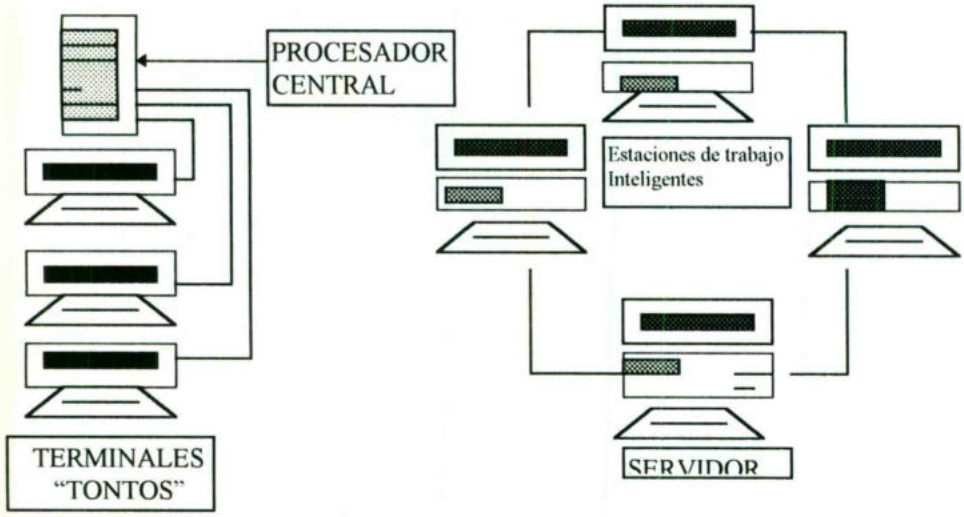
REDES

CONCEPTOS SOBRE REDES

En 1980, las microcomputadoras produjeron un cambio inmenso en el mundo de los negocios y de la industria, al darles a los usuarios acceso a recursos informáticos e información de la que no disponían anteriormente. La clásica máquina de escribir se vería sustituida tras más de 100 años de servicio por estos sistemas, a los cuales se les ha rebautizado adecuadamente como "computadoras personales".

En los años sesenta, los elementos de cálculo e información de toda una empresa se gestionaban desde un sistema con una computadora principal centralizada. Estos sistemas eran controlados de una forma estricta por unos departamentos de sistemas de información que distribuían su potencia de cálculo como tal o supervisaban su gestión desde un nivel superior. El precio del almacenamiento y procesamiento era alto, por lo que muchos usuarios no podían beneficiarse de estos sistemas. Pero cuando se hicieron disponibles las microcomputadoras esto cambió, al permitir que los departamentos pudieran poseer sus sistemas individuales por sólo una parte del coste de los sistemas centralizados.

Finalmente las computadoras personales ocasionarán un proceso similar dirigido a los puestos de trabajo de los usuarios. Sin embargo, la información que se encuentra en las computadoras personales no se puede compartir fácilmente, y es difícil de acceder. Además, la información de interés puede encontrarse diseminada entre varias computadoras, en lugar de estar integrada en el lugar central. Por ello, a mediados de los ochenta surgió una tendencia a volver a centralizar el almacenamiento de la información. Las computadoras personales se conectaban entre sí como ***redes*** de computadoras, y los archivos se almacenaban centralizados en sistemas de archivos que podían ser accedidos fácilmente por otros usuarios, tal y como se ve en la figura siguiente:



Sistemas centralizados (izquierda) y Sistemas en red (derecha).

Cuando se comparan redes frente a los sistemas centralizados de minis o grandes computadoras, se ha de tener en cuenta una característica en concreto. Una red está constituida por un conjunto de computadoras que acceden a los archivos y recursos de un ***servidor*** central, pero cada computadora ejecuta sus propios procesos. Un sistema con una mini o una gran computadora también centraliza el procesamiento, los terminales tontos dependen casi totalmente del sistema central para llevar a cabo el procesamiento, acceso a los archivos y otras actividades. Las redes se conocen como ***sistemas de proceso distribuido***, ya que cada sistema puede cargar y ejecutar programas en su propia memoria. Al no tener que ocuparse de realizar el procesamiento para los puestos de trabajo individuales, el servidor de archivos puede optimizarse para los servicios de archivo y red.

Las computadoras individuales en los sistemas distribuidos, denominados ***nodos*** o ***estaciones de trabajo*** no suponen una carga para el sistema central, ya que pueden ejecutar por sí mismas tanto tareas simples como complejas. *El servidor se utiliza* exclusivamente para controlar el almacenamiento y recuperación de información, las tareas de gestión de red, la gestión de usuarios y la seguridad. Cada uno de los PC se conecta al servidor para acceder a los programas, archivos y otros servicios de red como el correo electrónico.

RAZONES PARA INSTALAR UNA RED DE COMPUTADORAS.

¿Qué es una red? Una red es un sistema de comunicación que conecta computadoras y otros equipos de la misma forma que un sistema telefónico conecta teléfonos.

Las redes minimizan los problemas de distancia y comunicación, y les dan a los usuarios la posibilidad de acceder a información de cualquier punto de la red.

Las razones más usuales para instalar una red de computadoras son las que se listan a continuación :

Compartición de programas y archivos. Se pueden adquirir versiones para red de muchos paquetes de software muy populares, con un ahorro bastante considerable si se compara con su coste al comprar copias con licencia individual.

Compartición de los recursos de la red. Entre los recursos de la red se encuentran las impresoras, los trazadores, dispositivos de almacenamiento, e incluso otros sistemas informáticos como minis o grandes computadoras. Estos recursos informáticos se pueden compartir fácilmente mediante las redes.

Expansión económica de una base de PC. Las redes ofrecen una forma económica de expandir la informatización en la Organización utilizando puestos de trabajo de bajo coste sin discos, que utilicen el sistema de arranque del servidor en lugar de uno incorporado con el equipo. mediante la compartición de recursos, las impresoras y los otros dispositivos pueden ser utilizados por varios usuarios en lugar de sólo por los que utilicen los equipos a los que se encuentren directamente conectados.

Posibilidad de utilizar software de red. El software de gestión de bases de datos es el más utilizado en las redes; también es importante, sin embargo, el uso del correo electrónico.

Correo electrónico. Se utiliza para enviar mensajes o documentos a usuarios de la red. Los mensajes se dejan en "buzones", como lugar de almacenamiento en el que se leerán cuando convenga; puede haber alarmas que avisen al usuario de que tiene correo pendiente. Se pueden fijar citas y gestionar agendas.

Creación de grupos de trabajo. Los grupos de usuarios pueden trabajar en un departamento o ser asignados a un grupo de trabajo especial. Netware permite asignar a los grupos de usuarios directorios especiales y recursos que no serán accesibles a los restantes usuarios. Los mensajes y el correo electrónico podrán ser enviados a todos los miembros del grupo mediante el nombre del grupo.

Gestión centralizada. Debido a que la mayoría de los recursos de una red se encuentran organizados alrededor del servidor, su gestión resulta fácil. Las copias de seguridad y la optimización del sistema de archivos se pueden llevar a cabo desde un único lugar.

Seguridad. Netware ofrece elementos de seguridad avanzados que aseguran que los archivos van a estar protegidos de usuarios sin autorización. Los responsables pueden evitar que los usuarios trabajen fuera de unos directorios asignados, pudiendo aplicar también restricciones en la conexión.

Acceso a otros Sistemas Operativos. Netware 386 de Novell permite conectar los puestos de trabajo con sistemas de computadoras que utilicen sistemas operativos distintos.

Mejoras en la organización de la empresa. Las redes pueden suponer un cambio en la estructura administrativa más importante de la organización al estimular modos de trabajo en grupo según las cuales los departamentos sólo existen a nivel lógico dentro de una gestión computerizada y de una estructura de directorios.

COMPONENTES DE UNA RED.

Una red de computadoras está compuesta tanto por el *hardware* como por el *Software*.

Una red básica está compuesta por el siguiente Hardware:

* **Servidor**. Ejecuta el Sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo. Entre estos servicios se incluyen el almacenamiento de archivos, la gestión de usuarios, la seguridad, las órdenes de red generales, las órdenes del responsable de la red, y otros.

* **Estaciones de trabajo**. Cuando una computadora se conecta a una red la primera se convierte en un nodo de la última, y se puede tratar como una estación de trabajo. Pueden ser computadoras personales con el DOS, Sistemas Macintosh de apple, sistemas con el OS/2 o estaciones de trabajo sin disco.

* **Placas de interfaz de red (NIC).** La interfaz puede venir incorporada a cada computadora, en la mayor parte de los casos ha de añadirse como un monto opcional. La placa de interfaz de Red (NIC = Network Interface Card) ha de corresponder al tipo de red que se está utilizando. El cable de la red se conectará a la parte trasera de la placa.

* **Sistema de cableado**. Está constituido por el cable utilizado para conectar entre sí el servidor y las estaciones de trabajo. El cable puede ser ***Coaxial*** (similar al que se utiliza como cable de televisión) o de ***Par trenzado*** (como el que se utiliza en las instalaciones telefónicas). También se puede utilizar el cable de ***Fibra óptica*** de alta velocidad, el cual se utiliza para conectar distintas redes a gran distancia o en situaciones especiales con mucho tráfico de datos.

* **Recursos compartidos y periféricos**. Se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de disco óptico, las impresoras, los trazadores, y el resto de equipos que puedan ser utilizados por cualquiera en la red.

REALIZACIÓN DE CONEXIONES EN LA RED.

Las conexiones a la red se llevan a cabo con el cable o medio usado sobre las placas de interfaz de red para todos los PC y el Servidor. La arquitectura de la red viene definida por el sistema de cableado, además por las reglas y métodos utilizados para acceder al cable.

Placas de Interfaz de Red (NIC).

Los tres tipos más usuales de red son *ARCNET*, *Ethernet* y *Token Ring*. Las decisiones del uso de un tipo de red en la actualidad se toman en función del coste, distancia de cableado y topología. **Una topología puede incluir trenzados de cable lineales, circulares o en forma de estrella**.

Medios de transmisión de una Red.

El medio de transmisión de una red consiste en el cable que se utiliza para conectar la red. El cable Coaxial fue uno de los primeros tipos que se usaron, pero el Par trenzado ha ido ganando popularidad. El cable de fibra óptica se comienza a usar en las redes de computadoras. Los cables a usar en una red se evalúan según diversos parámetros:

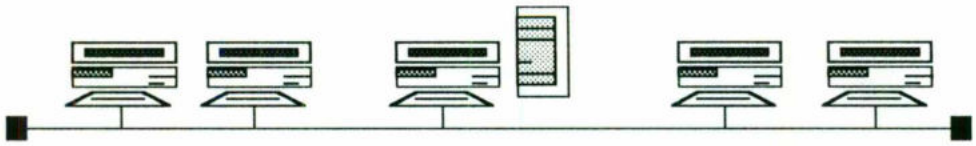
* La velocidad de transmisión, o tasa de trasferencia de información.
* La longitud de cable máxima sin necesidad de un amplificador.
* Las necesidades de apantallamiento.
* El precio.

Arquitectura de una red.

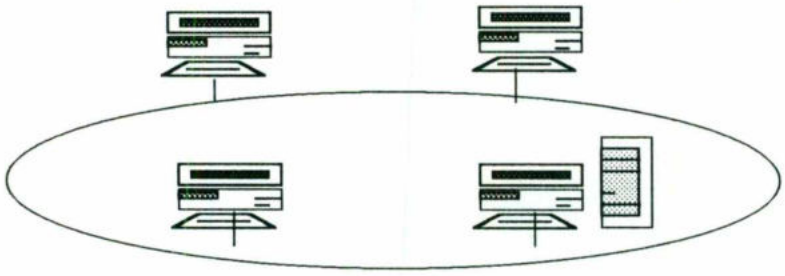
Define la estructura del sistema de cableado y de estaciones de trabajo conectadas a éste, además de las reglas utilizadas para transferir señales de una estación de trabajo a otra. La estructura física del sistema de cableado se denomina topología de la red.

Topología.

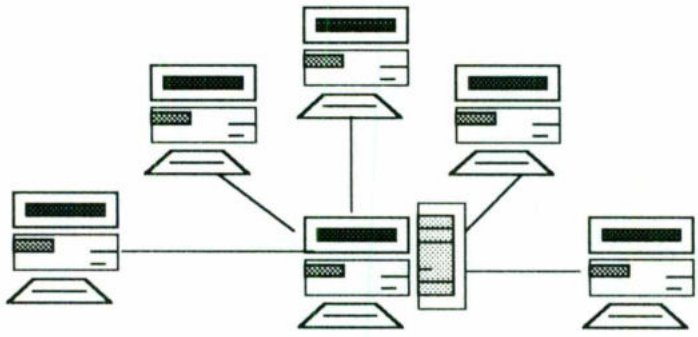
La topología de una red es la descripción de cómo va el cable de un nodo a otro. Es fácil verlo como un "plano" del sistema de cableado. La figura siguiente muestra las topologías según una descripción simple y general:



Topología lineal o en Bus. Ejem. Ethernet (Punto a punto).



Topología en anillo. Ejem. Token Ring (Multipunto).



Topología en estrella. Multipunto.

Método de acceso al cableado.

El ***Método de acceso al cableado*** muestra cómo un nodo accede a un sistema de cableado. Los sistemas de cableado lineales pueden utilizar un método de detección de portadora, mientras que los sistemas en anillo o estrella pueden utilizar un método de pase de testigo. Una vez que la placa accede al cable, comienza a enviar paquetes de información a otros nodos. Al adquirir una placa de interfaz de red, se adquiere para utilizarla en una topología y utilizando un método de acceso al cableado específicos. A continuación se describen los ***métodos de acceso al cableado***

:

Detección de portadora. Se utiliza fundamentalmente en los sistemas de cableado lineales. Antes de comenzar a transmitir, un nodo comprueba si el cable está siendo usado. Transmite como la difusión por radio a través de todo el cable; todos los nodos lo escuchan y determinan si la transmisión está destinada a ellos. Si no lo está, la rechazan. Si dos nodos emiten a la vez, se produce una colisión anulándose ambas emisiones los nodos esperan un cierto tiempo aleatorio, y lo vuelven a intentar.

Pase de testigo. Se utiliza normalmente con las redes en anillo, o las que se comportan como anillos. El concepto de "testigo" se utiliza para definir cómo una estación de trabajo puede acceder al cable. Cuando una estación de trabajo está preparada para trasmitir, debe esperar a que esté disponible un testigo, y tomar posesión de él.

Cada estación de trabajo examina la dirección del paquete para determinar si está dirigido a él. Si no lo estuviera, pasa el paquete a su vecino o próxima estación en la red. Pueden transmitirse cientos o miles de paquetes por segundo.

Protocolos de comunicación.

Son las reglas y procedimientos utilizados en una red para establecer la comunicación entre nodos. En los protocolos se definen distintos niveles de comunicación. Las reglas de nivel más alto definen cómo se comunican las aplicaciones, mientras que las reglas de nivel más bajo definen cómo se transmiten las señales por el cable.

Cobertura de las redes.

Niveles de interconexión.

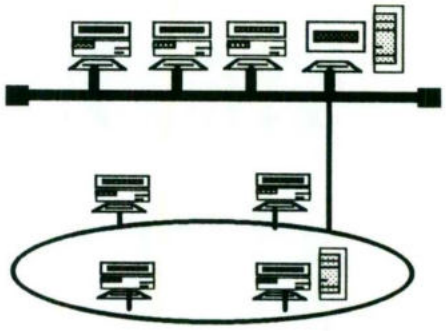
Red de área local (LAN). Una pequeña red (de 3 a 50 nodos) normalmente localizada en un solo edificio o grupo de edificios pertenecientes a una organización.

Redes interconectadas (Internetwork). Se pueden conectar dos o más redes para formar un sistema en red que cubra toda una empresa. También puede dividirse una red extensa en varias redes más pequeñas para optimizar el rendimiento y la gestión.

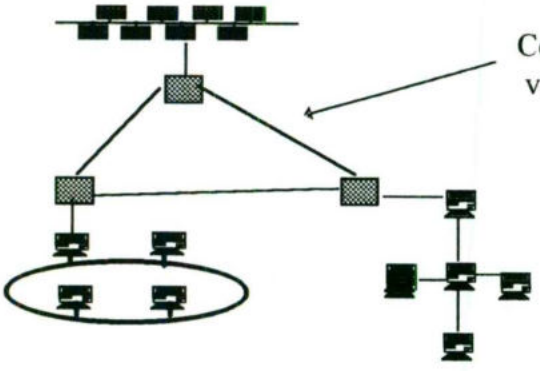
Red metropolitana (MAN). Se trata de un conjunto de redes de área local interconectadas dentro de un área específica, como un campus, un polígono industrial o una ciudad. Se ha de utilizar una base de cableado o sistemas de conexión especiales a alta velocidad, como una compañía telefónica, para conectar las redes en un sistema interconectado.

Red de gran alcance (WAN). Se trata de una red que cubre diversos países o incluso el mundo.

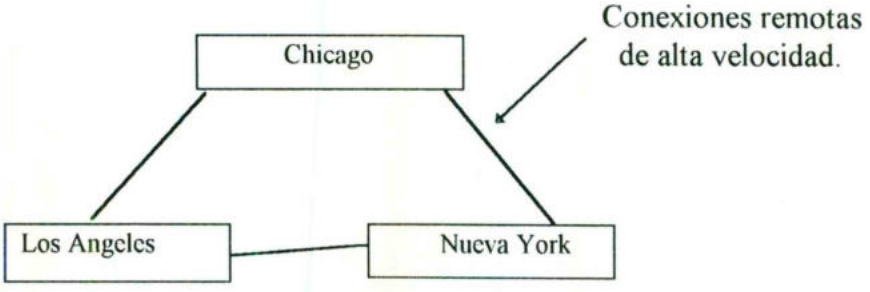
Red de área local (Lan)



Redes interconectadas



Red metropolitana (MAN)



Red de gran alcance (WAN).

Tipos de redes.

Características de los Sistemas Operativos de Red.

Servicios de archivos y directorios. En una red, los usuarios acceden a programas y archivos que se encuentran en el servidor de archivos central.

Sistema tolerante a fallos. Los sistemas operativos de red avanzados deben de ofrecer un sistema para asegurar la supervivencia de la red en el caso de que fallen los componentes.

Disk Caching (Optimización de acceso a disco). La optimización de acceso a disco mejora el rendimiento del disco fijo utilizando una parte de la memoria del sistema como una zona en la que almacenar bloques del disco a los que se puede acceder de nuevo. El obtener esta información de la memoria es mucho más rápido que el leerla del disco fijo.

Sistema de control de transacciones (TTS = Transaction tracking System). Una transacción es un cambio en un registro o conjunto de registros de un archivo de base de datos.

Seguridad. Las redes permiten a los usuarios almacenar sus archivos en lugar centralizado, en lugar de hacerlo en sus discos fijos o flexibles personales. Debido a esto, la seguridad de sistemas de archivos se convierte en un tema importante a tener en cuenta en el sistema operativo de red.

Compartición de recursos. Un recurso puede ser una impresora, trazador, sistema de copia de seguridad o cualquier otro dispositivo que necesiten utilizar muchos usuarios.

Acceso remoto. Puede que las redes necesiten conectarse con estaciones de trabajo u otras redes locales en puntos remotos.

Bridges (Puentes). Estos permiten que las redes se puedan interconectar con otras redes.

Gateways (Pasarelas). Los gateways permiten interconectar sistemas con distintos protocolos.

Interoperatividad. Es una tendencia en la industria de redes que permite que diversos tipos de sistemas operativos y productos de distintos fabricantes compartan provisional de interoperatividad hasta que no se pongan en uso los protocolos del modelo OSI más estandarizados.

Servidores especiales. Un sistema operativo de red puede permitir servidores especiales, como los dedicados a gestionar una base de datos o la impresión.

Herramientas de administración de software. Se hacen esenciales cuando crece el tamaño de las redes. Sin estas, puede llegar a ser imposible el hacer un seguimiento de las actividades y el rendimiento de las MAN y las WAN. Una solución es agrupar los responsables y darles herramientas para gestionar de forma remota los servidores y las estaciones de trabajo.

CABLEADO DE LA RED

El cable utilizado para conectar redes se denomina a menudo medio de la red. Podemos clasificar los tipos de cables basándonos en estos tres factores:

* Velocidad de transmisión.
* Longitud máxima
* protección contra interferencias.

Los tres tipos de cable más populares son:

PAR TRENZADO.

El par trenzado son dos hilos conductores de cobre aislados y trenzados entre sí, y en la mayoría de los casos, cubiertos por una malla protectora. Reduce las interferencias eléctricas. La mayoría del cableado telefónico utiliza par trenzado, y recientemente a comenzado a poder utilizarse como medio de conexión para redes. Aunque el par trenzado presenta una baja velocidad de transmisión y una longitud limitada para redes, debemos considerarlo por las siguientes razones:

* El par trenzado de encuentra ya instalado en muchos edificios como cable telefónico. Una manguera de éste cable contiene generalmente pares no utilizados, que pueden emplearse para el cableado de redes. Y, lo más importante, generalmente este cable se ramifica desde una caja de registro centralizada hacia las estaciones de trabajo. Esta caja de registro puede convertirse en el centro de cableado de la red.

* Aunque anteriormente la velocidad de transmisión de par trenzado era baja, los últimos avances tecnológicos en placas de red han permitido incrementar su velocidad, haciendo del par trenzado una solución viable para montar redes.

* El par trenzado resulta fácil de combinar con otros tipos de cable para formar redes extendidas. Por ejemplo, las cajas de conexión de dos departamentos separados pueden unirse mediante un cable coaxial largo, obteniendo dos redes enlazadas.

CABLE COAXIAL.

Se utiliza generalmente para señales de televisión. Consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa está rodeada de una malla metálica que ayuda a bloquear las interferencias. El conjunto está envuelto por una capa protectora. Algunas normas de construcción requieren que este cable sea ignífugo cuando se utiliza en espacios cerrados. Al quemarse, el cable de este tipo no produce gases tóxicos que podrían expandirse por el sistema de ventilación de un edificio.

La velocidad de transmisión puede ser alta, peor cuando mayor sea la velocidad, menor será la distancia posible por cubrir. Aunque el cable ARCNET ofrece una baja velocidad de transmisión, permite cubrir mayores distancias que Ethernet. Existen diversos tipos de cable coaxial, que puede ser grueso o fino. Los tramos largos de una red pueden implementarse con cable grueso; sin embargo, es más caro que el cable fino, que permite cubrir distancias menores.

CABLE DE FIBRA ÓPTICA.

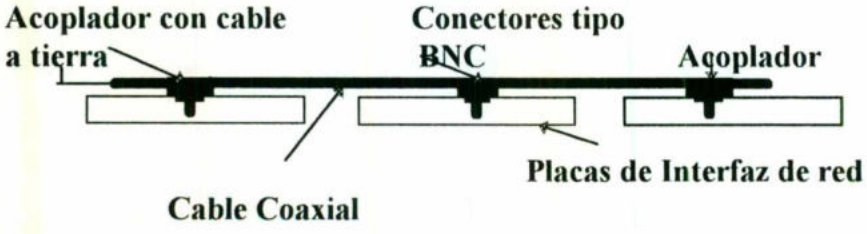
Transmite señales de datos mediante luz. La luz modulada pasa por un conductor de vidrio, rodeado por una capa reflectante. este conjunto envuelto por una capa protectora. La velocidad de transmisión de éstas redes se encuentran en el rango de los 100 Mbits por segundo, pero algunas aplicaciones especiales se alcanzan velocidades de hasta 500 Mbits por segundo. El cable de fibra óptica no resulta afectado por las interferencias, y no puede ser "pinchado", lo cual resulta útil en situaciones de gran confidencialidad.

TIPOS DE REDES.

REDES ETHERNET.

Una red local Ethernet utiliza una topología lineal (en bus) que consiste generalmente en un tramo de cable coaxial. Se utiliza un método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Tiene una velocidad de transmisión de 10 Mbtis por segundo.

En Ethernet se utilizan dos tipos de cable coaxial: grueso y fino. Aunque el cable fino es más manejable y accesible que el grueso, su longitud máxima es de 185 metros (607 pies). El cable grueso permite tramos mayores, de hasta 500 metros (1640 pies).

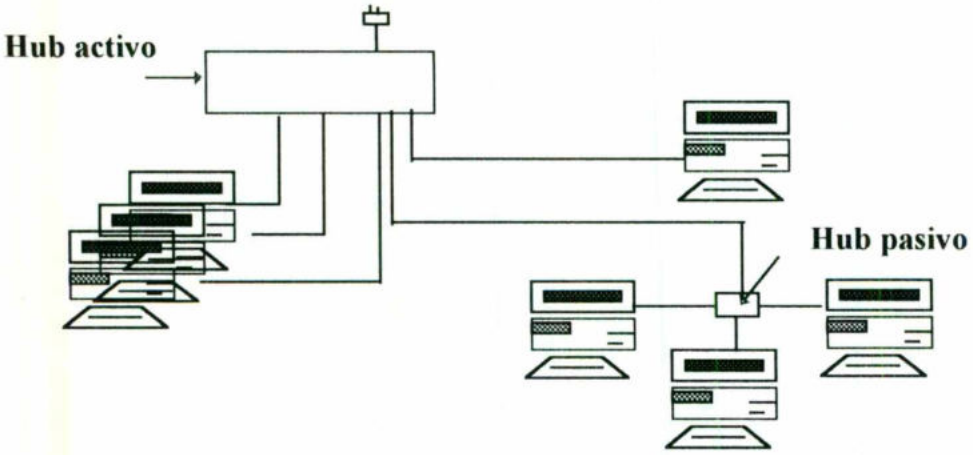


Configuración Ethernet con cable fino.

REDES ARCNET.

Generalmente utilizan cable Coaxial, pero la mayoría de placas de red actuales permiten usar par trenzado, que representa una solución más práctica para distancias cortas. Utilizan pase de testigo con una topología en bus, pero utilizan Hubs para distribuir las estaciones de trabajo en una configuración de estrella.

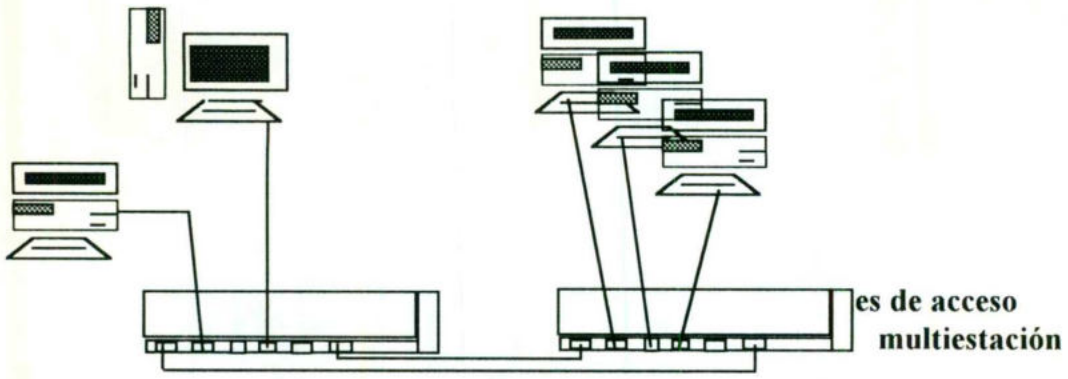
Para distribuir las estaciones de trabajo desde un punto central se utilizan hubs activos y pasivos. Un hub activo permite conectar a distancias de hasta 609 metros (2000 pies), mientras que uno pasivo permite tramos de hasta 30 metros (100 pies).



Configuración ARCNET.

REDES DE TOKEN RING

Utilizan un método de acceso por pase de testigo en una topología de anillo. Sin embargo, puede tomar el aspecto de una topología de estrella, ya que se pueden conectar estaciones en un dispositivo central o unidad de acceso multiestación (MAU).



Cables de conexión para mantener el bucle

Configuración Token Ring.

II. INSTALACION DEL

HARDWARE

DE LA RED

INSTALACIÓN DEL HARDWARE DE LA RED.

Para instalar y configurar una tarjeta de red en su computadora necesitará:

1. Comprobar que posee el hardware necesario, tal como la tarjeta de red, cables, conectores y otros elementos necesarios durante la instalación.

2. Configurar la tarjeta de red para que funcione con su computadora.

3. Insertar la tarjeta de red en su computadora.

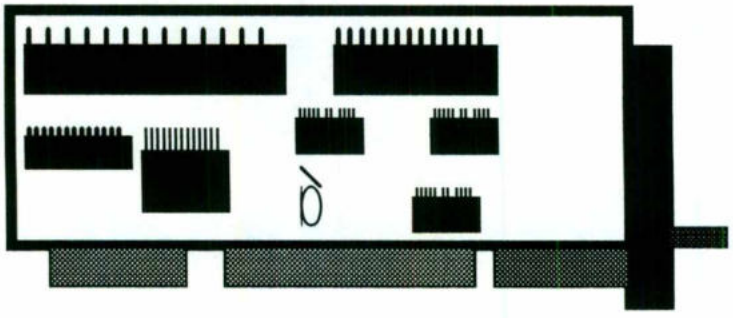
NOTA: En algunos casos, tendrá que insertar la tarjeta en su computadora antes de llevar a cabo el paso 2, Configuración de la tarjeta.

4. Conectar cables a la tarjeta de red y, a continuación, conectarse con las demás computadoras de su red.

1. MATERIAL NECESARIO.

Antes de comenzar, asegúrese de contar con los elementos siguientes:

Una Tarjeta de red.



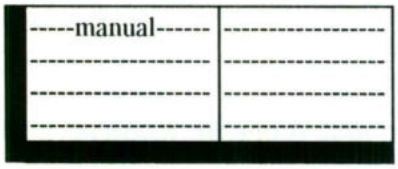
Además, asegúrese de que su tarjeta de red es compatible con el tipo de ranuras del bus de expansión que utiliza su computadora. Se trata de zócalos que se encuentran en el interior de su computadora, en los que puede insertar la tarjeta. La tabla siguiente muestra los tipos de ranuras utilizados en algunos tipos de computadoras habituales.

Tipo de ranuras del bus de expansión	Tipo de computadora
0ISA	IBM PC/AT y la mayoría de las compatibles.
EISA	Algunas compatibles PC/AT más potentes.
MCA	IBM PS/2 (la mayoría de los modelos).

Si no sabe que tipo de ranura utiliza su computadora, consulte el manual o la documentación de su computadora.

Los discos de Software, en caso de que su tarjeta de red los incluya.

Los manuales o documentación que acompañe al hardware de su sistema (computadora, tarjeta de red, cables y demás dispositivos que tenga instalados).



Cables, conectores, terminadores y demás hardware de conexión compatibles con la tarjeta de red. Consulte los requisitos de cableado de su tarjeta en el embalaje o la documentación de la tarjeta de red.

Un destornillador (para quitar la cubierta de su computadora y las placas de protección de las ranuras que se encuentran en su interior).

Configuración antes de insertar la tarjeta en su computadora.

En algunas tarjetas, tendrá que mover puentes o configurar modificadores manualmente antes de insertarla en su computadora.

Antes de insertar una tarjeta de red en su computadora, consulte la documentación que la acompaña para averiguar si es necesario configurar puentes o modificadores.

Configuración después de insertar la tarjeta en su computadora.

En el caso de las tarjetas MCA, la mayoría de las EISA y algunas ISA, deberá configurar la tarjeta ejecutando un programa de configuración después de insertarla en su computadora.

Uso de puentes y modificadores para configurar una tarjeta de red.

Si su tarjeta de red se configura manualmente (y no mediante programa de configuración), deberá establecer algunas opciones mediante puentes y modificadores DIP.

Modificación de la configuración mediante puentes.

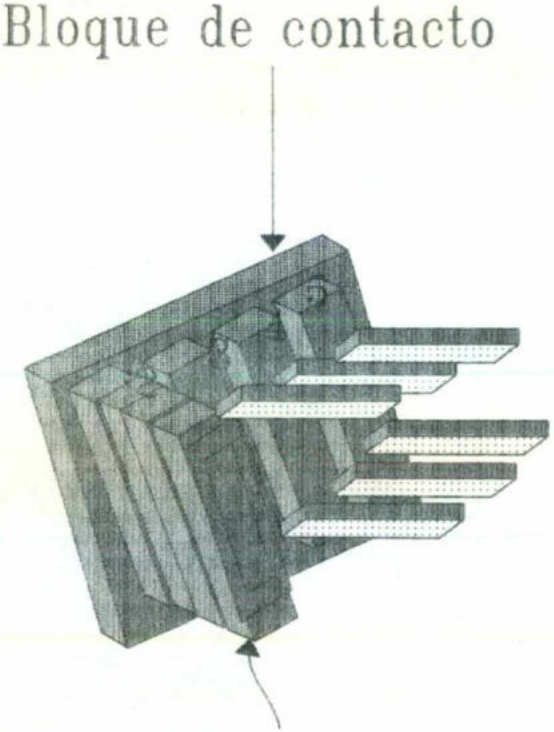
Para modificar una configuración mediante un puente, retire la pieza de plástico que encaja en las patillas del *bloque de puentes.* A continuación coloque la pieza de plástico en la patillas según las indicaciones de la documentación de su tarjeta de red. La ilustración 1.1 muestra el cambio de la configuración mediante puentes, desde la posición 2 a la 5, en un bloque de puentes de ejemplo.

Modificación de la configuración mediante modificadores DIP.

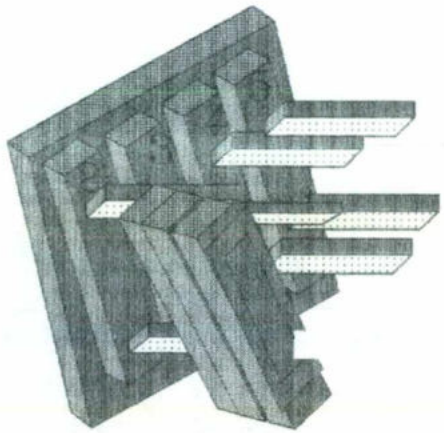
Los modificadores DIP se asemejan a modificadores de la luz en miniatura y funcionan de forma muy parecida. Para restablecer la configuración de su tarjeta de red mediante modificadores DIP, mueva los modificadores a la posición alternativa (On / Off u Open / Close) de acuerdo con la configuración que se indica en la documentación de su tarjeta de red.

Sugerencia: Puede usa un bolígrafo para cambiar fácilmente la configuración de los modificadores DIP.

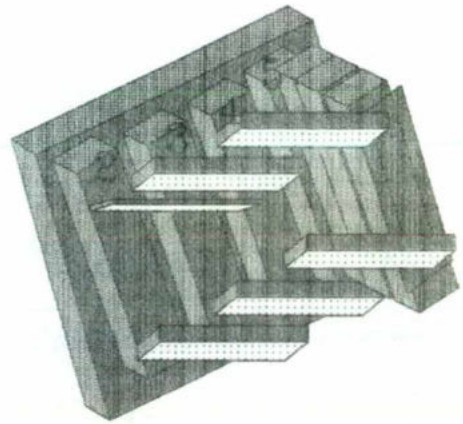
La ilustración 1.2 muestra dos tipos comunes de modificadores DIP.



Puente confugurado
en la posición 2



Pieza de plástico que
se está retirando



El puente se ha
colocado
en la posición 5

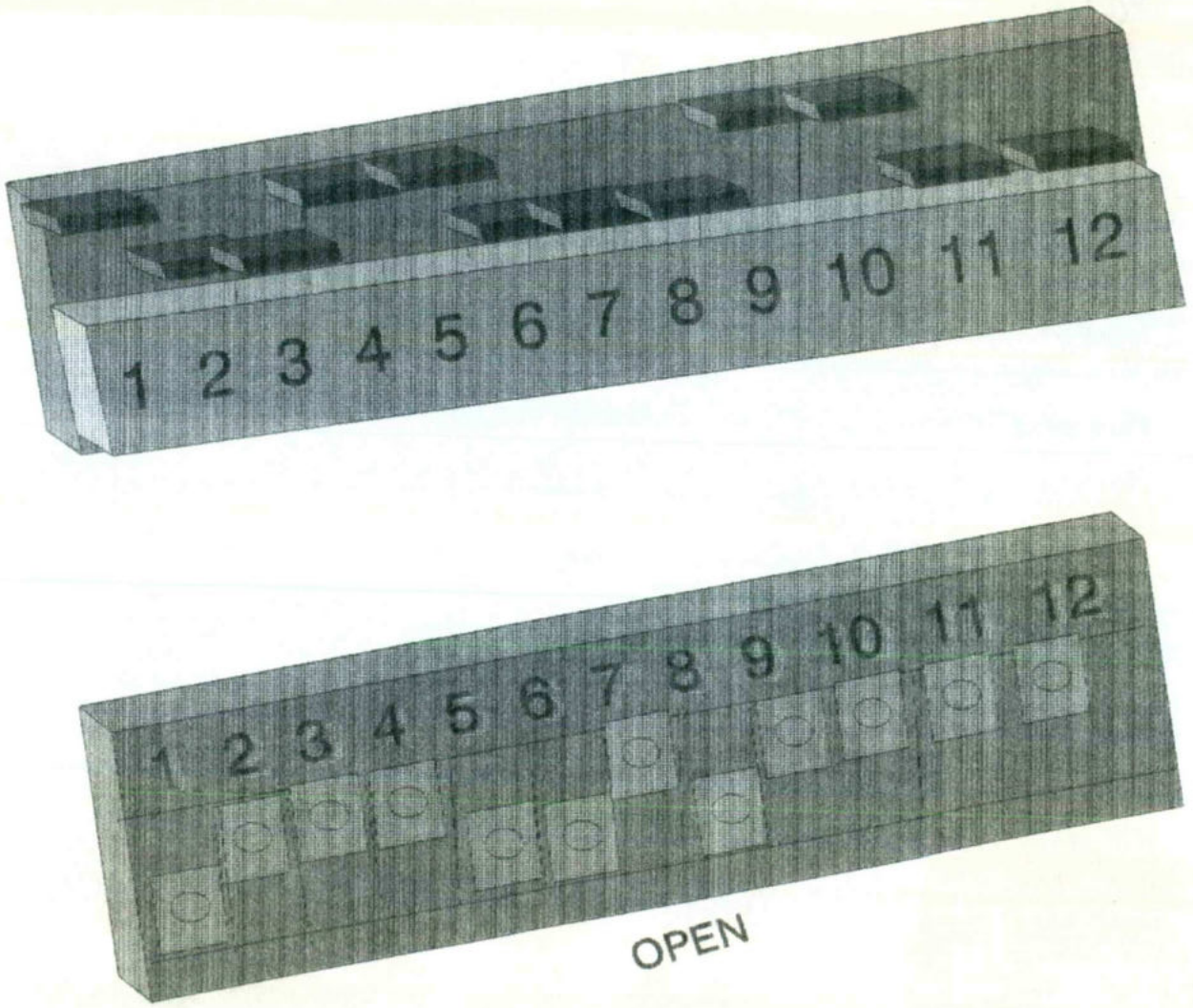


Ilustración 1.2. Tipos comunes de modificadores DIP

Determinación de los valores de configuración.

Distintas tarjetas de red requieren distintos tipos de configuración. En la mayoría de las tarjetas, deberá asignar un valor al menos a dos de las tres configuraciones que se describen en esta sección: Nivel de petición de interrupción (IRQ), dirección base del puerto de E/S (entrada/salida) y dirección base de memoria.

Para ver una lista completa de las configuraciones necesarias, consulte la documentación de su tarjeta de red.

Registro de la configuración de su tarjeta de red.

La tabla siguiente muestra algunas configuraciones comunes de determinado hardware. Utilícela para registrar los valores utilizados para configurar su tarjeta de red.

Si conoce la configuración del resto del hardware, puede serle útil realizar una lista de dicha información antes de configurar la tarjeta de red. Esto le ayudará a evitar utilizar los mismos valores para más de un dispositivo. La lista de estos valores de configuración puede encontrarse en la documentación que acompaña a su computadora y demás dispositivos.

Hardware	**IRQ**	**Dirección base del puerto de E/S.**
Puerto en serie (COM1, COM3)	4	3F8.
Segundo puerto en serie(COM1, COM4)	3	2F8
Controlador de unidad de Disquetes	6	3F0
Controlador de disco duro	14	1F0
LPT1	7	378
LPT2	5	278
Bus del Mouse	3, 4 ó 12	230
Módem		
Tarjeta de sonido		
Tarjeta de red		

Nivel de petición de interrupción (IRQ).

Cuando la tarjeta de red envía una petición a la unidad central de proceso (CPU) de su computadora, utiliza una señal electrónica denominada **interrupción.** Cada dispositivo de su sistema debe utilizar un *nivel de petición de interrupción* (IRQ) diferente, que se especifica durante la configuración del dispositivo (a menudo de utilizan indistintamente los términos de interrupción e IRQ). En la mayoría de los casos podrá utilizar la IRQ5, IRQ10, IRQ11 o IRQ15 para su tarjeta de red.

Compruebe si dichos niveles de interrupción ya se están utilizando, consultando la documentación que acompaña a su computadora y demás dispositivos. Si no está disponible la IRQ5, ni la IRQ10, ni la IRQ11, ni la IRQ15, busque en la tabla siguiente los valores alternativos que puede utilizar. Los niveles de interrupción que se mencionan como "disponible" pueden utilizarse habitualmente para la tarjeta de red.

Si su computadora no tiene el hardware citado junto a una IRQ concreta, dicha IRQ también debería estar disponible.

IRQ	Computadora con procesador 386SX (o superior)
2 (9)	No utilizar (reservado para el adaptador EGA/VGA).
3	Habitualmente no disponible (reservado para COM2 o COM4, a no ser que sólo haya un puerto serie instalado utilizado a veces por el bus del Mouse (ratón).
4	No utilizar (reservado para COM1 o COM3).
5	Disponible (excepto si se utiliza para un segundo puerto paralelo (LPT2) o bus del Mouse.
6	No utilizar (reservado para el controlador de unidad de disquete)
7	No utilizar (reservado para el puerto paralelo LPT1)
8	No utilizar (reservado para el reloj en tiempo real)
10	Disponible
11	Habitualmente disponible (salvo que se utilice para el controlador SCSI).

12 Habitualmente disponible (salvo que se utilice para un Mouse del tipo PS/2).

13 No utilizar (reservado para el procesador matemático).

14 No utilizar (reservado para el controlador de disco duro).

15 Disponible.

Dirección base del puerto de E/S.

La dirección base del puerto E/S (Entrada/salida) especifica un canal a través del cual se transfiere la información entre el hardware (como por ejemplo la tarjeta de red) y la CPU de su computadora. Para la CPU, el puerto aparece como una dirección.

Cada dispositivo hardware incluido en sus sistema posee una dirección de puerto de E/S diferente. Habitualmente, los números de puerto (en formato hexadecimal) que aparecen en la tabla siguiente están disponibles para asignarles su tarjeta de red. Las direcciones que se presentan a su lado un dispositivo suelen utilizarse para los dispositivos citados. Para determinar qué direcciones se están utilizando, consulte la documentación que acompaña a su computadora y demás dispositivos.

Puerto	Dispositivo	Puerto	Dispositivo
200 a 20F	Puerto de juegos	300 a 30F	Algunos controladores de disco
210 a 21F		310 a 31F	
220 a 22F		320 a 32F	Controlador de disco duro (sólo en el modelo PS/230).
230 a 23F	Bus del Mouse	330 a 33F	Controladores SCSI
240 A 24F		340 a 34F	
250 a 25F		350 a 35F	
260 a 26F		360 36F	
270 a 27F	LPT2(LPT3) comp. MCA	370 A 37F	LPT1(LPT2 en las comp. del tipo MCA
280 a 28F		380 a 38F	
290 a 29F		390 a 39F	
2A0 a 2AF		3A0 a 3AF	
2B0 a 2BF		3B0 a 3BF	LPT1 (sólo en la comp. del tipo MCA).
2C0 a 2CF		3C0 a 3CF	EGA/VGA
2D0 a 2DF		3D0 a 3DF	CGA(también EGA/VGA en los

modos de video de color).

2E0 a 2EF	COM1	3E0 a 3EF	COM3
2F0 a 2FF	COM2	3F0 a 3FF	Controlador de unidad de disquetes; COM1.

Dirección base de memoria.

Define la dirección de memoria de su computadora (RAM) que utilizará la tarjeta de red para intercambiar información entre su computadora y las demás computadoras conectadas con ella. Este valor se denomina a veces *dirección inicio de RAM.* A menudo, la dirección base de memoria para su tarjeta de red será D0000 (en algunas tarjetas de red desaparece el "0" final de la dirección, por ejemplo, D000).

NOTA: Algunas tarjetas no necesitan el valor de dirección base de memoria, ya que no utilizan RAM.

En algunas tarjetas de red, tal vez necesite especificar también la cantidad de memoria que se va a "correlacionar" o reservar para éste propósito. Por ejemplo, para algunas tarjetas puede especificar 16K - dejando más memoria libre para otros usos- o 32K, con lo que se consigue un mejor rendimiento pero se deja menos memoria disponible.

NOTA: Si utiliza EMM386, deberá excluir la dirección base de memoria utilizando el parámetro X= en la línea device=emm386 de su archivo CONFIG.SYS. Por ejemplo, si su tarjeta de red utiliza la dirección C800, la línea device = emm386 de su archivo CONFIG.SYS deberá ser similar a ésta:

```
device=emm386.exe x=c800-ceff
```

Valores adicionales.

Durante la configuración de su tarjeta de red, es posible que necesite definir otros valores. Por ejemplo, algunas tarjetas tienen más de un conector (el lugar donde se conecta el cable), lo que les añade flexibilidad a la hora de elegir un cable. Si su tarjeta tiene múltiples conectores, probablemente deberá especificar cuál utilizar. Esto se consigue bien mediante un puente o mediante la configuración por software. Consulte los detalles sobre éste y otros valores en la documentación que acompaña a su tarjeta de red.

3. Instalación de la tarjeta de Red.

Esta sección describe el procedimiento que debe seguir para insertar la tarjeta de red en su computadora.

Antes de insertar la tarjeta.

Antes de insertar su tarjeta de red en su computadora, efectúe los pasos siguientes:

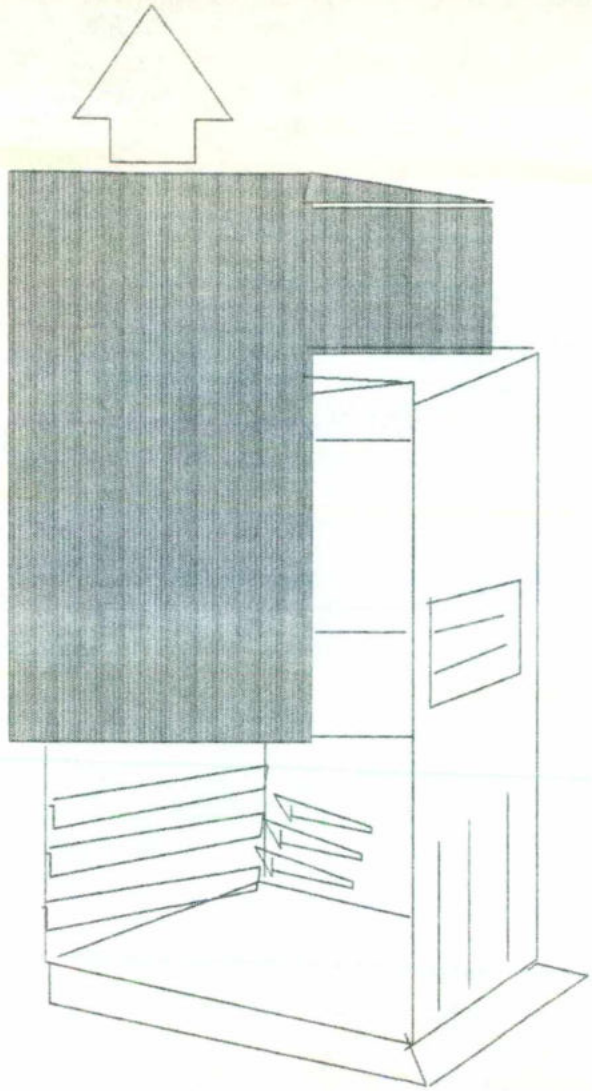
Atención. Apague y desenchufe siempre su computadora antes de retirar la cubierta.

•Antes de insertar la tarjeta en su computadora

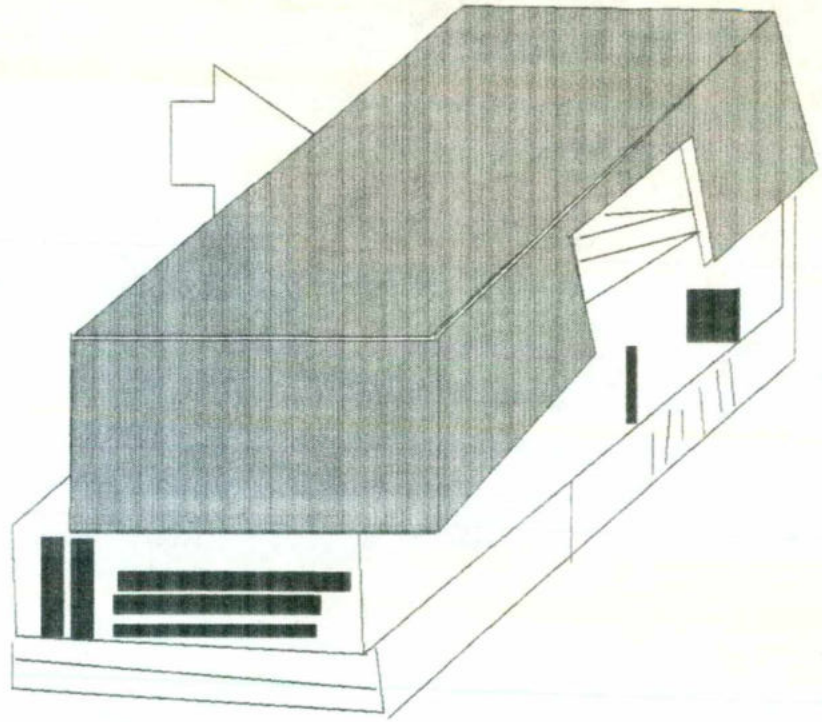
1. Salga de Windows y de todos los programas que esté ejecutando.

2. Apague su computadora y desenchufe todos los cables de alimentación.
3. Retire la cubierta de la unidad de sistema de su computadora.

Habitualmente, los tornillos que se sujetan se encuentran en la parte posterior y/o a los lados de su computadora. Generalmente sólo hay que quitar tres o cuatro tornillos. La cubierta puede deslizarse hacia atrás o hacia adelante o tal vez tenga que levantarla. Como lo muestra la Ilustración 3.1.



COMPUTADORA TIPO TORRE



COMPUTADORA TIPO ESCRITORIO

Ilustración 3.1 Retirar cubierta de la unidad de sistema de su computadora.

4. Si necesita modificar las configuraciones de puentes o de modificadores DIP en su tarjeta de red, hágalo antes de insertar la tarjeta en su computadora (si no sabe si es necesario, consulte la instalación).

NOTA: Antes de tocar la tarjeta, asegúrese de descargar sus manos de electricidad estática tocando una superficie de metal que esté conectada a tierra, como por ejemplo el tornillo de la cubierta de un enchufe eléctrico.

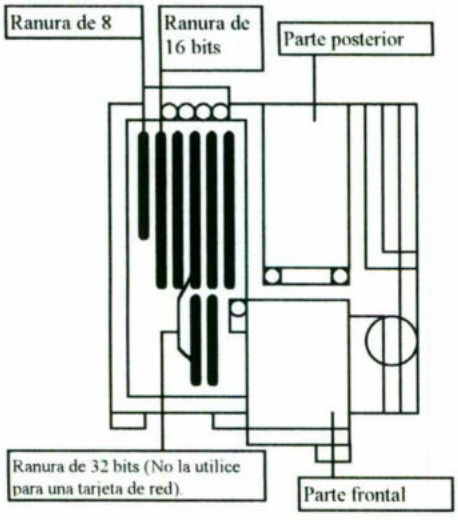
Inserción de la tarjeta en su computadora.

Una vez que haya apagado su computadora y retirado la cubierta, puede insertar la tarjeta de red.

•Para insertar una tarjeta de red en su computadora.

1. Localice una ranura del Bus de expansión que no esté utilizando en el interior de su computadora. Asegúrese de que esta ranura es la adecuada para la tarjeta (para obtener mas información al respecto, consulte la documentación de su tarjeta). Las tarjetas ISA suelen utilizar ranuras de 8 bits o de 16 bits. Si hay alguna ranura de 16 bits libre, utilícela, pues le dará mejor rendimiento. Las tarjetas EISA y MCA suelen utilizar una ranura de 32 bits.

En la ilustración siguiente, que muestra una computadora vista desde arriba, se ve el aspecto que pueden presentar las ranuras de su computadora, aunque también pueden ser distintas, especialmente si su computadora es del tipo EISA o MCA.



2. Retire la cubierta de protección de la ranura y guarde el tornillo para utilizarlo en el paso 7. Ver ilustración 3.2.

3. Descargue la electricidad estática de sus manos tocando una superficie de metal conectada a tierra, como por ejemplo el tornillo de la cubierta de un enchufe eléctrico.

4. Saque la tarjeta de red de su envoltorio protector. tenga cuidado de no tocar los contactos de oro que se encuentran en la parte inferior de la tarjeta.

5. Alinee el fondo de la tarjeta (los contactos de oro) con la ranura e insértela en el zócalo presionando fuertemente. Si se instala la tarjeta correctamente, quedará automáticamente bloqueada. Ver la ilustración 3.3.

6. Asegúrese de que el borde superior de la tarjeta está nivelado (no inclinado) y de que el agujero situado en la parte superior de la escuadra de metal de la tarjeta queda alineado con el agujero roscado de la parte posterior de la ranura.

7. Sujete la tarjeta en su sitio mediante el tornillo que retiró en el paso 2. Ver ilustración 3.4.

8. Coloque de nuevo la cubierta de su computadora y los tornillos.

9. Conecte de nuevo todos los cables que desenchufó anteriormente.

Tarjetas configuradas mediante software.

Si su tarjeta de red se configura mediante un programa de configuración (como ocurre con las tarjetas MCA, la mayoría de las tarjetas EISA y algunas tarjetas ISA), siga las instrucciones que se indican a continuación después de insertar la tarjeta de red en su computadora (si no está seguro del tipo de tarjeta que posee, consulte el embalaje o la documentación que la acompaña).

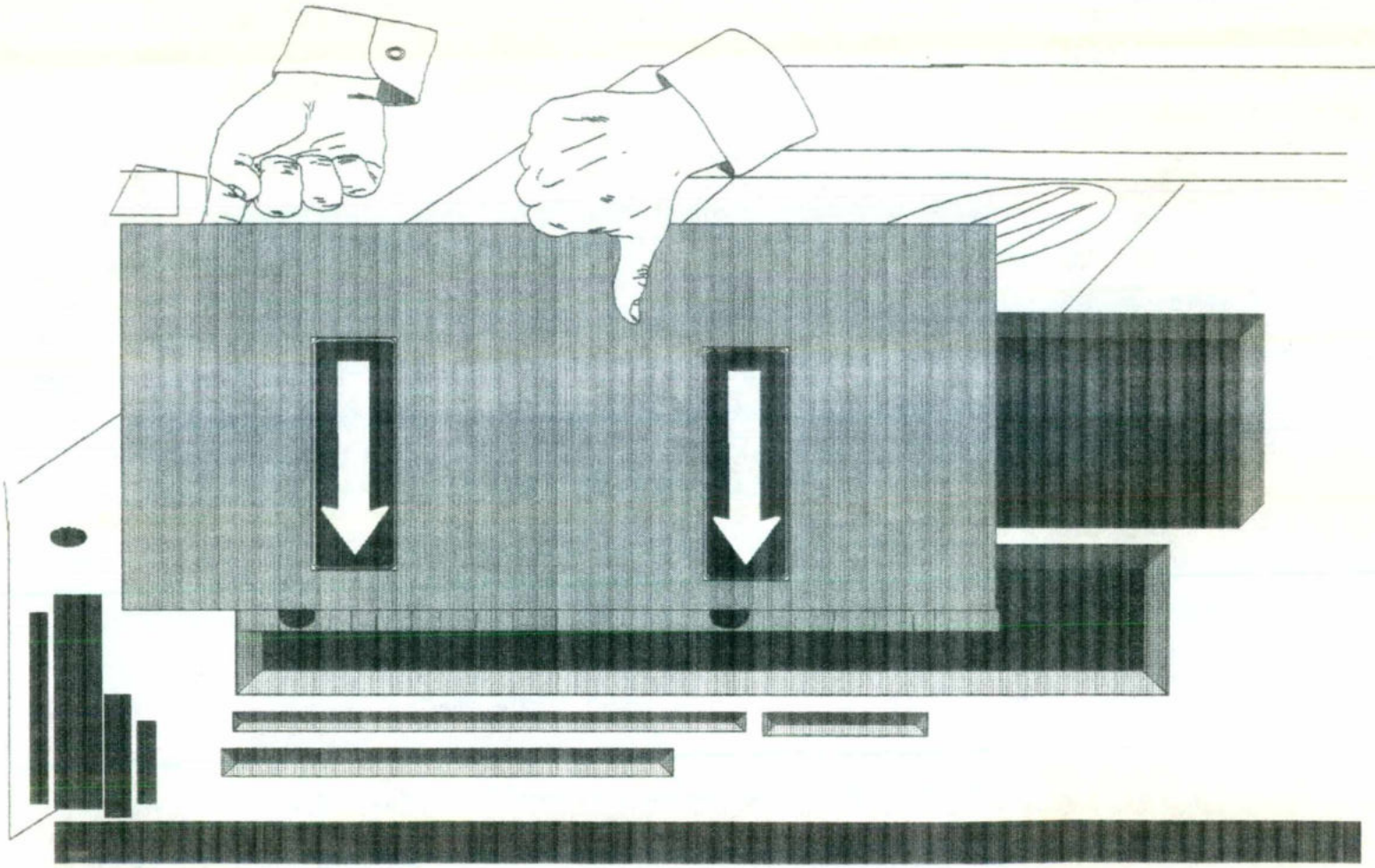


Ilustración 3.3. Insertar tarjeta

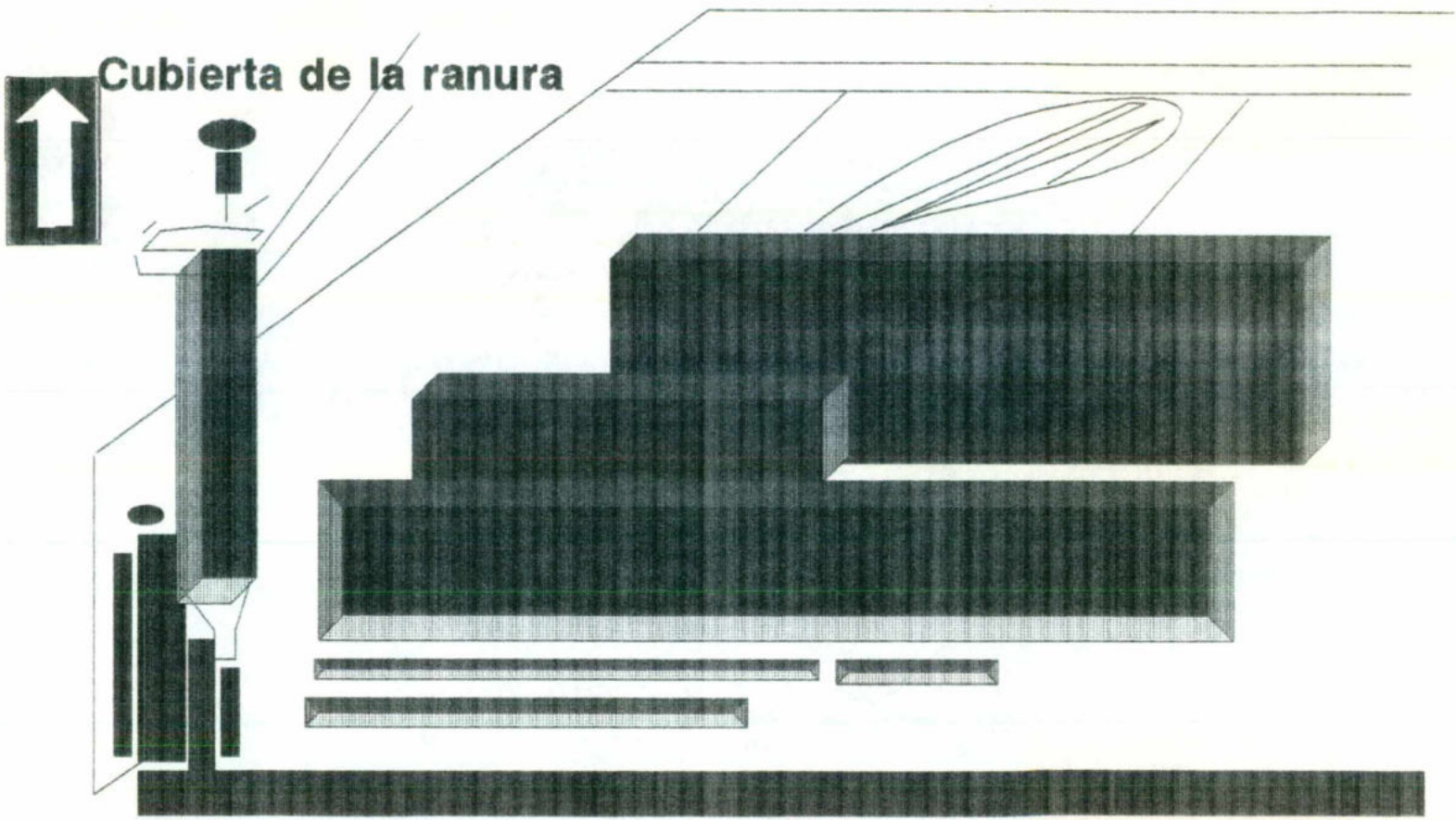


Ilustración 3.2. Retirar la cubierta de protección de la ranura.

•Si tiene una tarjeta MCA o una tarjeta ISA configurada mediante software.

1. Introduzca el disco de configuración de su computadora en la unidad de disquete de inicio (arranque) y, a continuación, reinicie (vuelva a arrancar) su computadora.

2. Cuando aparezca un mensaje informándole de que su computadora no reconoce la tarjeta de red, sustituya el disco de configuración de su computadora por el disco de configuración de su tarjeta de red y ejecute el programa de configuración (consulte la información de la tarjeta de red).

3. Configure la tarjeta de red. Para más información al respecto, consulte la sección "Determinación de los valores de configuración", anteriores.

4. Retire el disco de configuración de la tarjeta de red e introduzca el disco de configuración de su computadora. En el caso de algunas tarjetas EISA, la información de configuración de la tarjeta se copia automáticamente en el disco de configuración de su computadora. En el caso de las tarjetas MCA y de otras tarjetas EISA, se le ofrece la opción de copiar dicha información.

•Si tiene una tarjeta ISA configurada mediante software.

1. Reinicie (vuelva a arrancar) su computadora.

2. Introduzca el disco de configuración de la tarjeta de red en una unidad de disquete, cámbiese a dicha unidad y, a continuación, inicie el programa de configuración (consulte la información sobre el inicio del programa en la documentación de la tarjeta de red).

3. Configure la tarjeta de red. Para más información al respecto, consulte la sección "Determinación de los valores de configuración", anteriores.

4. Conexión de los cables.

Una vez instalada y configurada la tarjeta de red, el paso siguiente es conectar los cables que enlazan su computadora con las demás computadoras de la red. En la sección siguiente se describen los cuatro tipos más comunes de configuración de cable/computadora: Ethernet fino, Ethernet grueso, Par trenzado y Token ring.

- **Para conectar su computadora a la red, efectúe los pasos siguientes:**

1. determine a cuál de los cuatro tipos de sistemas mencionados se va a conectar y pase a la sección que describe dicho sistema.

2. Conecte la tarjeta de red a las demás computadoras de su red.

Ethernet fino.

Un sistema Ethernet fino, conocido también como "Thinnet", tiene la ventaja de utilizar un cableado menos caro que su sistema Ethernet grueso y un hardware cuya configuración es algo más sencilla.

Para conectar la tarjeta de red de su computadora a un sistema Ethernet fino, guíese por la ilustración 4.1.

En la tabla siguiente se describen los componentes de hardware.

Elemento	Descripción

Tarjeta de red con conector macho. El conector BNC macho de la parte posterior de su tarjeta de red sirve para conectar la tarjeta con un conector T.

Conector T BNC. El conector T se enchufa en el conector macho de la tarjeta de red. Los cables Ethernet finos se conectan a los conectores machos de ambos lados de la "T" (en las computadoras situadas en los extremos del grupo, uno de los cables de conexión se sustituye por un terminador).

Cable Ethernet fino con conectores BNC. Cable coaxial fino (RG-58), para redes que utilizan la norma 10Base2 u 802.3 (según la definición del Instituto de Ingeniería Eléctrica y Electrónica, IEEE).

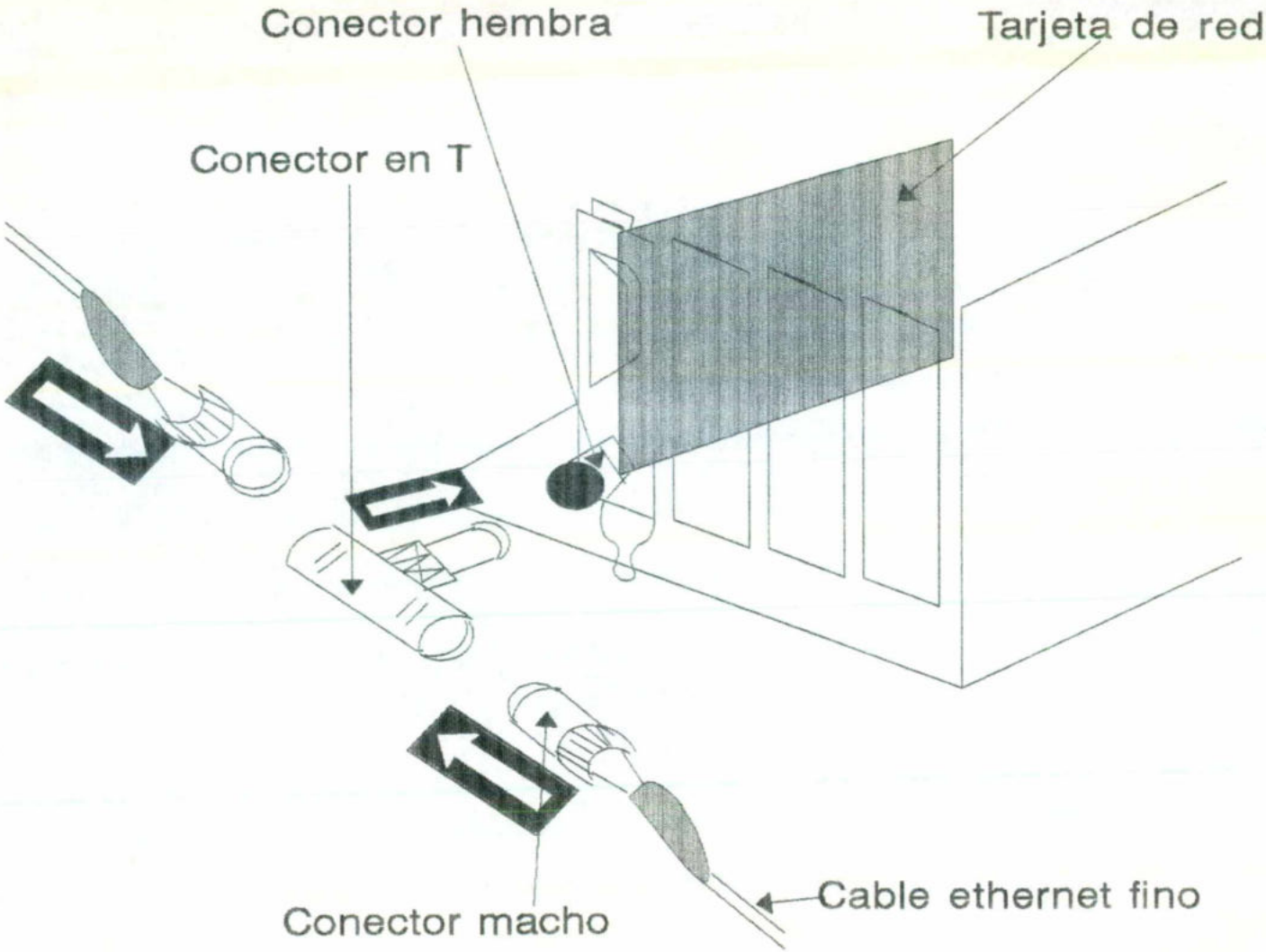


Ilustración 4.1 Conección de la tarjeta de red a un Sistema Ethernet Fino.

El cable Ethernet fino tiene conectores en ambos extremos.

Se puede utilizar el cable Ethernet fino en segmentos de longitud comprendida entre 0.5 y 185 mts., con un máximo de 30 computadoras conectadas a él. Generalmente, un segmento de cable está formado por varios cables más cortos unidos mediante conectores.

Terminador. Cuando una computadora es la última de un grupo, debe conectarse un terminador al extremo abierto al conector T de dicha computadora. Los terminadores utilizados por el cable RG-58 son de 50 ohmios.

En algunos casos, puede necesitar materiales siguientes para su sistema.

Elemento	**Descripción.**

Terminador conectado a tierra. Si en su sistema se produce un nivel excesivo de interferencias electromagnéticas o "ruido", tal vez necesite sustituir el terminador de uno de los extremos de la red por un terminador conectado a tierra. Este terminador tiene un hilo de tierra conectado a un extremo, hilo que se conecta con una toma de tierra (como por ejemplo, el tornillo de la cubierta de un enchufe eléctrico).

Conector de rodillo. Si es necesario, puede utilizarse un conector de rodillo para unir dos piezas de cable ethernet fino. Cuantas menos conexiones de rodillo haya en una red, mayor será su fiabilidad. No utilice conectores T en lugar de conectores de rodillo.

Una vez instalada la tarjeta de red y conectado el cableado, sus sistema Ethernet fino debería quedar configurado como se muestra en la ilustración 4.2.

Ethernet grueso.

Un sistema Ethernet grueso (denominado también "Thichnet") recibe su nombre del cable Ethernet estándar o grueso, que se utiliza. El cable grueso permite conectar más computadoras a un sistema y la distancia entre ellos puede ser mayor; sin embargo, este cable es más caro y más difícil de instalar que el cable Ethernet fino.

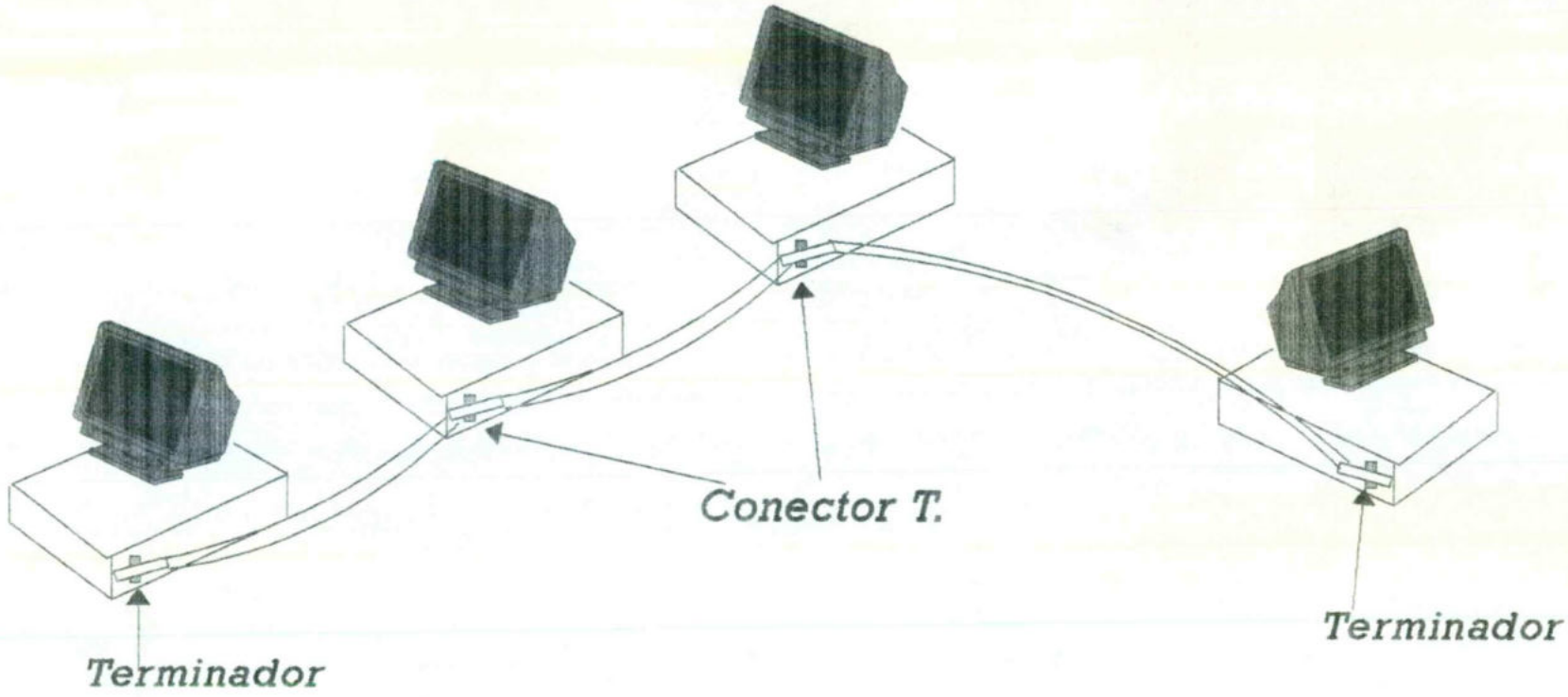


Ilustración 4.2. Ejemplo de Sistema Ethernet Fino

Nota: Deben conectarse terminadores en ambos extremos de la red.

Conecte la tarjeta de red de su computadora al sistema Ethernet grueso, guiándose por la ilustración 4.3.

En la tabla siguiente se describen los componentes de hardware:

Elemento	Descripción

Tarjeta de red con conector DIX hembra. El conector hembra de la parte posterior de la tarjeta de red se conecta con el cable de transmisión.

Cable de transmisión con un conector DIX macho y otro hembra. El cable de transmisión conecta su computadora con un transceptor de un sistema Ethernet grueso.

En un extremo del cable de transmisión hay un conector macho, que se conecta a la tarjeta de red.

En el otro extremo del cable de transmisión hay un conector hembra que se conecta a un transceptor.

La longitud máxima de un cable de transmisión es de 50 metros.

Transceptor. El transceptor conecta su computadora a una red Ethernet gruesa (en sistemas que incorporan muchas computadoras, los transceptores suelen estar ubicados dentro de las paredes de la oficina.).

Cable Ethernet grueso. Conocido también como cable "estándar" o, simplemente, cable "grueso". Es un cable coaxial. La longitud máxima del segmento es de 500 mts. y el número máximo de transceptores es 100.

Terminador. Debe conectarse a un terminador (de la serie N) al cable Ethernet en ambos extremos de la red.

En algunos casos, puede necesitar los materiales siguientes:

Terminador conectado a tierra. Si en su sistema se produce un nivel excesivo de interferencias electromagnéticas o "ruido", tal vez necesite sustituir el terminador de uno de sus extremos de la red por un terminador conectado a tierra (de la serie N). Este terminador tiene un hilo de tierra conectado a un extremo, hilo que se conecta con una toma de tierra (por ejemplo, el tornillo de la cubierta de un enchufe eléctrico).

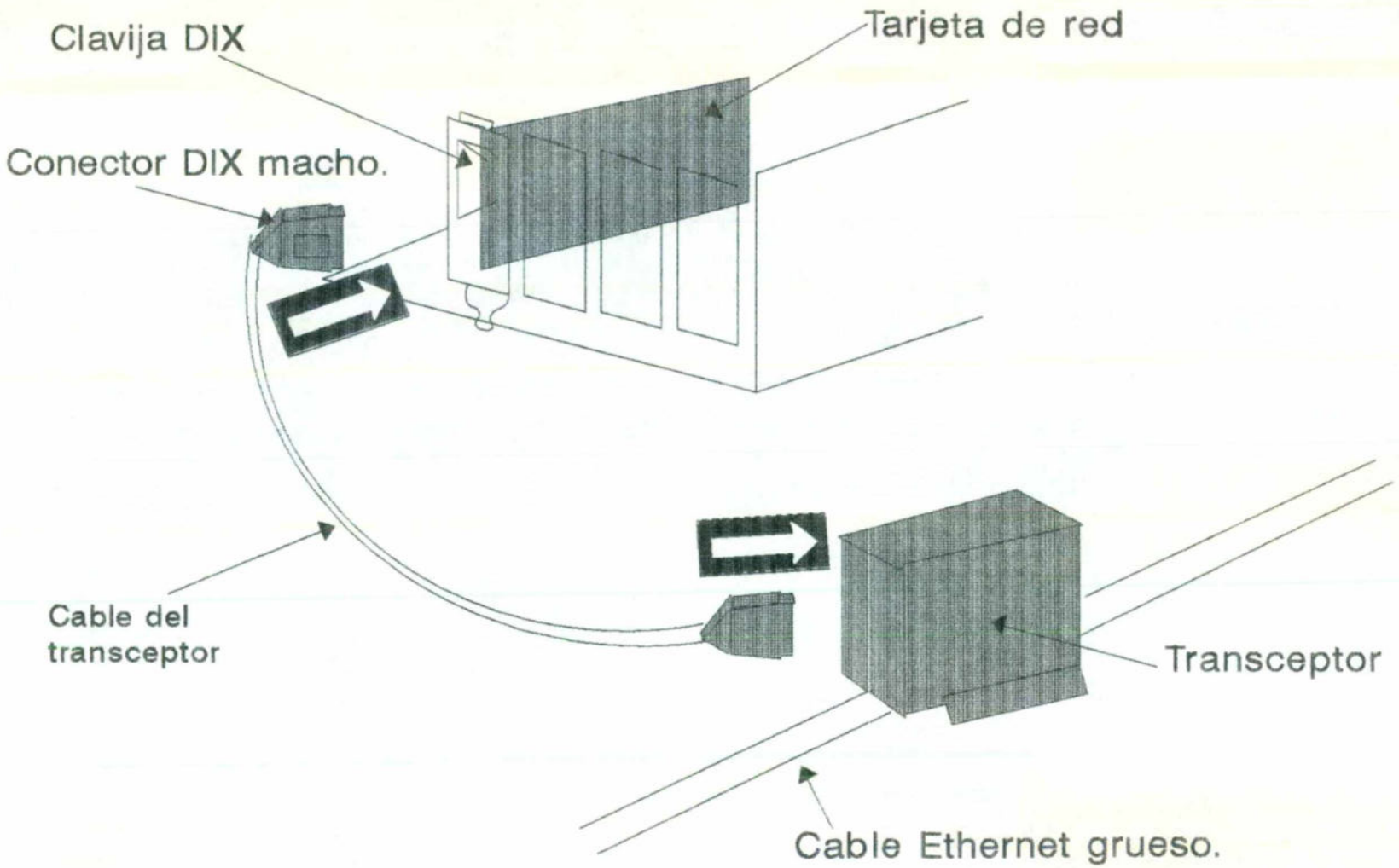


Ilustración 4.3 Conección tarjeta, sistema Ethernet Grueso.

Una vez instalada la tarjeta de red y conectado el cableado, su sistema debería quedar configurado como se muestra en la ilustración 4.4.

Ethernet de par trenzado.

Las ventajas de un sistema Ethernet par trenzado son que el cable suele ser menos caro que el de otros sistemas -como el Ethernet grueso- y que resulta relativamente sencillo instalar el cable.

Conecte la tarjeta de red de su computadora a un sistema Ethernet de par trenzado, guiándose por las ilustración 4.5.

En la tabla siguiente describen los componentes de hardware:

Elemento **Descripción.**

Tarjeta de red con un conector hembra. El conector hembra RJ-45 de la parte posterior de su tarjeta de red conecta la tarjeta con el cable de red.

Conector RJ-45. Hay un conector RJ-45 en cada extremo del cable de par trenzado. Para conectar el cable a la tarjeta, alinee el conector de forma que la patilla de plástico que de en línea con la ranura de la hembra y empuje el conector hasta que escuche un clic (el conector es similar al enchufe de plástico que se utiliza para conectar un cordón telefónico con un enchufe telefónico de pared).

Cable Ethernet de par trenzado. El cable que se utiliza en un sistema Ethernet de par trenzado puede ser bien par trenzado sin pantalla (UTP) o bien par trenzado apantallado (STP). Ambos tipos de cable consisten en dos o más pares de hilos de cobre trenzados; sin embargo, el cable STP incorpora una capa de pantalla formada por una lámina de papel metálico y un trenzado de hilo de cobre al rededor del cable interior, que lo protege de las interferencias electromagnéticas o "ruido". La longitud máxima del cable es de 100 metros.

Concentrador (centro). Las computadoras de un sistema de par trenzado se conectan entre sí mediante un concentrador o centro. El cable de cada computadora se enchufa en una hembra del centro.

Cada centro es un repetidor multipuerto 802.3 completo, compatible con la norma IEEE 802.3 10BaseT para conexión de cableado UTP.

Una vez instalada la tarjeta de red y conectado el cableado, su sistema debería quedar configurado como se muestra en la ilustración 4.6.

Token Ring

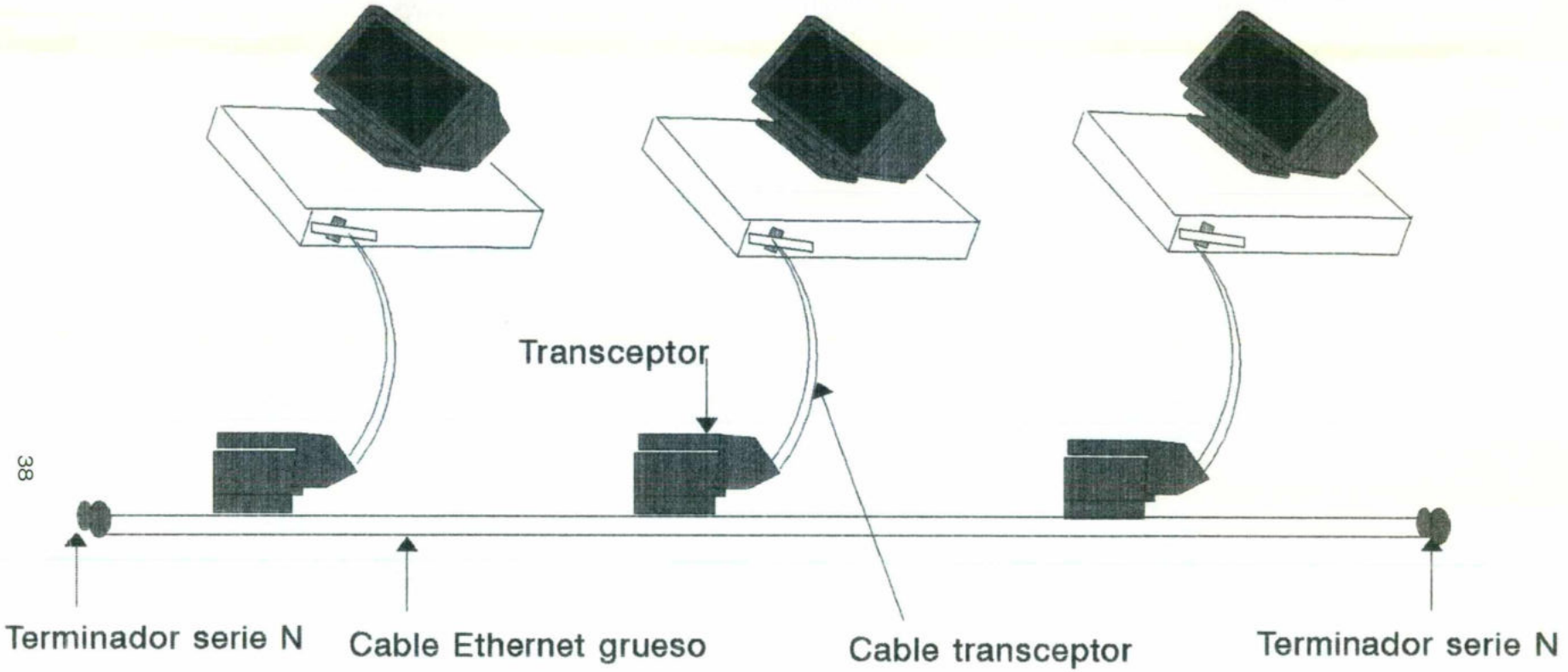


Ilustración 4.4 Ejemplo de Sistema Ethernet Grueso.

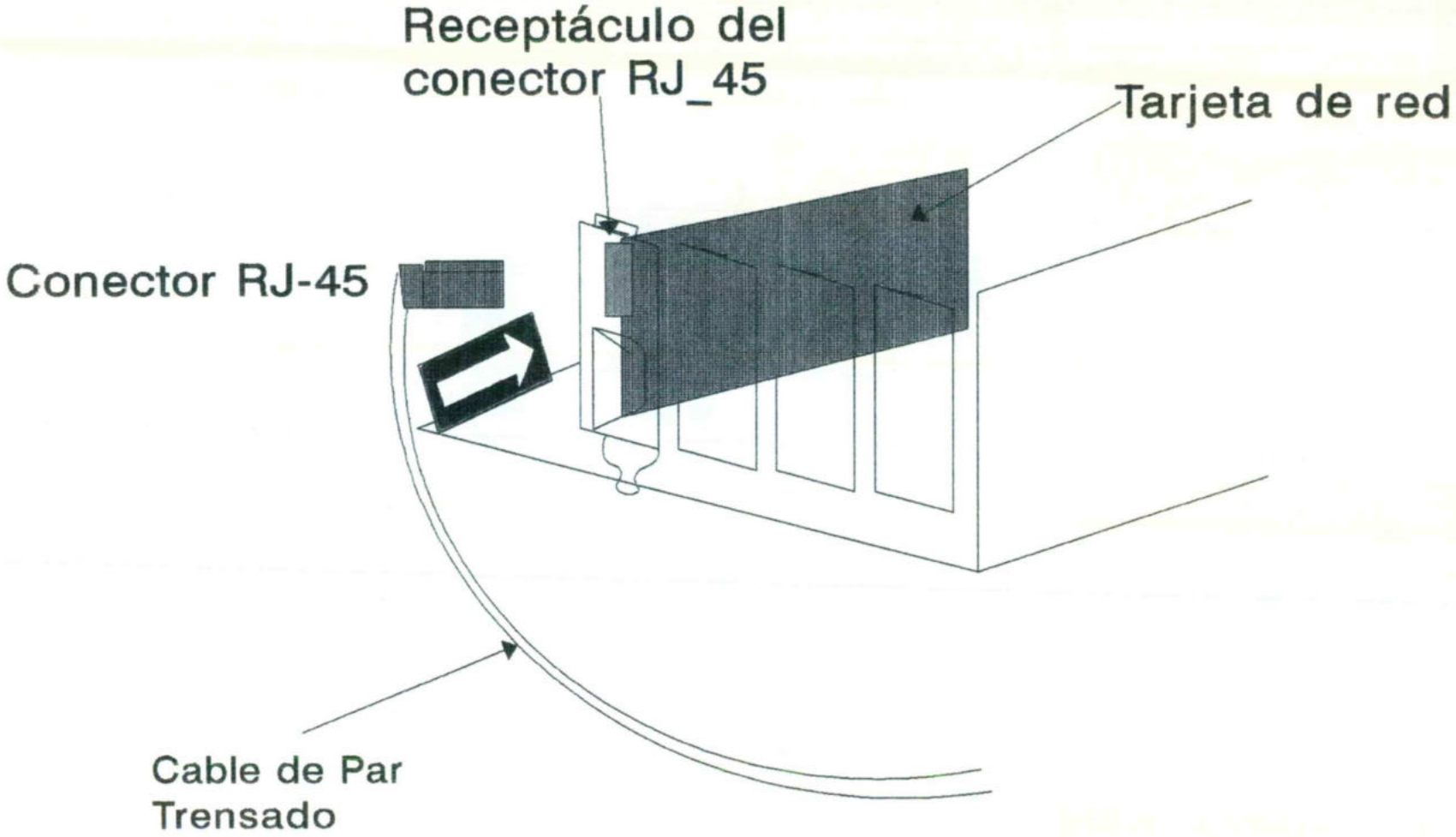


Ilustración 4.5 Conección tarjeta, Sistema Ethernet de Par Trensado.

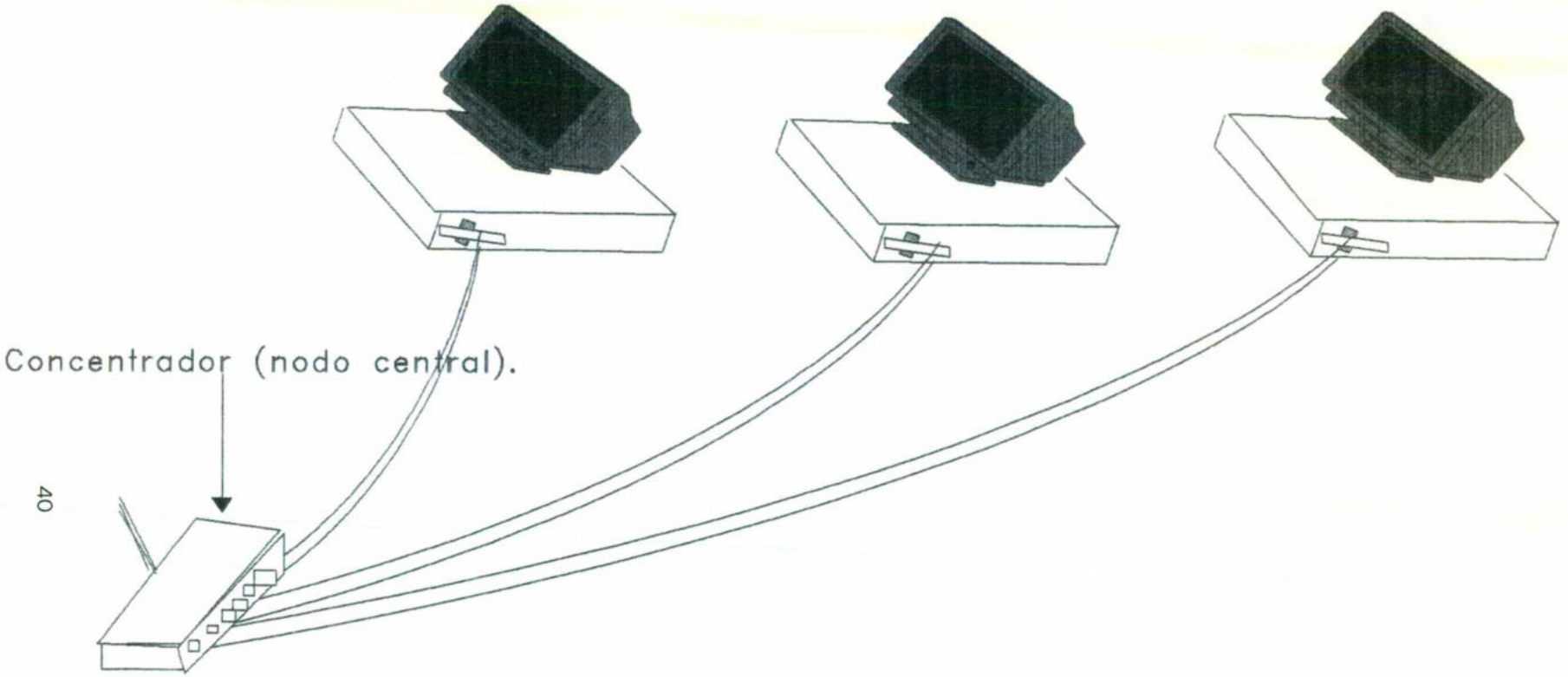


Ilustración 4.6 Ejemplo de Sistema Ethernet de Par Trensado.

Una de las ventajas del sistema token ring es la redundancia: si falla una pieza del sistema o incluso si se corta el cable, la señal retrocederá pero seguirá funcionando. Además, el software de las unidades centrales de IBM soporta el sistema token ring, lo que puede representar una ventaja en algunas situaciones.

Las desventajas estriban en que el cableado token ring es generalmente más caro y complejo que el de los otros sistemas (si utiliza cables de par trenzado, necesitará cuatro hilos). Además, a veces es más difícil localizar las averías.

Conecte la tarjeta de red de su computadora a un sistema token ring, guiándose por la ilustración 4.7.

En la tabla siguiente se describen los componentes del hardware.

Elemento **Descripción.**

Tarjeta de red. Necesita una tarjeta de red compatible con el sistema token ring.

Cable. Los sistemas token ring suelen utilizar el tipo 1, que es cable rígido de cobre o el tipo 3, que es cable de par trenzado sin pantalla (UTP).

Unidad de acceso multiestación (MAU). Dispositivo que ejerce como punto de encuentro de los cables en un sistema token ring. Los cables parten de la MAU para conectar las computadoras a la red.

Una vez instalada la tarjeta de red y conectado el cableado, sus sistema debería quedar configurado como se muestra en la ilustración 4.8.

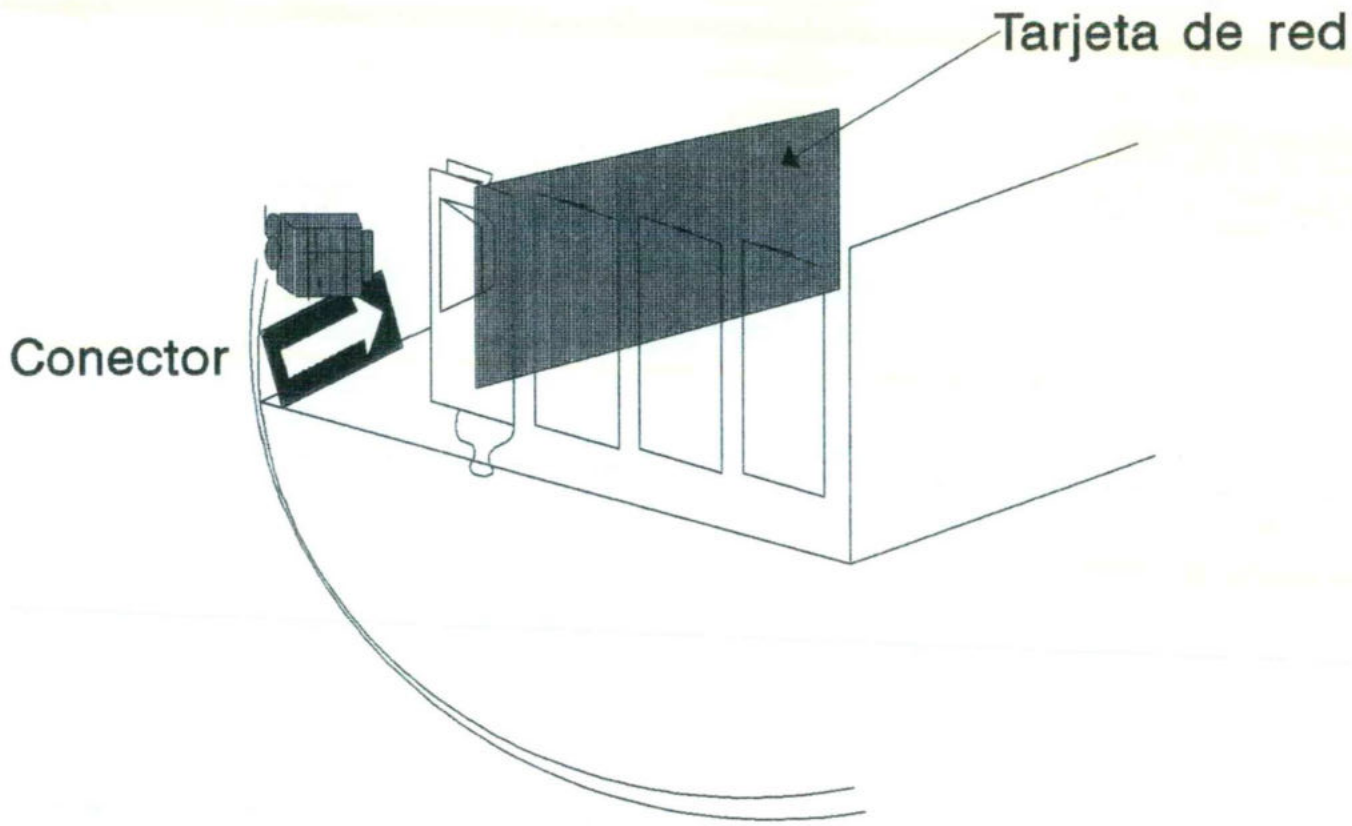


Ilustración 4.7 Conección tarjeta, sistema Token Ring.

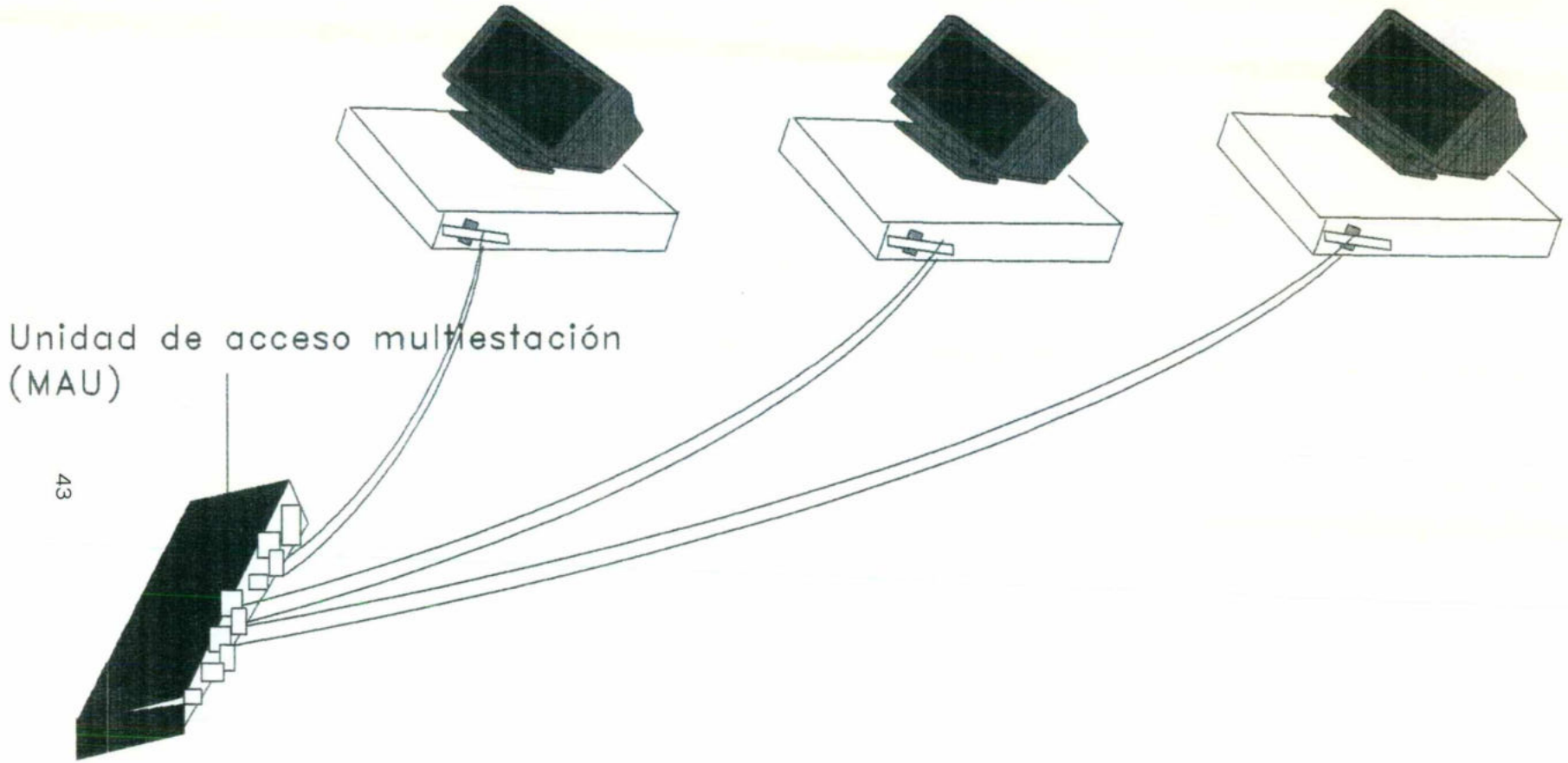


Ilustración 4.8 Ejemplo de Sistema Token Ring.

III. TOPOLOGÍA

DE LA RED

TOPOLOGÍA DE LA RED.

La topología que usa la empresa New Holan de México, es una PUNTO A PUNTO, de tipo Ethernet.

Este tipo de redes utiliza una topología de Bus lineal con un protocolo de acceso CSMA/CD (Carrier Sense Multiple Acces / Collision Detection).

En este tipo de red cada estación se encuentra conectada bajo un mismo Bus de datos, es decir, las computadoras se conectan a la misma línea de comunicación (cableado), y por esta transmiten los paquetes de información hacia el servidor y/o otros nodos.

Cada estación se encuentra monitoreando constantemente la línea de comunicación con el objeto de trasmitir o recibir sus mensajes, si la línea presenta tráfico en el momento que una estación quiere trasmitir, la estación espera un periodo muy corto (mili segundos) para continuar monitoreando la red.

Si la línea está libre, la estación transmisora envía su mensaje en ambas direcciones por toda la red. Cada mensaje incluye una identificación del nodo transmisor hacia el receptor y solamente el nodo receptor puede leer el mensaje completo.

Cuando dos estaciones trasmiten sus mensajes simultáneamente una colisión ocurre y es necesaria una retransmisión. Ya que el nodo aún está monitoreando, sabe que ha ocurrido una colisión, es decir, es capaz de detectar la colisión, e intentará de nuevo la transmisión del mensaje. el protocolo incluye las reglas que determinan cuánto tiempo tendrán que esperar los nodos o estaciones para realizar sus envíos nuevamente.

La velocidad de transmisión de Ethernet es de 19 Mbps, por lo contrario de lo que pudiese pensar conforme al tipo de comunicación y operación, en el que se tienen tiempos de respuesta inconsistentes e imprescindibles, su rendimiento es muy superior al de otro tipo de redes locales.

Ethernet soporta distintos tipos de cableado. Todo lo que se ha descrito es cuando se utiliza un cable coaxial. pero, ¿Qué sucede cuando se utiliza cable telefónico UTP o fibra óptica?. El concepto de Bus lineal se altera que en este tipo de cableado la topología ya no es precisamente un Bus lineal, sino tipo estrella.

Se parece físicamente a las redes Arcnet o Token Ring, ya que los nodos se conectan a través de un centro de cableado o concentradores y éstos podrían o no enlazarse a un Bus de cable coaxial o de fibra óptica. Lo que realmente está sucediendo es que estos concentradores Ethernet de cable UTP internamente con su electrónica, llevan ese Bus lineal para la conexión de los nodos.

Esta forma de conexión con cableado UTP día a día se introduce en el grueso de las instalaciones ya que presenta una instalación más fácil, un monitoreo y administración de la red, así como el bajo costo de cableado y un crecimiento de la red mucho más sencillo.

Actualmente,. este tipo de redes bajo cableado UTP y por la misma evolución de la tecnología está regida bajo el estándar 10 Base-T.

La estructura que tiene actualmente la red es la siguiente:

10BT Concentores RJ45
10B2 y 10B5 Concetores
BNC

Abel
Jose Luis
Roger
Juvenal
Fidel
Mario
Jose A.

Novell

Paco M. Fco.
Consulta Acer Aburto
Consulta HP Uso común
Marlyn Juana
Betty Tranquilino
Olivia Enrrique O.
Martha E. Finch

Usuarios

E. Heerrera
Vicente
Juan E.
Elias

Usuarios

Almacen
Raúl R.
Anselmo Angélica
Gonzalo Manufactura
Htas. Cecilia
Manufact. Planeación
Arturo D. Marcela
Angel Armando
Manuel Salgado
Yura Liz
Agustin Rocío
Gustavo Herrera
Ricardo Marcelo
Ana Ma. Ramón

Salgado
Callejas
Tomás
Diana
Yuira
Mary M.
Lupita
E. Villareal

Usuarios

Campos Sarahi
Salvador Moisés
Monse Apolinar
Humberto Vicky
Morales Miguel
Lupita Fernando

Usuarios

Hub Ingeniería

Hub Ingeniería

Hub refacciones

DTC comedor

Hub
Comedor

Hub manufactura

10B2 10B5 10B2 10B2 10B2

ETHERNET

10B2 10B2

10b2

Prepintura
Linea final

Hub
Operación

10B2 10B2

Hub's
Sistemas

10BT

DTC sistemas

10BT

10BT

Hub sala
sistemas

Felisa
Moreno
Tráfico

Nacho Gustavo Cederborg
Sergio Felisa Braham
Oscar Raymundo Lorena
Martin Paty Martha
Lidia Alejan. Gerardo
Esteban Jose L. Alejandra
Mary Joaquin Florencio
Sergio U. Gelly

10BT

Servidor J
Servidor I
Servidor G
DS0
Pepe
HP 847s
HP 877s

Router NH USA

Usuario 1
Usuario5
Sala sistemas

IV. DESCRIPCION

DE LOS COMPONENTES

DE LA RED

DESCRIPCIÓN DE LOS COMPONENTES DE LA RED.

SERVIDORES:

1. PROCESADOR : 486 a 66 Mhz.
   RAM: 16 Mb.
   DRIVE´S: 1 de 31/2
   1 de 51/4
   CAPACIDAD DISCO DURO: 1 Gb.
   MARCA: HP (Heweltt Packard)

2. PROCESADOR : 486 a 66 Mhz.
   RAM: 16 Mb.
   DRIVE´S: 1 de 31/2
   1 de 51/4
   CAPACIDAD DISCO DURO: 1 Gb.
   MARCA: HP (Heweltt Packard)

3. PROCESADOR : 486 a 66 Mhz.
   RAM: 16 Mb.
   DRIVE´S: 1 de 31/2
   1 de 51/4
   CAPACIDAD DISCO DURO: 1 Gb.
   MARCA: HP (Heweltt Packard)

4. PROCESADOR : PENTIUM a 100 Mhz.
   RAM: 16 Mb.
   DRIVE´S: 1 de 31/2
   CAPACIDAD DISCO DURO: 1 Gb.
   MARCA: HP (Heweltt Packard)
   1 CD ROM - Velocidad Cuadruple, Marca HP

ESTACIONES DE TRABAJO:

Se tiene 29 Terminales Tontos y 83 Pc´s.
Las características en general de las terminales tontas son:
MARCA: HP
MODELO: 700/80

Las características de las PC´S se describen a continuación:

TARJETAS.

TARJETA	MARCA
NOVELL	NE 2000
SMC	Ethernet Card Plus y Elite 16T
3COM	Ethernet Link III
XIRCOM	Net (Entrada)
HP	8 Lan y 16 Bit´s - Star Land
INTEL	Ether express

TIPO DE CABLE.

COAXIAL (Bus principal) 10 Base 2
10 Base 5

PAR TRENSADO (Terminales) 8 y 10 Hilos
Entradas RJ45

CONCENTRADORES.

Se cuenta con 14 concentradores y 3 por instalar. Sus características son:

1. SMC 8 Puertos
1. SMC 8 Puertos
1. SMC 8 Puertos
1. SMC 8 Puertos
1. CNET 16 Puertos
1. CNET 16 Puertos
1. CNET 16 Puertos
1. CNET 12 Puertos
1. CNET 12 Puertos
1. CNET 12 Puertos
1. CNET 8 Puertos
1. CNET 8 Puertos
1. CNET 8 Puertos
1. CNET 8 Puertos

CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO

USUARIO	DIR. IP	CABLE	MARCA_PC	DEPARTAMENTO	PROCESADOR	CAP. D.D	RAM	TARJETA
Enrique O.	11	427	Texas	Logística	486DX/50	370	8	SMC
Ignacio R.	12		COMPAQ	Sistemas	Pentium / 170 Mhz	1 Gb	16	HP
Lidia G.	13	125	COMPAQ	Sistemas	75 Mhz	630	8	SMC
Oscar O.	14	126	COMPAQ	Sistemas	75 Mhz	630.5	8	HP
Olivia R.	16	4111	COMPAQ	Logística	Pentium / 75	630	8	HP
Marlyn	17	413	HP QS	Logistica	80386/16	117.1	4	SMC
Mary S.	18	128	COMPAQ	Sistemas	75 Mhz	630.5	8	SMC
Vicky/Sarahi	19	623	Acer	Rec. Hum.	486DX/33	170	4	SMC
José Manuel	22	511	HP	Compras	80386/25	84.7	4	3COM
Alejandra L.	23	127	HP	Caja	80386/20	116	4	3COM
Sergio A.	24	122	COMPAQ	Sistemas	Pentium / 75	360.5	8	3COM
Fernando D.	25	625	COMPAQ	Rec. Humanos	Pentium / 75	630	8	HP
Moisés G.	26	624	HP	Rec. Hum.	80386/20	121.8	2	SMC
José Gpe. P.	27		COMPAQ	Sistemas	75 Mhz	630.5	8	INTELL
Betty C.	28	415	COMPAQ	Logística	Pentium / 75	630.5	8	SMC
Lupita A.	29	627	HP	Rec. Hum.	80386/25	84.7	4	SMC
Elias S.	36	714	COMPAQ	Refacciones	Pentium / 75	630.5	8	SMC
Tomás R.	37	513	HP	Compras	386DX/66	340	8	SMC
Vicente S.	38	712	COMPAQ	Refacciones	Pentium / 75	630	8	3COM
Eduardo	39		HP	Refacciones	486DX/33	230	8	3COM
Antonio C.	40	613	HP	Rec. Hum.	486DX/66	470	8	SMC
Salvador	41		Acer	Calidad	486DX4 / 100 Mhz	520	8	SMC
Rocío	42		HP	Refacciones	386 / 25 Mhz	84	4	3COM

CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO

USUARIO	DIR. IP	CABLE	MARCA_PC	DEPARTAMENTO	PROCESADOR	CAP. D.D	RAM	TARJETA
Mary M.	43	516	COMPAQ	Compras	Pentium/75	630	8	3COM
Francisco M.	44		HP	Pre-pintura	80386/20		4	3COM
Jesús R.	45		HP	Linea final	80386/20		4	SMC
Angelina L.	46	11	HP	Costos	80386/25	84.7	4	SCOM
Paty R.	47	112	HP	Contabilidad	80386/25	84.7	4	SMC
Apolinar H.	48	626	Acer	Dir. Operación	486DX/66	425.5	8	SMC
Tranquilino B.	49	425	COMPAQ	Logística	Pentium / 75	630.5	8	INTEL
J.J. Braham	50	14	COMPAQ	Dir. Finanzas	Pentium / 120	631.5	16	3COM
Florencio T.	51	118	HP	Crédito y Cobranza	80386/20	52	4	HP
Raymundo G.	52	137	Acer	Contabilidad	486DX/66	425	8	SMC
Francisco M.	53	416	Acer Mate	Calidad Integral	486DX4/100 Mhz	540	8	SMC
Uso Común	54	428	HP	Ingeniería	486DX/33	427	4	SMC
Esteban T.	55	124	COMPAQ	Sistemas	75 Mhz	630.5	8	SMC
Joseé A.	56	417	HP	Ingeniería	486DX/33	427	4	SMC
Rogelio M.	57	419	HP	Ingeniería	486DX/33	427	4	SMC
Consulta	58	4112	HP QS	Ingeniería	80386/16	41.8	4	SMC
Lupita R.	59	517	HP	Planeación	80386/20	52	4	3COM
Antonio M.	60	618	COMPAQ	Rec. Humanos	Pentium / 75	630	8	SMC
Consulta	61	4110	Acer	Ingeniería	486DX/66	408	8	3COM
Juan 2	62	512	HP	Compras	486DX/66	345	4	INTEL
Yiura L.	63	515	HP	Compras	80386/25	84.7	4	SMC
Eduardo V.	64	518	HP	Compras	80386/20	52	4	3COM
Ma. Gpe. L.	65	622	HP	Manufactura	80386/20	120	4	SMC

CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO

USUARIO	DIR. IP	CABLE	MARCA_PC	DEPARTAMENTO	PROCESADOR	CAP. D.D	RAM	TARJETA
Gustavo H.	66	138	HP	Contabilidad	80386/25	84.7	4	SMC
Alejandro M.	67	135	Acer	Contabilidad	486DX4/100	520	8	SMC
José Luis L.	68	133	COMPAQ	Contabilidad	Pentium / 75	630.5	8	3COM
Felisa E.	69	134	Acer	Contabilidad	486DX/66	300	8	SMC
Sergio U.	70	136	HP	Crédito y Cobranza	486DX/33	427.3	4	SMC
Diana O.	71	514	COMPAQ	Compras	Pentium / 75	630	8	3COM
Carlo M.	72		TOSHIBA	Dir. general	Pentium / 75		8	XIRCOM
Monserrat	73	615	Acer	Planeación	486DX/66	260	8	3COM
Joaquin N.	74	129	HP	Costos	486DX/33	520	4	3COM
Gerardo R.	75	113	Acer	Impuestos	486DX/66	212	8	SMC
Juana	77	4212	HP	Logística	80386/25n	84.7	4	3COM
Miguel	78	426	HP	Logística	486DX/33Mhz	170.45	4	INTEL
Francisco P.	79	424	HP	Logistica	486DX/33	84.75	4	SMC
Martha R.	80	4211	HP	Logística	486DX/66	345	8	SMC
Martha O.	81	117	HP	Dir. Rec. Hum.	486DX/33	84.7	4	SMC
Lorena V.	82	115	HP	Dir. general	80386/25	84.7	8	SMC
Usuario 2	83	33	HP	Sala Capacitación	80386/25	84.7	4	3COM
Usuario 4	84	35	HP	Sala capacitación	80386/25	84.7	4	3COM
Usuario 1	85	32	HP	Sala capacitación	80386/25	84.7	4	SMC
Usuario 3	86	34	HP	Sala Capacitación	80386/25	84.7	4	SMC
Usuario 5	87	36	HP	Sala Capacitación	80386/25	151.1	4	3COM
Mario C.	186	121	COMPAQ	Manufactura	Pentium / 75	630	8	NOVELL
Juan C.	249	116	HP	Dir. Rec.Hum.	486DX/66	213	8	SMC

CARACTERISTICAS DE LAS ESTACIONES DE TRABAJO

USUARIO	DIR. IP	CABLE	MARCA_PC	DEPARTAMENTO	PROCESADOR	CAP. D.D	RAM	TARJETA
Edwin F.	253	429	HP	Ingeniería	80386/25	290	4	SMC
José Luis P.	NIVELL	412	COMPAQ	Ingeniería	Pentium / 75	630	8	NOVELL
Orlando	NOVELL		Acer	Manufactura	486DX/66		8	NOVELL
Abel M.	NOVEL	414	COMPAQ	Ingeniería	Pentium / 75	630	8	NOVELL
Juvenal	NOVEL	422	COMPAQ	Ingeniería	Pentium / 75	630	8	NOVELL
Fidel A.	NOVEL	423	COMPAQ	Ingeniería	Pentium / 75	630	8	NOVELL
Mario O.	NOVEL	418	COMPAQ	Ingeniería	Pentium / 75	630	8	NOVELL
Humberto M.	NOVEL	617	COMPAQ	Manufactura	Pentium / 75	630	8	NOVELL
Enrique M.			HP	Refacciones	486DX/66	299	8	3COM
Dalia			HP	Tráfico	80386/20	52	4	3COM
Elia H.			Acer	Calidad	486DX/100	543.7	8	SMC
Brenda			Apple Manchitoch	Publicidad	7600 / 120	1 Gb	16	APPLE

REGULADORES.

Se cuenta con 50 reguladores, en una parte de la planta, de diferentes marcas. La otra parte de la planta, donde se encuentra el área de Sistemas, se tiene instalación eléctrica con regulador integrado.

NO BREAK.

Se cuenta con 2 No Break, marca TRIP.

ELIMINADORES.

No se cuenta con eliminadores de corriente.

IMPRESORAS.

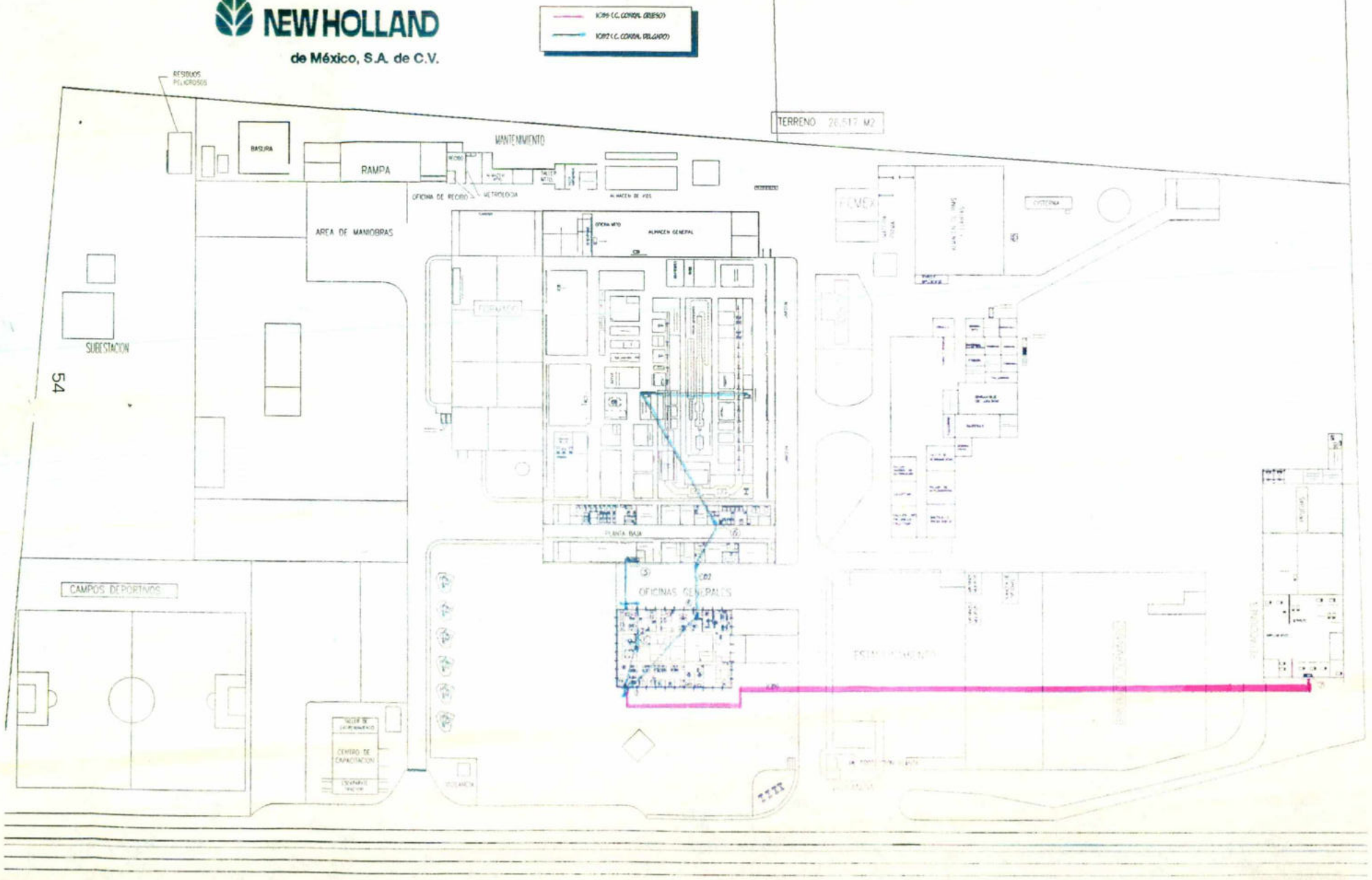
DEPARTAMENTO	CANTIDAD	MARCA
Sistemas	1	HP 4
Sistemas	1	DESK JET 660c
Impuestos	1	HP 4
Costos	1	HP 3
Contabilidad	1	HP 3
Contabilidad	1	PANASONIC
Dir. de finanzas	1	HP 4
Dir. Gral.	1	HP 3
Logística	1	HP 4
Tráfico	1	HP 4
Ingeniería	1	HP 3
Ingeniería	1	PLOTTER
Ingeniería	1	DESK JET 1200
Ventas	1	DESK JET 1200
Compras	1	OKIDATA
Compras	1	HP 4
Compras	1	PANASONIC
R. Humanos	1	HP 4
R. Humanos	1	HP 3
Refacciones	1	DESK JET 660 c
Operación	3	HP (Reportes)

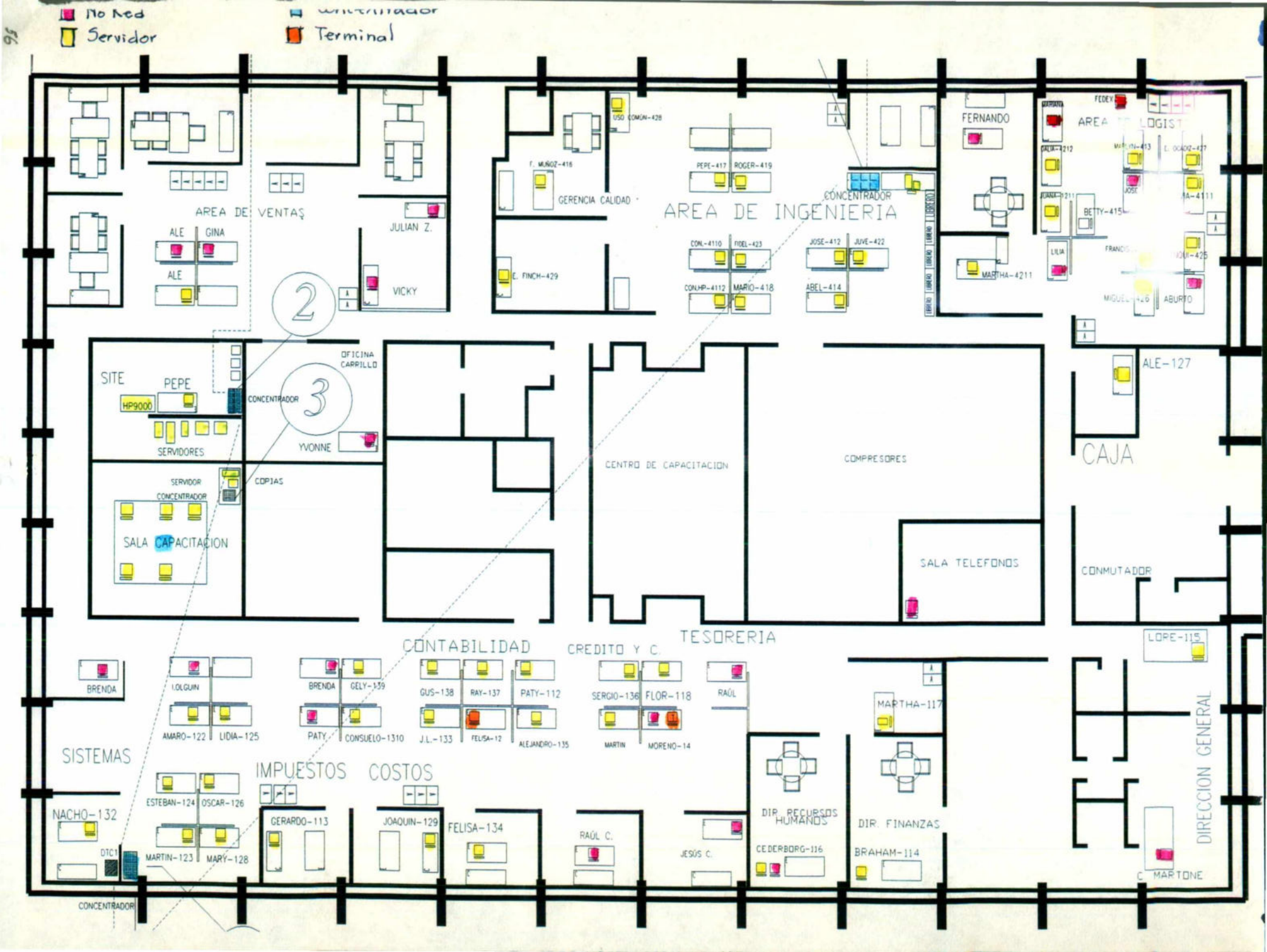
V. PSEUDOMAPA

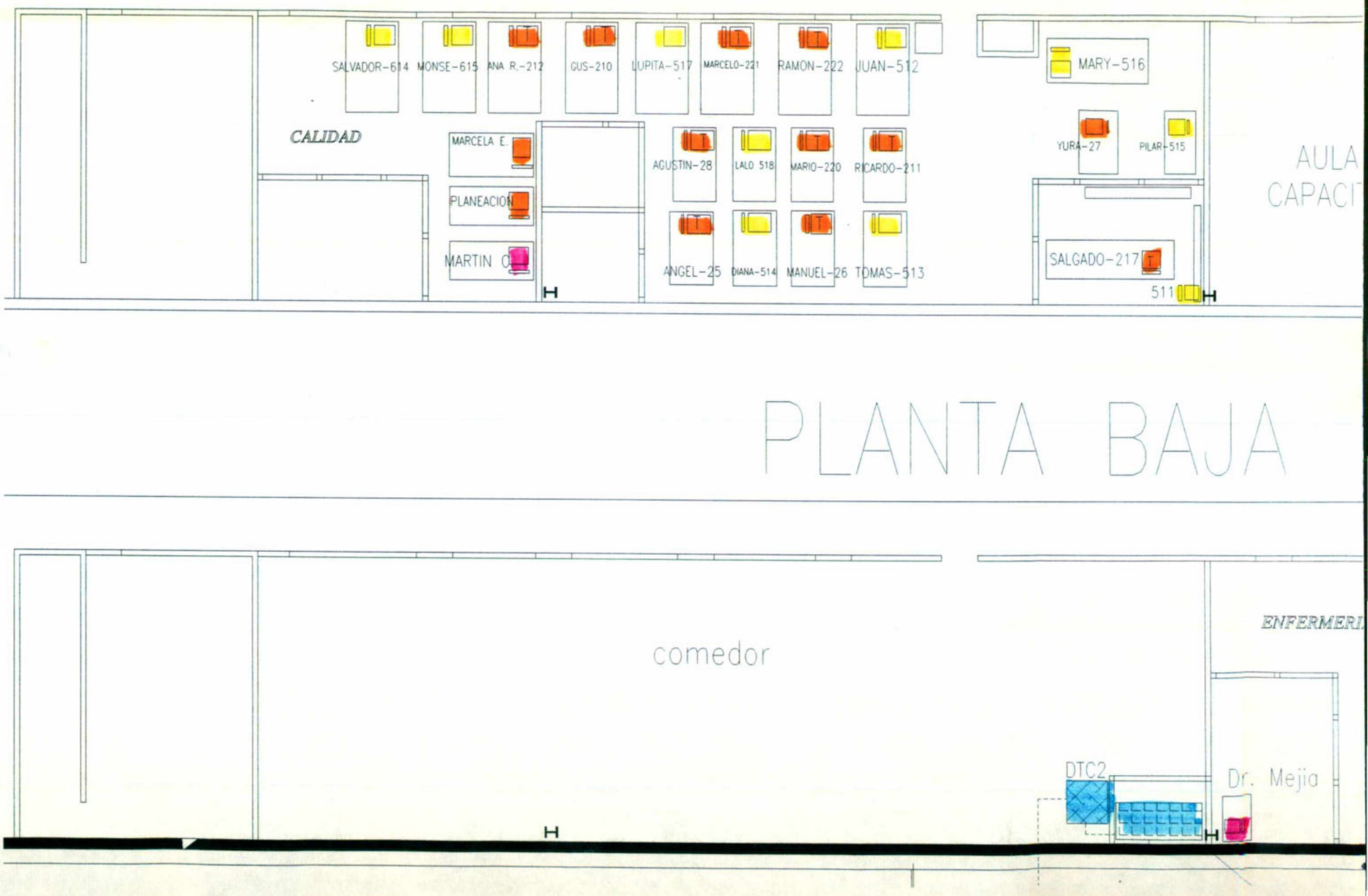
(DIAGRAMA DE CABEADO)

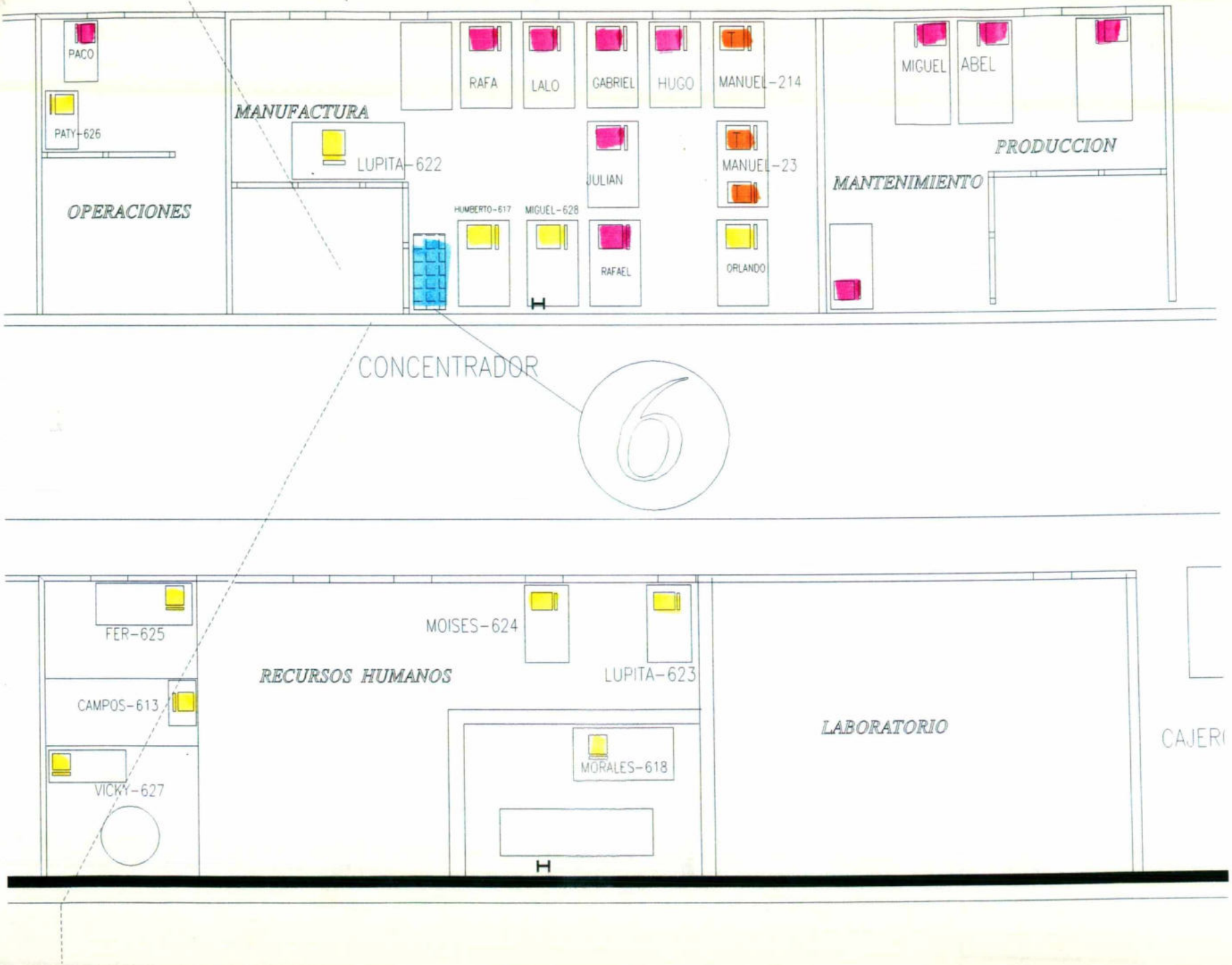
LAY-OUT GENERAL RED INTERNA

NEW HOLLAND
de México, S.A. de C.V.

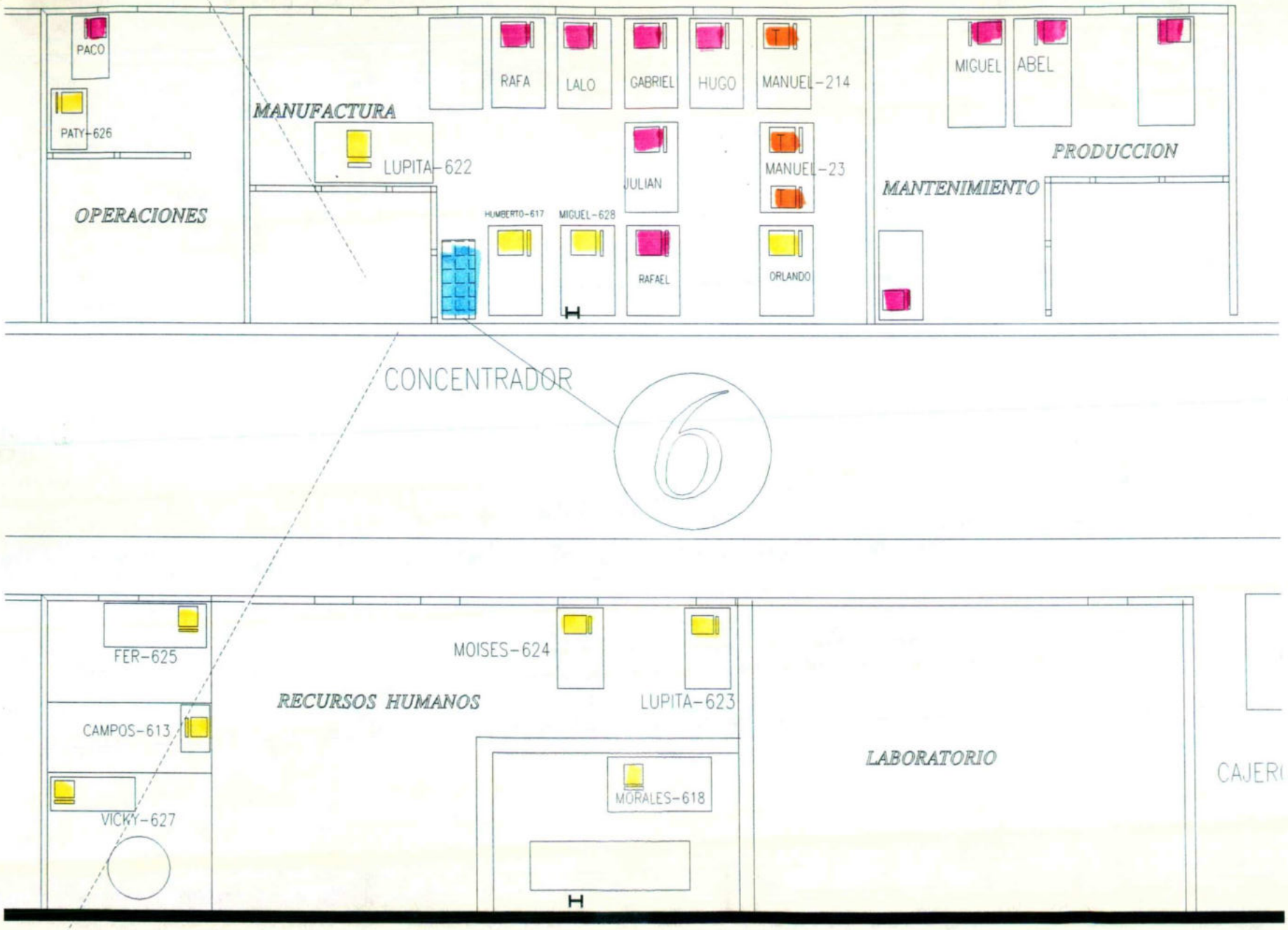


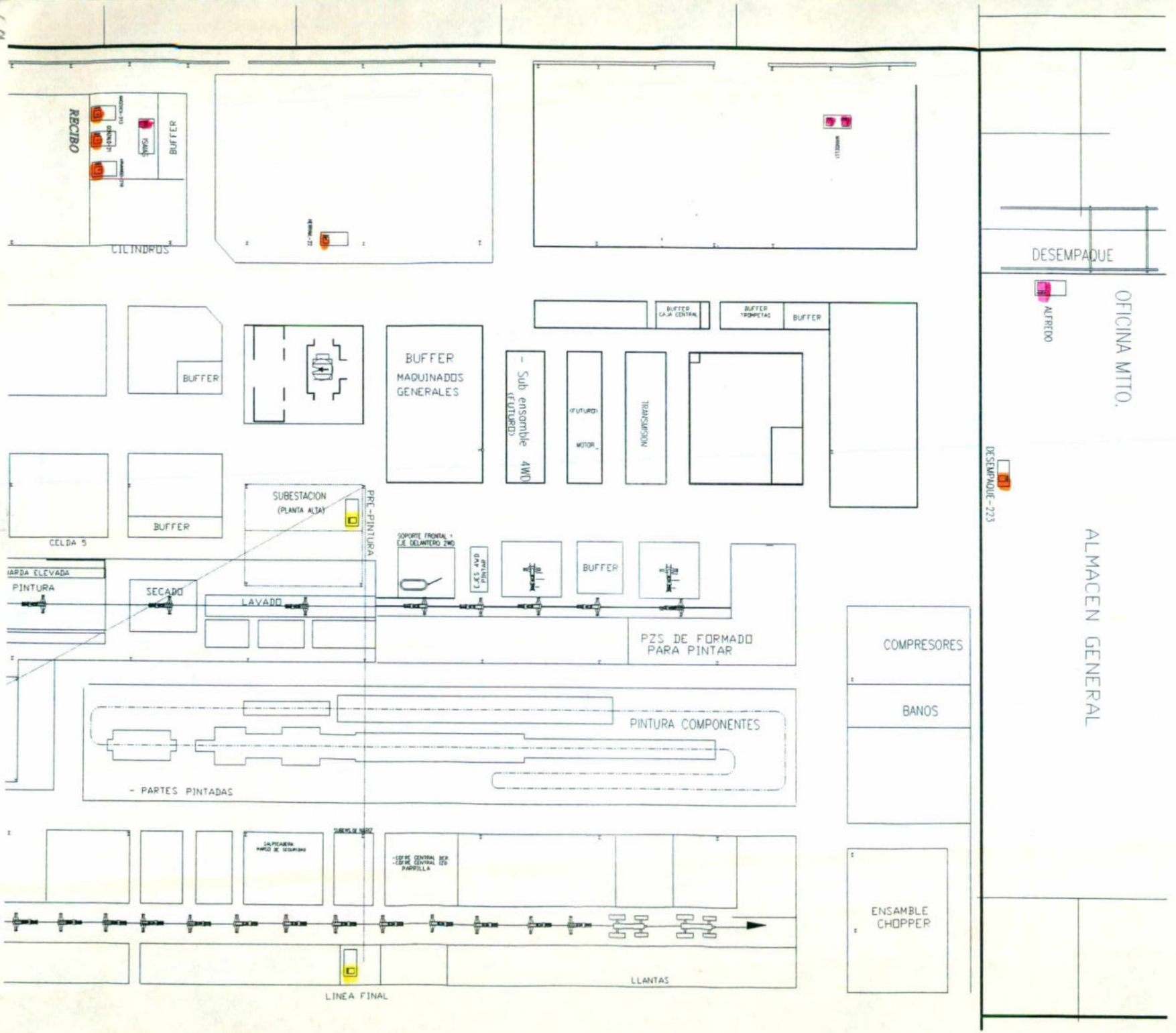

No Red
Servidor
Terminal
AREA DE VENTAS
ALE
GINA
ALE
JULIAN Z.
VICKY
2
USO COMÚN-426
F. MUÑOZ-416
GERENCIA CALIDAD
E. FINCH-429
AREA DE INGENIERIA
PEPE-417
ROGER-419
CONCENTRADOR
CON.-4110
FIDEL-423
CON.HP-4112
MARIO-418
JOSE-412
JUVE-422
ABEL-414
FERNANDO
MARTHA-4211
FEDEX
AREA DE LOGIST
CALIA-4212
JUANA-4211
BETTY-415
JOSE
L'LIA
ABURTO
ALE-127
CAJA
SITE
PEPE
HP9000
CONCENTRADOR
SERVIDORES
OFICINA CARRILLO
3
YVONNE
SERVIDOR CONCENTRADOR
COPIAS
SALA CAPACITACION
CENTRO DE CAPACITACION
COMPRESORES
SALA TELEFONOS
CONMUTADOR
TESORERIA
CONTABILIDAD
CREDITO Y C.
LOPE-115
BRENDA
I.OLGUIN
AMARO-122
LIDIA-125
BRENDA
GELY-139
PATY
CONSUELO-1310
GUS-138
RAY-137
PATY-112
J.L.-133
FELISA-12
ALEJANDRO-135
SERGIO-136
FLOR-118
MARTIN
MORENO-14
RAÚL
MARTHA-117
SISTEMAS
IMPUESTOS
COSTOS
ESTEBAN-124
OSCAR-126
NACHO-132
DTC1
MARTIN-123
MARY-128
GERARDO-113
JOAQUIN-129
FELISA-134
RAÚL C.
JESÚS C.
DIR. RECURSOS HUMANOS
CEDERBORG-116
DIR. FINANZAS
BRAHAM-114
DIRECCION GENERAL
C. MARTONE
CONCENTRADOR


SALVADOR-614
MONSE-615
ANA R.-212
GUS-210
LUPITA-517
MARCELO-221
RAMON-222
JUAN-512
CALIDAD
MARCELA E.
PLANEACION
MARTIN C.
AGUSTIN-28
LALO 518
MARIO-220
RICARDO-211
ANGEL-25
DIANA-514
MANUEL-26
TOMAS-513
MARY-516
YURA-27
PILAR-515
AULA
CAPACI
SALGADO-217
511
PLANTA BAJA
comedor
ENFERMERI
DTC2
Dr. Mejia


PACO
PATY-626
OPERACIONES
MANUFACTURA
LUPITA-622
RAFA
LALO
GABRIEL
HUGO
MANUEL-214
JULIAN
MANUEL-23
HUMBERTO-617
MIGUEL-628
RAFAEL
ORLANDO
MIGUEL
ABEL
PRODUCCION
MANTENIMIENTO
CONCENTRADOR
6
FER-625
MOISES-624
RECURSOS HUMANOS
LUPITA-623
CAMPOS-613
VICKY-627
MORALES-618
LABORATORIO
CAJER


ANSELMO-225
RAUL-224
AMADOR
SERVICIO
LIZ-218
VICENTE-712
ROCIO-219
CECILIA-215
IMPLEMENTOS
HERRERA-711
ELIAS-714
JUAN-713
ARTURO-24
CONCENTRADOR
7


PACO
PATY-626
OPERACIONES
MANUFACTURA
LUPITA-622
RAFA
LALO
GABRIEL
HUGO
MANUEL-214
JULIAN
MANUEL-23
HUMBERTO-617
MIGUEL-628
RAFAEL
ORLANDO
MIGUEL
ABEL
PRODUCCION
MANTENIMIENTO
CONCENTRADOR
6
FER-625
MOISES-624
LUPITA-623
RECURSOS HUMANOS
CAMPOS-613
VICKY-627
MORALES-618
LABORATORIO
CAJER


RECIBO
BUFFER
CILINDROS
DESEMPAQUE
ALFREDO
OFICINA MTTO.
ALMACEN GENERAL
DESEMPAQUE-223
BUFFER
BUFFER MAQUINADOS GENERALES
BUFFER CAJA CENTRAL
BUFFER TROMPETAS
BUFFER
- Sub ensamble 4WD (FUTURO)
(FUTURO) MOTOR
TRANSMISION
CELDA 5
BUFFER
SUBESTACION (PLANTA ALTA)
PRE-PINTURA
SOPORTE FRONTAL + EJE DELANTERO 2WD
BUFFER
PINTURA
SECADO
LAVADO
PZS DE FORMADO PARA PINTAR
COMPRESORES
BANOS
PINTURA COMPONENTES
- PARTES PINTADAS
ENSAMBLE CHOPPER
LLANTAS
LINEA FINAL


ANSELMO-225
RAUL-224
AMADOR
SERVICIO
LIZ-218
VICENTE-712
ROCIO-219
CECILIA-215
IMPLEMENTOS
HERRERA-711
ELIAS-714
JUAN-713
ARTURO-24
CONCENTRADOR
7

VI. CAPACIDAD

DE EXPANSIÓN

DE LA RED

CAPACIDADES DE EXPANSION DE LA RED

No se tiene estimada la capacidad de expansión de la red, debido a que al momento de la implantación de la red no se llevó a cabo un cableado estructurado, ya que se implementó una red pequeña en el departamento de ingeniería con un servidor y cinco estaciones de trabajo, y de ahí se han realizado las implementaciones en los demás departamentos conectando más terminales y servidores.

En la actualidad se cuenta con cinco servidores y 80 terminales conectadas a la red, pero en realidad sólo están funcionando tres servidores y los otros dos servidores se utilizan para pruebas.

Desde mi punto de vista, sería recomendable utilizar los cinco servidores, para evitar tanto tráfico en la red, y de acuerdo a la división de grupos de trabajo que ya se tienen establecer qué, grupos se envían a procesar a cuál servidor.

Además, se instalaran también más servidores de impresión, ya que sólo existe una impresora a la que se envían los reportes de todas las terminales, y ,esto por consecuencia es demasiado lento.

Se cuenta con un excelente equipo de impresión, pero sólo es utilizado en forma independiente dentro de los departamentos; una opción podría ser que hubiera un servidor de impresión por cada departamento o grupo de trabajo y que se tomar también en cuenta que de cualquier otro grupo o departamento que estén relacionados enviar reportes que se requieran de un grupo a otro.

VII. CICLO DE VIDA

ESPERADO

CICLO DE VIDA ESPERADO.

No se tiene un determinado ciclo de vida, porque se implementó y se diseño de acuerdo a las necesidades actuales y futuras de la empresa, pero cada adición de la red o modificación se planea para futuro, por esta razón no tiene un determinado ciclo de vida.

En la actualidad, se ha estado realizando la adquisición de equipo de cómputo, que se piensa implementar a la red, de tal manera que queden 104 terminales conectadas a red.

VIII. AMBIENTE

Y

SOPORTE

DE

APLICACIONES

AMBIENTE Y SOPORTE DE APLICACIONES

PAQUETE	VER.	DESCRIPCION
VISIO	3.0	DISEÑO
VISUAL BASIC	STANDAR	MANEJADOR DE BASE DE DATOS
VSAT PRESENTATION		
WIN FAXLITE/DOS FAXLITE	3.0	COMUNICACION
WINDOWS	3.1	SISTEMA OPERATIVO
WINDOWS	3.1	SISTEMA OPERATIVO
WINDOWS	3.0	SISTEMA OPERATIVO
WINDOWS 3.1 PARA HP VECTRA	F.00.00	SISTEMA OPERATIVO
WINDOWS 95		SISTEMA OPERATIVO
WINDOWS FOR GROUP	3.1	SISTEMA OPERATIVO
WINDOWS NT		SISTEMA OPERATIVO
WINDOWS NT		SISTEMA OPERATIVO
WINDOWS TRABAJO EN GRUPO	3.11	SISTEMA OPERATIVO
WINDOWS TRABAJO EN GRUPO	3.11	SISTEMA OPERATIVO
WINDOWS TRABAJO EN GRUPO	3.11	SISTEMA OPERATIVO
WINDOWS TRABAJO EN GRUPO	3.1	SISTEMA OPERATIVO
WORD	6.0	PROCESADOR DE TEXTO
WORD	2.0	PROCESADOR DE TEXTO
WORD	2.0	PROCESADOR DE TEXTO
WORD	2.0	PROCESADOR DE TEXTO
WORD	2.0	PROCESADOR DE TEXTO
WORD	2.0	PROCESADOR DE TEXTO
WORKS FOR WINDOWS		PROCESADOR/B.D./HOJA C.
XVISION	5.0	ANIMACION

AMBIENTE Y SOPORTE DE APLICACIONES

PAQUETE	VER.	DESCRIPCION
PROGRESS BATCH 10	6.2G07	PROGRAMACION
PRJECT FOR WINDOWS	3.0	TRABAJOS
PRJECT FOR WINDOWS	3.0	PROYECTOS
PUBLISHER	2.0	DISEÑO/DIBUJO
SCANAT		VACUNA
SCO		SISTEMA OPERATIVO
SCO	3.0	SISTEMA OPERATIVO
SCO UNIX SYSTEM V/386 (INSTALACION)	3.2V2.0S	SISTEMA OPERATIVO
SCO UNIX SYSTEM V/386	3.2V2.0S	SISTEMA OPERATIVO
SCO UNIX SYSTEM V/386	3.2V2.0N	SISTEMA OPERATIVO
SCO UNIX V/386 (UTILIDADES EXTENDIDAS)	3.2V2.0N	SISTEMA OPERATIVO
SCO UNIX VARIOS	3.2.4	SISTEMA OPERATIVO
SECRET WEAPON OF THE LUFTWARE		GAMES
SHERLOCK HOLMES	1.0	GAMES
SISTEMA OPERATIVO DR DOS	5.0	SISTEMA OPERATIVO
SMART CAM	7.59	DISEÑO INGENIERIA
SMART CAM	4.00	DISEÑO
SMART CAM	4.10	DISEÑO
SMC CONTROLADOR DE TARJETA		CONTROLADOR TARJETA
SOUND BLASTER		CONTROLADOR COMPAC DISK
TCP-IP FOR DOS		PROTOCOLO DE COMUNICACION
TEXAS INSTRUMENTS TRAVELMATE		CONTROLADOR
TEXAS INSTRUMENTS TRAVELMATE		CONTROLADOR
THE GRAPHICS GALLERY (GALLERY UTILITY DISC)	B.03.00	DISEÑO

AMBIENTE Y SOPORTE DE APLICACIONES

PAQUETE	VER.	DESCRIPCION
NOVELL NETWARE 4 (UPGRADE) DOCUMENTACION		SISTEMA OPERATIVO
OFFICE	4.2	APLICACIONES
OFFICE	4.2	APLICACIONES
OFFICE	4.2	APLICACIONES
OFFICE 95	WIN 95	APLICACIONES
OKIDATA SOFTWARE SUPPORT	1.0	CONTROLADOR
OMNIPAGE PROFESIONAL	2.0	DIBUJO/DISEÑO
OMNIPAGE PROFESIONAL	2.11	DIBUJO/DISEÑO
OMNIPAGE PROFESIONAL	5.0	DIBUJO/DISEÑO
OMNIPAGE PROGRAM	3.10	DIBUJO/DISEÑO
PATHWAY FROM WOLLONGONG	2.0	CONTROLADOR RED
PATHWAY FROM WOLLONGONG (CLIEN NFS)	2.0	COMUNICACION
PATHWAY FROM WOLLONGONG PACK	1.0	COMUNICACION
PCTOOLS	5.0	HERRAMIENTA
POWER PAC	2.19P16	DEMO
POWER POINT	3.0	PROCESADOR GRAFICO
POWER POINT	3.1	PROCESADOR TEXTO / GRAFICO
POWER POINT PRESENTATION		APLICACION
PROGRESS	V7.3D	MANEJADOR DE B.D.
PRESUPUESTO 1995 (XLS)		RESPALDO
PRESUPUESTO GASTOS ´95 (SISTEMAS)		RESPALDO
PROGRESS	7.2A	MANEJADOR DE BASE DE DATOS
PROGRESS	7.2D	MANEJADOR DE BASE DE DATOS
PROGRESS	7.2D01/6.2B	MANEJADOR DE BASE DE DATOS

AMBIENTE Y SOPORTE DE APLICACIONES		
PAQUETE	**VER.**	**DESCRIPCION**
MFG PRO	8.3	SOPORTE/SISTEMA
MFG PRO GUI	0.0	PRESENTACION EN POWER POINT
MICROTECHNET	feb-94	INFORMACION
MICROTECHNET	oct-94	INFORMACION
MICROTECHNET	jun-94	INFORMACION
MICROTECHNET	sep-94	INFORMACION
MICROTECHNET	nov-94	INFORMACION
MICROTECHNET	jul-94	INFORMACION
MICROTECHNET	abr-94	INFORMACION
MODEM 16550 SUPPORT		CONTROLADORES
MOUNTAIN FIKETALK	1.12	SOFT. RESPALDO
MOUNTAIN FILESAFE	5.3.2SCSI	SOFT. RESPALDO
MOUSE	9.0	APLICACIONES
MOUSE	9.0	APLICACIONES
MOUSE DRIVER		APLICACIONES
MULTITECH MULTIEXPRESS FOR WINDOWS	2.1	SOFTWARE DE COMUNICACION
NETWARE 4.1 UPGRADE LICENSE 10 USERS/REGISTER	NOVEL 4.1	REGISTROS
NETWARE BOOTDISK ESPAÑOL	NOVEL 4.1	CONTROLADOR
NETWARE CLIENT FOR DOS/WINDOWS	NOVEL 4.1	CONTROLADOR
NETWARE CLIENT FOR DOS/WIN.AND BOOT DISK	4.1 COPIA	ANIMACION
NETWARE NOVELL	3.11	REDES
NOI	4.21	CONTABILIDAD
NOMIPAQ	3.0	CONTABILIDAD
NOVELL NETWARE	3.11	SISTEMA OPERATIVO

AMBIENTE Y SOPORTE DE APLICACIONES		
PAQUETE	**VER.**	**DESCRIPCION**
HP PAINTJET		INSTALACION/CONTROLADOR
HP PAINTJET XL 300/DESKJET 1200C	3.0/3.1	CONTROLADORES
HP SCANJET IIC (SCANNER) (DESKCAN II)	A.01.01	CONTROLADOR
HP SUPPORT		SOPORTE
HP SUPPORT ASSISTENT	AGUS93	INFORMACION
HP VARIOS		
IFPS / PERSONAL	2.5	COMUNICACION
INDIANAPOLIS 500 (SIMULACION)	1989.0	ANIMACION
INFONET		DEMO
INTEL ETHER EXPRES LAN ADAPTER DRIVER		CONTROLADOR DE RED
INTEL FAXMODEM		CONTROLADOR MODEM
INTEL COPROCESADOR MATEMATICO	SX	COPROCESADOR
LAPLINK	3.0	ADMINISTRADOR DE SOFTWARE
LAPLINK	5.0	CONTROLADOR DE SOFTWARE
LAPLINK III	3.0	COMUNICACION
LAPLINK V	5.0	COMUNICACION
LOTUS 1-2-3	2.01	CONTABILIDAD
LOTUS 1-2-3 FOR WINDOWS	1.1	MANEJADOR DE B.D.
LOTUS AMIPRO	3.0	PROCESADOR DE TEXTO
LOTUS FREELANCE GRAPHICS	2.0	CONTABILIDAD
LOTUS ORGANIZER	0.0	DEMO/ORGANIZADOR AGENDA
MCAFEE ASSOCIATES		VACUNA
MFG PRO	7.2	SERVIDOR/SISTEMA
MFG PRO	7.1C	SERVIDOR/SISTEMA

AMBIENTE Y SOPORTE DE APLICACIONES

PAQUETE	VER.	DESCRIPCION
CAF	1.2	CONTABILIDAD
CNET ETHERNOTIC NETWARE DRIVE	2.6	CONTROLADOR RED
COLORADO CBACKUP FOR WINDOWS	2.7	SOPORTE PARA BACKUP
COMPUSERVE	1.3.1	COMUNICACION
CONPAQ	1.0	CONTABILIDAD
COREL DAW!	4.0	DISEÑO
COREL DAW!	4.0	DISEÑO/DIBUJO
COREL DAW!	5.0	DISEÑO
CORELFLOW		DISEÑO/ANIMACION
CROSTALK COMMUNICATOR	2.0	DEMO
DASHBOARD		ADMINISTRADOR DE TRABAJOS
DATA EASE (PHOENIX)	4.2	COMPRAS
DESKCAN II (SCANJET IIC)	A.01.01	CONTROLADOR DEL SCAN DISK
DESKCAN II (SCANJET IIC) SCANNER	A.01.01	SCANER
DIRECTORIO CANACINTRA 1996	4.0	
DISCOS DE ARRANQUE (COMPAQ, QS, 486U/33, QS/RS)		
DOS	6.2	SISTEMA OPERATIVO
DOS	6.2 ACTUAL	SISTEMA OPERATIVO
DOS	V6.0 ACER	SISTEMA OPERATIVO
DOS	5.0	SISTEMA OPERATIVO
DOS	6.22	SISTEMA OPERATIVO
DRIVERS PLOTTER CAL-COM (INGENIERIA)	5.0/4.1	CONTROLADOR DE PLOTTER
ENCYCLOPEDY		INFORMACION
EPSON DRIVERSDISK	1.03E	CONTROLADOR DE IMPRESORA

AMBIENTE Y SOPORTE DE APLICACIONES		
PAQUETE	**VER.**	**DESCRIPCION**
EPSON STYLUS 800+	3.1	CONTROLADOR DE IMPRESORA
EPSON STYLUS COLOR		CONTROLADOR DE IMPRESORA
EXCEL FOR WINDOWS	4.0	PROCESADOR GRAFICO
EXCEL FOR WINDOWS	5.0	PROCESADOR GRAFICO
EXCEL FOR WINDOWS	4.0	PROCESADOR GRAFICO
EXCEL FOR WINDOWS	4.0	PROCESADOR GRAFICO
EXPERT FORMS FOR WINDOWS		DISEÑO DE FORMAS
EXSORCISTA ANTIVIRUS NATAS		VACUNA
FAXLAN		CONTROLADOR DE FAX
FOXPRO	2.5	MANEJADOR DE BASE DE D.
FOXPRO	2.6	MANEJADOR DE BASE DE D.
FOXPRO 6 PACK	2.0	MANEJADOR DE BASE DE D.
FOXPRO FOR DOS	2.0	MANEJADOR DE BASE DE D.
FOXPRO FOR WINDOS	2.5	MANEJADOR DE BASE DE D.
FOXPRO 6 PACK/KIT	2.0	MANEJADOR DE BASE DE D.
HARVARD GRAPHICS	1.02	DIBUJO/DISEÑO
HARVARD GRAPHICS	3.0	DIBUJO/DISEÑO
HARVARD GRAPHICS FOR WINDOWS	2.0	DISEÑO
HP DESKJET 1200/HP PAINTJET XL300		DISCO INSTALACION DE IMP.
HP DESKJET 600 Y 660C		DISCO INSTALACION DE IMP.
HP DESKJET SERIE (varios)	3.0	INSTALACION DE SOFTWARE
HP LASERJET 4	4.0	CONTROLADOR IMPRESORA
HP LASERJET 4 PLUS	4PLUS	CONTROLADOR IMPRESION
HP NETSERVER LMSERIES	F.10.00	COMUNICACION

AMBIENTE Y SOPORTE DE APLICACIONES

PAQUETE	VER.	DESCRIPCION
3 Com ETHERDISK	4.2	DRIVER TARJETAS
ACCESS FOR WINDOWS		MANEJADOR DE B.D.
ACCESS	1.0	MANEJADOR DE B.D.
ACER UTILITIES	1.32	CONF. B.D.
ALDUS PAGEMAKER	5.0	DISEÑO
ALDUS PHOTOSTYLER SE	2.0	DISEÑO
AMEIRCA ONLINE FOR WINDOWS	1.0	COMUNICACION
AM-WORKFLOW	2.0	DEMO/ADMON. DIBUJOS
AM-WORKFLOW FOR WINDOWS	4.01	ADMINISTRADOR DE DIBUJOS
AUREX CVS/CVP	96	VACUNAS
AUTOCAD	12I	DISEÑO
AUTOCAD	12I	DISEÑO/ANIMACION
AUTOCAD 12	12I	DISEÑO INGENIERIA
AUTOCAD 12	12I	DISEÑO
AUTOCAD ADI DRIVER PLOTTER	4.1	PLOTTER/DISEÑO TECNICO
AUTOCAD BONUS		INFORMACION
AUTOCAD LT FOR WINDOWS		DISEÑO
AUTODESK	3.0	
AUTODESK MULTIMEDIA EXPLORER	1.0	DISEÑO/ANIMACION
AUTODESK MULTIMEDIA EXPLORER	1.0	MULTIMRDIA
AUTODISK ANIMATOR PRO	1.3	ANIMACION
AUTOMANAGER WORKFLOW MSDOS/WIN	4.01	ADM. DIBUJOS AUTOCAD
BANCO	1.2	CONTABILIDAD

IX. AMBIENTE

DE

ADMINISTRACIÓN

DE

LA RED

AMBIENTE DE ADMINISTRACION DE LA RED

USUARIO	DEPARTAMENTO	CAP. D.D	SOFTWARE UTILIZADO. BASICO, PATWAY WINDOWS 3.1 Y OFICE
Enrique O.	Logística	370	DOS,BASICO
Ignacio R.	Sistemas	1 Gb	DOS, BASICO, SOFTWARE DE COMUNICACIONES, PROGRESS, PROYECT
Lidia G.	Sistemas	630	BASICO, VISIO, AUTOCAD LT
Oscar O.	Sistemas	630.5	PROYECT, COREL 5, COMUNICACIONES, WINDOWS 95, CONTROLADOR DE CD., EXPLORER, VISIO
Olivia R.	Logística	630	INTERNET, PITEX,BASICO, AUTOCAD, COMUNICACIONES, WINDOWS95, CHAMALEON
Marlyn	Logistica	117.1	BASICO
Mary S.	Sistemas	630.5	BASICO
Vicky/Sarahi	Rec. Hum.	170	BASICO
José Manuel	Compras	84.7	BASICO
Alejandra L.	Caja	116	BASICO
Sergio A.	Sistemas	360.5	BASICO, EXPLORER, VISIO, AUTOCAD, COREL, EXPLORER, WINDOWS95, PUBLICER
Fernando D.	Rec. Humanos	630	BASICO, FOXPRO 2.5
Moisés G.	Rec. Hum.	121.8	BASICO
José Gpe. P.	Sistemas	630.5	BASICO, PUBLICER, FOXPRO, DESKCAN
Betty C.	Logística	630.5	BASICO
Lupita A.	Rec. Hum.	84.7	BASICO
Elias S.	Refacciones	630.5	BASICO, COREL
Tomás R.	Compras	340	BASICO
Vicente S.	Refacciones	630	BASICO, COREL
Eduardo	Refacciones	230	BASICO, COREL
Antonio C.	Rec. Hum.	470	BASICO
Salvador	Calidad	520	BASICO
Rocío	Refacciones	84	BASICO, COREL

AMBIENTE DE ADMINISTRACION DE LA RED

USUARIO	DEPARTAMENTO	CAP. D.D	SOFTWARE UTILIZADO. BASICO: PATWAY WINDOWS 3.1 Y OFICE
Enrique O.	Logística	370	DOS,BASICO
Ignacio R.	Sistemas	1 Gb	DOS, BASICO, SOFTWARE DE COMUNICACIONES, PROGRESS, PROYECT
Lidia G.	Sistemas	630	BASICO, VISIO, AUTOCAD LT
Oscar O.	Sistemas	630.5	PROYECT, COREL 5, COMUNICACIONES, WINDOWS 95, CONTROLADOR DE CD., EXPLORER, VISIO
Olivia R.	Logística	630	INTERNET, PITEX,BASICO, AUTOCAD, COMUNICACIONES, WINDOWS95, CHAMALEON
Marlyn	Logistica	117.1	BASICO
Mary S.	Sistemas	630.5	BASICO
Vicky/Sarahi	Rec. Hum.	170	BASICO
José Manuel	Compras	84.7	BASICO
Alejandra L.	Caja	116	BASICO
Sergio A.	Sistemas	360.5	BASICO, EXPLORER, VISIO, AUTOCAD, COREL, EXPLORER, WINDOWS95, PUBLICER
Fernando D.	Rec. Humanos	630	BASICO, FOXPRO 2.5
Moisés G.	Rec. Hum.	121.8	BASICO
José Gpe. P.	Sistemas	630.5	BASICO, PUBLICER, FOXPRO, DESKCAN
Betty C.	Logística	630.5	BASICO
Lupita A.	Rec. Hum.	84.7	BASICO
Elias S.	Refacciones	630.5	BASICO, COREL
Tomás R.	Compras	340	BASICO
Vicente S.	Refacciones	630	BASICO, COREL
Eduardo	Refacciones	230	BASICO, COREL
Antonio C.	Rec. Hum.	470	BASICO
Salvador	Calidad	520	BASICO
Rocío	Refacciones	84	BASICO, COREL

AMBIENTE DE ADMINISTRACION DE LA RED

USUARIO	DEPARTAMENTO	CAP. D.D	SOFTWARE UTILIZADO. BASICO PATWAY WINDOWS 3.1 Y OFICE
Mary M.	Compras	630	BASICO
Francisco M.	Pre-pintura		
Jesús R.	Linea final		
Angelina L.	Costos	84.7	BASICO
Paty R.	Contabilidad	84.7	BASICO, CONPAQ,BANCO,CAF,LOTUS
Apolinar H.	Dir. Operación	425.5	BASICO
Tranquilino B.	Logística	630.5	BASICO
J.J. Braham	Dir. Finanzas	631.5	BASICO,LOTUS FOR WINDOWS
Florencio T.	Crédito y Cobranza	52	BASICO,LOTUS
Raymundo G.	Contabilidad	425	BASICO, CONPAQ,BANCO,CAF,LOTUS
Francisco M.	Calidad Integral	540	BASICO
Uso Común	Ingeniería	427	BASICO,COREL, AUTOCAD
Esteban T.	Sistemas	630.5	BASICO, PUBLICER, FOXPRO, DESKCAN
Joseé A.	Ingeniería	427	BASICO,COREL, AUTOCAD
Rogelio M.	Ingeniería	427	BASICO,COREL, AUTOCAD
Consulta	Ingeniería	41.8	BASICO,COREL, AUTOCAD
Lupita R.	Planeación	52	BASICO
Antonio M.	Rec. Humanos	630	BASICO
Consulta	Ingeniería	408	BASICO,COREL, AUTOCAD
Juan 2	Compras	345	BASICO
Yiura L.	Compras	84.7	BASICO
Eduardo V.	Compras	52	BASICO
Ma. Gpe. L.	Manufactura	120	BASICO

AMBIENTE DE ADMINISTRACION DE LA RED

USUARIO	DEPARTAMENTO	CAP. D.D	SOFTWARE UTILIZADO. BASICO, PATWAY, WINDOWS 3.1 Y OFICE						
Gustavo H.	Contabilidad	84.7	BASICO, CONPAQ,BANCO,CAF,LOTUS, NOMIPAQ						
Alejandro M.	Contabilidad	520	BASICO, CONPAQ,BANCO,CAF,LOTUS, NOMIPAQ						
José Luis L.	Contabilidad	630.5	BASICO, CONPAQ,BANCO,CAF,LOTUS, NOMIPAQ						
Felisa E.	Contabilidad	300	BASICO, CONPAQ,BANCO,CAF,LOTUS, NOMIPAQ						
Sergio U.	Crédito y Cobranza	427.3	BASICO						
Diana O.	Compras	630	BASICO						
Carlo M.	Dir. general								
Monserrat	Planeación	260	BASICO						
Joaquin N.	Costos	520	BASICO,LOTUS						
Gerardo R.	Impuestos	212	BASICO						
Juana	Logística	84.7	BASICO						
Miguel	Logística	170.45	BASICO						
Francisco P.	Logistica	84.75	BASICO						
Martha R.	Logística	345	BASICO						
Martha O.	Dir. Rec. Hum.	84.7	BASICO						
Lorena V.	Dir. general	84.7	BASICO						
Usuario 2	Sala Capacitación	84.7	BASICO						
Usuario 4	Sala capacitación	84.7	BASICO						
Usuario 1	Sala capacitación	84.7	BASICO						
Usuario 3	Sala Capacitación	84.7	BASICO						
Usuario 5	Sala Capacitación	151.1	BASICO						
Mario C.	Manufactura	630	BASICO						
Juan C.	Dir. Rec.Hum.	213	BASICO						

AMBIENTE DE ADMINISTRACION DE LARED

USUARIO	DEPARTAMENTO	CAP. D.D	SOFTWARE UTILIZADO. BASICO PATWAY WINDOWS 3.1 Y OFICE						
Edwin F.	Ingeniería	290	BASICO,COREL, AUTOCAD						
José Luis P.	Ingeniería	630	BASICO,COREL, AUTOCAD						
Orlando	Manufactura								
Abel M.	Ingeniería	630	BASICO,COREL, AUTOCAD						
Juvenal	Ingeniería	630	BASICO,COREL, AUTOCAD						
Fidel A.	Ingeniería	630	BASICO,COREL, AUTOCAD						
Mario O.	Ingeniería	630	BASICO,COREL, AUTOCAD						
Humberto M.	Manufactura	630	BASICO						
Enrique M.	Refacciones	299	BASICO						
Dalia	Tráfico	52	BASICO						
Elia H.	Calidad	543.7	BASICO						
Brenda	Publicidad	1 Gb	BASICO						

X. PROBLEMAS

POTENCIALES,

RIESGOS

PROBLEMAS POTENCIALES, RIESGOS

SEGURIDAD LÓGICA Y CONFIDENCIAL.

Los problemas más comunes que suelen ocurrir en el mundo de las redes locales, cuando no se cuenta con una red eficiente y confiable, se mencionan a continuación.

ROBOS, FRAUDES O SABOTAJES.

Las computadoras son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

La computadora ha modificado las circunstancias tradicionales del crimen; muestra de ello son los fraudes, falsificaciones y venta de información hechos a las computadoras o por medio de computadoras.

Los sistemas de seguridad normalmente no consideren la posibilidad de fraude cometida por los empleados en el desarrollo de sus funciones. La introducción de información confidencial a la computadora puede provocar que esté concentrada en las manos de unas cuantas personas y una alta dependencia en caso de pérdida de los registros.

VIRUS.

En la actualidad, se ha dado el factor a considerar, llamado: "virus" de las computadoras, el cual, aunque tiene diferentes intensiones, se encuentra principalmente para paquetes copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.

Se trata de pequeñas subrutinas escondidas en los programas que se activan cuando se cumple alguna condición; por ejemplo, haber obtenido una copia en forma

ilegal, y puede ejecutarse en una fecha o situación predeterminada. El virus normalmente lo ponen los diseñadores de algún tipo de programa (software) para "castigar" a quienes lo roban o copian sin autorización o bien por alguna actitud de venganza en contra de la organización.

Al auditar los sistemas, se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarse en red con otras computadoras, no exista la posibilidad de transmisión de virus.

Los motivos de los delitos por computadora normalmente son por:

- Beneficio personal.

- Beneficios de la organización.

- Síndrome de Robin Hood (por beneficiar a otras personas)

-Jugando a jugar

- Fácil desfalcar

- El departamento es deshonesto.

- Odio a la organización (revancha)

- El individuo tiene problemas financieros.

- La computadora no tiene sentimientos ni delata.

- Equivocación de ego (deseo de sobresalir de alguna forma)

- Mentalidad turbada.

Se considera que hay 4 factores que han permitido el incremento en los crímenes por computadora, estos son:

1. El aumento del número de personas que se encuentran estudiando computación.

2. El aumento del número de empleados que tienen acceso a los equipos.

3. La facilidad del uso de los equipos de cómputo.

4. El incremento en la concentración del número de aplicaciones y, consecuentemente, de la información.

En la actualidad las compañías cuentan con grandes dispositivos de seguridad física de las computadoras y se tiene la idea que los sistemas no pueden ser violados si no se entra al centro de cómputo, olvidándose del uso de terminales y de sistemas remotos de teleproceso.

El tipo de seguridad puede comenzar desde la simple llave de acceso (contraseña o password) hasta, sistemas más complicados, pero se debe evaluar que, cuando más complicados sean los dispositivos de seguridad, resultan más costosos. Por lo tanto, se debe mantener una adecuada relación de seguridad-costo de los sistemas de información.

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

El sistema integral de seguridad debe comprender:

Elementos administrativos.

Definición de una política de seguridad.

Organización y división de responsabilidades.

Seguridad física y contra catástrofes (incendio, terremoto, etc.)

Prácticas de seguridad del personal.

Pólizas de seguros.

Elementos técnicos y procedimientos.

Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales).

Aplicación de los sistemas de seguridad, incluyendo datos y archivos.

El papel de los auditores, tanto internos como externos.

Planeación de programas de desastre y prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, *para lo cual se debe considerar lo siguiente:*

Clasificar la instalación en términos de riesgo (alto, mediano y pequeño).

Identificar aquellas aplicaciones que tengan alto riesgo.

Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con alto riesgo.

Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.

La justificación del costo de implantar las medidas de seguridad.

Para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo debemos preguntarnos lo siguiente:

¿Qué sucedería si no se puede usar el sistema?
Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riesgo.

La siguiente pregunta es: ¿Qué implicaciones tiene el que no se obtenga el sistema y cuánto tiempo podríamos estar sin utilizando?

¿Existe un procedimiento alterno y qué problemas nos ocasionaría?

¿Qué se ha hecho en caso de emergencia?

Para clasificar la instalación en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.

- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien que pueda provocar un gran impacto en la toma de decisiones.

- Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para clasificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- Especificar la aplicación, los programas y archivos.

- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.

- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.

En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de organización.

1. El personal que prepara la información no debe tener acceso a la operación.

2. Los analistas y programadores no deben tener acceso al área de operación y viceversa.

3. Los operadores no deben tener acceso irrestringido a las librerías a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.

4. Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar Sistemas de Seguridad, puede reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

SEGURIDAD EN EL PERSONAL.

Un buen centro de cómputo depende, en gran medida, de la integridad, estabilidad y lealtad de personal, por lo que al momento de reclutarlo es conveniente hacerle exámenes psicológicos, médicos y tener muy en cuenta sus antecedentes de trabajo.

En los equipos de cómputo es normal que se trabajen horas extras, con gran presión y que no haya una adecuada política de vacaciones debido a la independencia que se tiene con algunas personas, lo cual va haciendo que se crean "indispensables", que son muy difíciles de sustituir y que ponen en gran riesgo la organización. Se debe verificar que existan adecuadas políticas de vacaciones y de reemplazo.

También se deben tener políticas de rotación del personal que disminuya la posibilidad de fraude, ya que un empleado puede estar haciendo otra actividad en un mes y sería muy arriesgado cometer un fraude, sabiendo que la nueva persona que esté en su lugar puede detectarlo fácilmente.

SEGURIDAD FÍSICA.

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundación, huelgas, disturbios, sabotaje, etc. y continuar en un medio de emergencia hasta que sea restaurado el servicio por completo.

Entre las precauciones que se deben revisar están:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas de polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.

- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.

- En cuanto a los extintores, se debe revisar en número de éstos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.

- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.

- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.

- Los materiales más peligrosos son las cintas magnéticas que, al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

SEGUROS.

Los seguros de los equipos en algunas ocasiones se dejan en segundo término aunque son de gran importancia.

El seguro debe cubrir todo el equipo y su instalación, por lo que es probable que una sola póliza no pueda cubrir todo el equipo con las diferentes características, por lo que tal vez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

El seguro debe cubrir daños causados por factores externos (terremoto, inundación, etc.) como por factores internos (daños ocasionados por negligencia de los operadores, daños debidos al aire acondicionado, etc).

También debe asegurar la pérdida de software (programas), de la información, de los equipos y el costo de recuperación de lo anterior.

SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO.

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes **medidas**:

1. Se debe restringir el acceso a los programas y a los archivos.

2. Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.

3. Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.

4. No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.

5. En los casos de información confidencial debe usarse , de ser posible, en forma codificada o criptografiada.

6. Se debe realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.

7. Se debe monitorear periódicamente el uso que se les está dando a las terminales.

8. Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

9. El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.

10. Debe existir una perfecta división de responsabilidades entre los capturistas de datos y los operadores de computadoras, y entre los operadores y las personas responsables de las librerías.

11. Deben existir registros que reflejen la transferencia de información entre las diferentes funciones de un sistema.

12. Debe controlarse la distribución de las salidas (reportes, cintas, etc.).

13. Se deben guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad, por ejemplos: los bancos.

14. Se debe tener un estricto control sobre el transporte de discos y cintas de la sala de cómputo al local de almacenaje distante.

15. Se deben identificar y controlar perfectamente los archivos.

16. Se debe tener estricto control sobre el acceso físico a los archivos.

17. En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema y versión. Esto nos servirá para identificar el número de veces que se ha compilado o corrido un programa, y nos permitirá costear en el momento que se encuentre un sistema en producción.

XI. PLANES

DE

CONTINGENCIA

PLANES DE CONTINGENCIA

Los problemas más comunes son el tráfico y el no tener software de monitoreo de red.

Su plan de contingencia es: dividir o segmentar en miniredes la red, esto es para no tener cuellos de botella, también estar lo más actualizado en software de monitoreo de red para detectar los cuellos de botella y las posibles colisiones dentro del sistema.

Algo recomendable para la empresa, es que se realice un plan de contingencia, que se revice, y se de a conocer a los usuarios, para que sepan qué hacer en caso de siniestro. A continuación, describiré una forma facible para llevarlo a cabo:

SEGURIDAD AL RESTAURAR EL EQUIPO

Cuando ocurra una contingencia, es esencial, que se conozca al detalle el motivo que la origino y el daño causado, lo que permitir recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable; y es necesario analizar y extender estos factores para establecer los procedimientos que permitan eliminarlos al máximo y, en caso que ocurran, poder reparar el daño y reanudar la operación lo mas rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

* En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.

* Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.

* El procedimiento anterior complementado con un registro de las transacciones que afectaron los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo y a partir de el reanudar el proceso.

* Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.

* Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Además de los procedimientos de recuperación y reinicio de la información, de deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falla de corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de computo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

Con frecuencia un problema en algún programa, un error de datos, un error de operación o una falla del equipo hacen que una corrida en la maquina aborte antes de terminar el proceso.

El objetivo del siguiente cuestionario es evaluar los procedimientos y repetición de procesos en el sistema de procedimientos relativos al centro de cómputo:

1. ¨ Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?

SI ( ) NO ( )

2. Enuncie los procedimientos mencionados en el inciso anterior

---

3. ¨ Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?

SI ( ) NO ( )

En el momento en que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:

1. Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.

2. los nuevos sistemas deben estar adecuadamente documentados y probados.

3. Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

Los datos de entrada deben de estar debidamente probados y verificados contra la entrada de datos durante el procesamiento. Uno de los fraudes mas comunes se comete durante el periodo en el cual ya se obtuvieron las cifras de control pero no se han emitido los reportes definitivos; por ejemplo, la obtención de cheques. Esto se puede hacer si es que se permite que se metan datos en el periodo previo a la obtención de los reportes definitivos, y si no se tiene control sobre estos datos introducidos posteriormente a las cifras de control.

PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE

Se debe establecer en cada dirección de informática un plan de emergencia, el cual ha de ser probado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia se tenga la seguridad que funcionara.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se han de utilizar respaldos (posiblemente en otras instituciones). Hay que cambiar la configuración y, posiblemente se tengan que usar algunos métodos manuales, no sólo simulando un ambiente ficticio cercano a la realidad sino considerando que la emergencia existe.

El plan de emergencia, una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerar como confidencial o de acceso restringido.

Para la preparación del plan se seleccionara el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática (por ejemplo, el jefe de operación, el jefe de análisis y programación y de auditoria interna). Cada uno de ellos debe tener tareas especificas como la operación del equipo de respaldo, la interfaz administrativa, de logística; por ejemplo, el proporcionar los archivos necesarios para el funcionamiento adecuado. Cada miembro del grupo debe tener asignada su tarea con una persona de respaldo para cada uno de ellos. Se deber elaborar un directorio que contenga los nombres, direcciones y números telefónicos.

Los desastres que pueden suceder podemos clasificarlos así:

a) Completa destrucción del centro de cómputo.
b) Destrucción parcial del centro de cómputo.
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire acondicionado, etc.).
d) Destrucción parcial o total de los equipos descentralizados.
e) Pérdida total o parcial de información, manuales o documentación.
f) Pérdida del personal clave.
g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

* La documentación de programación y de operación de los equipos.
* El equipo completo.
* El ambiente de los equipos.
* Datos y archivos.
* Papelería y equipo accesorio.
* Sistemas (sistemas operativos, bases de datos, programas de utilería, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estar en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deber :

* Asegurar que todos los miembros sean notificados.
* Informar al director de informática.
* Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que, parte del plan debe ser activada.
* Determinar el estado de todos los sistemas en proceso.
* Notificar a los proveedores del equipo cuál fue el daño.
* Establecer la estrategia para llevar a cabo las operaciones de emergencia tomando en cuenta:

- Elaboración de una lista con los m,todos disponibles para realizar la recuperación.

- Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustitución de procesos en línea por procesos en lote).

- Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.

- Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deber reducir la carga de procesos, analizando alternativas como:

* Posponer las aplicaciones de prioridad baja.

* Cambiar la frecuencia del proceso de trabajos.

* Suspender las aplicaciones en desarrollo.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc., a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de proceso, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.

- Se debe tener documentados los cambios de software.

- En caso de respaldo en otras instituciones, previamente se deber conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.

- Configuración de equipo de captación de datos.

- Sistemas operativos.

- Configuración de equipos periféricos.

Finalmente se deber estudiar que se tenga una lista de los requerimientos mínimos que deben tener para un efectivo plan de recuperación en caso de desastre.

Lo más importante es identificar el número y tipo de componentes esenciales que puedan ser críticos en caso de emergencia o de desastre.

I. Equipo principal (equipo, canales de comunicación, memoria, etc.)

Equipo fabricante	Proyecto en el equipo	¿ Es esencial para procesar?

II. Unidades de disco (incluyendo controladores, número de unidades, paquetes de discos, número de discos por paquete).

Fabricante	Número de unidades	Capacidad	Proyectos el q' se usa	¿Es esencial p' procesar?

III. Unidades de cinta.

IV. Unidades de almacenamiento (en línea o fuera de línea).

V. Equipo periféfico (lectoras, impresoras, etc.).

VI. Unidades de comunicación, controladores.

Equipo	Número de equipo conectado	Proyecto en el que se usa	¿Es esencial para procesar?

VII. Sistemas operativos.

VIII. Terminales.

Equipo	Unidad/ modelo	Localización	Proyectos en el que se usa	¿Es esencial para procesar?

IX. Equipo adicional

Electricidad KVA
Aire acondicionado BTU
Temperatura requerida
Humedad requerida

RED DE COMUNICACIÓN

1. Descripción de la red de comunicación.

1. En caso de emergencia, ¿es esencial el uso de la red de comunicación?. Describa el porqué de su respuesta.

2. Programas necesarios para la comunicación.

Identificación de los circuitos	Fabricante	Tipo/ Condición	Bauds velocidad	Protocolo
Ejemplo	A++	C-1	9600	Asíncrono
				Punto final

Servicio Dedicado	Computadora	Interfase Dispositivo	Tipo	Localización
Multipunto	Timeplex mux	Bell z/2	ADDM II	Coyoacán México D.F.

Se debe contar con:

a) Copia de programa de ejecución.

b) Copia de archivos maestros de las aplicaciones clave y sistemas operativos.

c) Copia de la documentación de los sistemas e instructivos de operación.

d) Copia de los archivos necesarios para procesar las transacciones.

e) Inventario de formas especiales utilizadas en la operación normal (se deben incluir también papelería normal, cintas magnéticas, cintas de impresión).

f) Un local con las instalaciones necesarias (energía, aire acondicionado, piso adecuado, etc.).

g) Convenios para el uso de computadoras compatibles.

XII. POLÍTICAS

DE LA RED

POLÍTICAS DE LA RED.

No se cuenta con políticas de la red, a los usuarios sólo se les entrega un reporte de las pantallas a las cuales tiene acceso dentro del Software utilizado == Patway == y si algún usuario requiere acceso de otra pantalla, tiene que llenar un formato de CONTROL DE USUARIOS MFGPRO, que incluye la solicitud de la(s) pantalla(s) a la(s) que se desea acezar, el departamento, quién lo solicita, la fecha, y finalmente la firma del jefe de departamento que da su Visto Bueno.

Pero pese a que no se tienen políticas, si se lleva a cabo un respaldo cada fin de semana, aunque no en toda la red, sino en las aplicaciones de mayor importancia, como por ejemplo NOMINA.

Además, el control de acceso a la red no se tiene restringido, ya que la red tiene acceso las 24 horas y todo el año, debido a que tiene acceso por modem, el cual permite la comunicación con el extranjero, se suspende el servicio sólo cuando se realiza un mantenimiento, que por lo general se realiza en periodos vacacionales para evitar retrasos.

XIII.ACRÓNIMOS

ESTANDARES

ACRÓNIMOS ESTÁNDARES

Conectividad, grupos de trabajo, TCP/IP, OSI, ISO, etc, son términos de uso común para los que se dedican a la conectividad de equipos y redes. Sin embargo, conocerlos todos es una tarea casi imposible. Peor aún cuando muchos de ellos se repiten, ya sea con significados muy parecidos o totalmente diferentes. En este espacio se revisarán algunas definiciones.

Con el avance tecnológico se generan constantemente nuevos términos que los especialistas no terminan de aprender. Lejos están los días en que todo mundo conocía el significado de IBM, NCR y para los de mejor memoria hasta el código hollerit. Ahora primero hay que aclarar a qué fabricante, tecnología arquitectura o topología se hace referencia, debido a la constante repetición de siglas y términos.

Revisemos algunos términos relacionados con la conectividad y redes:

ARCNET: Attached Resourse Computer Network. Es una red Token Bus de 2.5 Mbps desarrollada a finales de los 70's y principios de los 80 por la compañía Datapoint Corporation. Debido a su bajo costo y relativa facilidad de instalación (para la época en que apareció), su uso se extendió ampliamente casi en extinción, en México todavía se encuentran redes de éste tipo, a pesar de su baja velocidad de comunicación.

ARPNET: Red de comunicación de paquetes desarrollada a principios de los 70. Se divide en dos partes interconectadas: Milnet, para uso militar e Internet, para uso comercial y académico. Evolucionó dentro de Internet y el término fue oficialmente retirado en 1990.

ASÍ: Adaptar Support Interface. Especificación para el desarrollo de manejadores de Software, hecho por IBM para proporcionar una interfaz común entre tarjetas Token Ring y las fabricadas por terceros.

AUI: Attachment Unit Interface. Cable de la norma IEEE 802.3 que interconecta al MAV (Media Access Unit) y el dispositivo en red.

BGP: Border Gateway protocol. Protocolo para el intercambio de información de enrutamiento entre dominios.

BNC: Conector empleado para la conexión del cable coaxial en la norma 802.3 10 base 2 a un transceiver.

BROADCAST: Mensaje enviado a todos los nodos de una red.

BUS: Arquitectura lineal de red en la cual las transmisiones de los nodos en la red se mueven por toda la longitud del medio y son recibidas también por las otras estaciones.

CCITT: Consultative Comittee for International Telegraph and Telephone (Comité Consultivo Internacional de telegrafía y Telefonía). Organización Internacional que desarrolla los estándares en comunicaciones.

CIRCUITO VIRTUAL: Tipo de conexión que se comporta como si hubiera una conexión física dedicada entre la fuente y el destino. Empleada en redes de comunicación de paquetes.

COMPUERTA (GATEWAY): Dispositivos que permiten conectar dos redes. Dependiendo del contexto en el que se hable, este dispositivo desarrolla actividades de traductor de protocolos (para conectar dos redes heterogéneas), o para enrutar los paquetes de información entre diferentes segmentos de red.

CONCENTRADOR: en términos generales, es un dispositivo en el que confluye el sistema de cableado para mejorar su distribución, haciéndolo en una topología física de estrella. En algunos tipos de redes, también desempeña funciones especiales o como simple repetidor o divisor de la señal.

CSMA/CA: Carrier Sense Multiple Access / Colisión Avoidance. Protocolo de acceso al medio utilizado en las redes inalámbricas. Se distingue del usado en las redes Ethernet, en que aquí las colisiones son evitadas, en lugar de detectadas.

CSMA/CD: Carrier Sense Multiple Access / Colisión Detection. Es un método de acceso al medio de redes Ethernet. Aquí el cable es accezado por competencia. Una vez que la tarjeta de red sólo escucha la portadora, empieza a trasmitir. En caso de que otro nodo lo intente en forma simultánea, se detecta la colisión y es necesario retransmitir.

DATAGRAMA: Unidad de datos con la que trabajan los protocolos. Es un método de transmisión en el que las secciones de un mensaje son enviados en cualquier orden. el orden corrector se restablece en la estación que recibe (trabajo realizado por los protocolos). Estas unidades contienen su propia dirección.

DES: Data Encryption Standard. Algoritmo Criptográfico Estándar usado en circuitos integrados especiales dentro de las tarjetas de red.

DOWNSIZING: Concepto que se aplica al proceso de acondicionar aplicaciones hechas originalmente para una plataforma de cómputo, a fin de que se ejecuten en otra de "menor" potencia.

EGP: Exterior Gateway Protocol. Protocolo de Internet, para el intercambio de información de enrutamientos de control. Usado por los protocolos de comunicaciones para el control de flujo, direccionamiento y verificación de errores.

ENRUTADOR: Dispositivo que permite direccionar los datos enviados desde un equipo a otro situado en una red distinta. este Sistema se basa en direcciones de red de dispositivos únicas.

ETHERNET: Especificación de red inventada por XEROX Corporation y desarrollada conjuntamente por esta firma, Intel y DEC. Opera a 10 Mbps sobre cable Coaxial (y recientemente sobre UTP), utilizando el Protocolo de acceso al medio CSMA/CD. Está comprendido dentro del estándar 802.3 de la IEEE.

FDDI: Fiber Distributed Data interface. Estándar Definido por la ANSI que especifica una red Token Passing de 100 Mbps utilizando un cable de fibra óptica. Para proporcionar redundancia se instrumenta con una arquitectura de anillo dual.

FRAME: Es un conjunto de información lógica enviada como una Unidad formada por la capa de enlace (del nivel OSI) sobre un medio de transmisión. Los términos: Datagrama, Paquete, Segmento y Mensaje son usados también para describir grupos de información lógica en varias de las capas del modelo OSI y en otros conceptos tecnológicos.

FTP: File Transfer Protocol. Un protocolo de aplicación de IP para el envío de archivos entre nodos en una red TCP/IP.

El autor es Ing. en Comunicaciones y Electrónica por el Instituto Politécnico Nacional. Actualmente es responsable de los proyectos en conectividad en el Banco Nacional de Comercio Exterior. Su dirección electrónica es eropesa@ spin.com.mx.

HDLC: High Level Data Link Control. Protocolo de la capa de enlace de datos, estandarizado por la ISO y derivado de SDLC (las modificaciones y adaptaciones fueron hechas por el (ANSI). Especifica un método para el encapsulamiento y transporte de paquetes de datos sobre enlaces sincronos. De este protocolo se deriva también los protocolos LAN / LAPB (modificaciones hechas por el CCITT).

HOST: Sistema de computo en una red. Similar a los términos dispositivos (device) o nodo, excepto que host usualmente implica un sistema de cómputo, mientras que dispositivo y nodo se implican a cualquier otro elemento conectado en la red, como los servidores de comunicaciones y enrutadores.

HUB: Término usado generalmente para describir un dispositivo que sirve como el centro de una red en topología de estrella. En la terminología de la IEEE

802.3 *un Hub* es un dispositivo repetidor multipuerto ethernet que también se conoce como concentrador.

El término también se usa para referir al dispositivo de hardware/software que contiene múltiples segmentos de red conectados pero independientes. Los Hubs pueden ser activos (repiten la señal que los atraviesa) o pasivos (sólo dividen las señales que los atraviesan).

ICMP: Inthernet Control Message Protocol. Protocolo de Internet de la capa de red que provee de paquetes de mensajes que reportan errores y otra información relevante al procesamiento de los paquetes de IP.

IEEE: Institute of Electrical and Electronic Engineers. Organización de profesionistas que se encarga de definir, mantener y soportar estándares de comunicaciones y redes.

IEEE - 802.1: Define, entre otras cosas, un algoritmo de enrutamiento de frames denominados Spanning Tree.

IEEE - 802.2 : Empleado en redes 802.3 y 802.5, define las tareas de interacción entre los niveles dos y tres del modelo OSI. En otras palabras es un protocolo que especifica la instrumentación de la subcapa LLC (Logical Link Control) de la capa de enlace. Esta especificación maneja errores, control de flujo y el servicio de interfaz con el nivel tres de OSI.

IEEE - 802.3 : Protocolo de red que da las especificaciones del nivel uno (físico) y la subcapa MAC (Media Access Control) del nivel de enlace de datos del modelo OSI. Este protocolo está basado en el CSMA/CD. Está relacionado con el ethernet y se usa en diversos medios físicos (cable grueso, delgado, UTP).

IEEE - 802.4 : Protocolo de red que da las especificaciones del nivel uno (físico) y la subcapa MAC del nivel de enlace de datos del modelo OSI. define un tipo de red Token Bus similar a Arcnet.

IEEE - 802.5 : Protocolo de red que da las especificaciones del nivel uno (físico) y la subcapa MAC del nivel de enlace del modelo de datos OSI. Usa un método de acceso de Token passing a 4 o 16 Mbps sobre un cableado de Par torcido con malla (STP y últimamente también en UTP). La definición del Token Ring de IBM, quien promovió éste estándar, difiere en algunos aspectos.

XIV. CONCLUSIONES

CONCLUSIONES

Después de haber realizado la documentación de la red de la Empresa Tractores New Holan de México, me di cuenta de que la Organización cuenta con un gran equipo de cómputo, pero que quizás no se está explotando al máximo, por la falta de un buen software para la administración de los recursos de la red.

Debido a lo anterior, se genera uno de los principales problemas == Falla en el monitoreo de la red ==, ya que la mayoría de los usuarios necesitan esperar demasiado tiempo para poder accesar la red, y cuando la logran accesar tratan de no salirse de ella; ésto obviamente ocasiona también un conflicto, ya que hay usuarios que no salen de la red para evitar el problema de volver a accesarla. Pero existe un momento en el que no la usan y aún así no dejan trabajar a otros. La solución que se puede dar a éste problema es la adquisición de un eficiente software de monitoreo. Además de establecer un calendario de tiempos de acceso a la red, para que en él se describan Hora, Día , en que los grupos de trabajo accesen la red, de acuerdo a sus cargas de trabajo.

Otro aspecto importante es el hecho de que se cuenta con cinco servidores y sólo tres de ellos se encuentran trabajando, los otros dos se tienen para realizar pruebas. Yo pienso que si se pusieran a trabajar los cinco servidores, y se determinara una buena estructura de archivos y directorios de trabajo para cada grupo de usuarios, el tráfico de la red sería más factible, ya que de esta manera se determinaría que un determinado grupo de usuarios enviara su información a procesar a un determinado servidor.

En cuanto a la división de los grupos de trabajo se tiene muy bien determinado que existen ocho grupos de trabajo, y en cuanto a la distribución del trabajo también, ya que a cada usuario se le entrega un reporte de todas las pantallas a las cuales tiene acceso su grupo de trabajo, y si algún usuario requiere para mejor desempeño de su trabajo accesar a otra pantalla adicional, necesita llenar una solicitud de acceso a determinada pantalla, ésta por consecuencia, debe de ser previamente autorizada por su jefe de departamento.

Un ejemplo de los reportes que se le envían a los usuarios se muestra a continuación:

NEW HOLLAN DE MÉXICO S.A. DE C.V.
FECHA: 11/10/96 REPORTE PANTALLAS DE SEGURIDAD x CLAVE
Pag: 1 Clave: gl*

Menú	Sel	Descripción
0	1	Arts/Almacén
0	2	Direcciones/Impuestos
0	3	Ctrl de Inventarios
0	4	Inventario Físico
0	5	Compras
0	6	Cotizaciones de Vtas
0	7	Ordenes Vtas/Facturas
0	8	Pods Configurables
0	10	Ords Servicio/Reparac
0	11	Servicio al cliente
0	12	Plan de Distribución
0	13	Estructuras Producto
0	14	Rutas/Centros de Trabajo
0	15	Formula/Proceso
0	16	Ordenes de Trabajo
0	17	Control de Piso
0	18	Repititiva
0	19	Admon de Calidad
0	20	Plan Línea Prod.
0	21	Plan de Recursos
0	22	Pronostico/Plan Maestro
0	23	Plan Rqmt Materiales
0	24	Plan Rqmts Capacidad
0	25	Contabilidad General
0	26	Divisas Múltiples
0	27	Cuentas por cobrar
0	28	Cuentas por pagar
0	30	Admon. de Costos
0	31	Admon de Efectivo
0	32	Activos Fijos
0	33	Plan de Operaciones
0	34	Bases de datos múltiples
0	35	EDI
0	36	Admon. del Sistema
1	5	Menú Reportes de Artículos
1	12	MNTO Maestro de Comentarios

NEW HOLLAN DE MEXICO S.A. DE C.V.

FECHA: 11/10/96 REPORTE PANTALLAS DE SEGURIDAD x CLAVE
Pag: 2 Clave: gl*

Menú	Sel	Descripción
1	16	MNTO Artículos Cliente
1.2	17	MNTO Cuenta de Ventas
1.4	18	MNTO Costo Artículo-Almacén
1.5	22	Valuación de Inv. por Ubicación
1.5	23	Valuación de Inv. por Fecha
1.5	24	Valuación de Inv. por Ubic
2.3	3	REP Direcciones de Proveedores
3.20	1	MNTO Tabla Cuentas de Orden
3.20	5	Registro Aplicación Ctas Orden
5	14	Impr Documento Recepción Compras
5	19	Impr Documento Devoluciones Compras
7	4	Impresión Orden de ventas
7.6.3	13	REP se Programa
7.6.3	15	Comparativo de Programa
7.6.3	17	REP Autorización de Programa
25	1	Cambio Entidad Actual
25.13	1	MNTO Pólizas de Diario
25.13	3	MNTO Pólizas Inversas
25.13	4	Copia de Pólizas
25.13	14	Registro pólizas no aplicadas
25.19	4	MNTO Referencia Cruzada de Cta.
25.19	25	To-Account Cross-Reference Maint
26	13	MNTO de Bancos
28	3	Regostro de Vouchers
28	6	Confirmación Automática Vouchers
28	7	Confirmación Manual Vouchers
28	9	Menú Pagos/Cheques a Proveedores
28.9	1	MNTO. de Bancos
28.9	12	Registro de pagos
29	17	** Sin descripción en LS **
29.17	21	** Sin descripción en LS **
30	1	MNTO. grupo de costos
30	3	Copia Gpo. Costos a Gpo. Costos
30	9	Asignación Gpo. Costos a Almacén
30.13	5	MNTO. Costo Simul Art-Elemento
30.13	19	Simulación Rollup Ctos. Estruct.

NEW HOLLAN DE MEXICO S.A. DE C.V.
FECHA: 11/10/96 REPORTE PANTALLAS DE SEGURIDAD x CLAVE
Pag: 2 Clave: gl*

Menú	Sel	Descripción
30.13	21	Copia Simulación a Simulación
30.13	22	Copia Simulación a CT/Rutas
30.13	23	Copia Art/Rutas a Simulación
30.15	1	MNTO. Plan de costos por Almacen
30.15	3	Actualización Plan Costos por Almac.
		Fin de Reporte

Además, algo similar a lo anterior, es el hecho de que sólo se tiene un servidor de impresión disponible para todos los usuarios conectados a la red; se tiene un buen número de impresoras, pero sólo se ocupan en forma independiente de la red, yo pienso que si se utilizaran por lo menos una de las impresoras que se tienen en cada departamento como servidores de impresión, ésto haría las impresiones más rápidas y de mayor calidad.

En la Organización no se tienen establecidas en forma definida, las políticas de la red, pero a pesar de ello, se llevan a cabo respaldos de datos en forma continua, el acceso a la red no tiene horario, ya que la red puede ser accesada las 24 horas, debido a que se encuentra conectada a Estados Unidos mediante un ruteador, y en muchas ocasiones, cuando algunos usuarios requieren quedarse a trabajar por exceso de trabajo, pues la red se debe encontrar disponible para ellos, lo bueno , es que sí se tiene un buen control de acceso a la red, para verificar quién, cuando y a que hora acceso la red algún usuario. Aún así, pienso que sería factible que se establecieran políticas por escrito, y que se dieran a conocer a todos los usuarios y además, se den los posibles castigos o consecuencias que puede acarrear el no sujetarse a ellas.

XV. BIBLIOGRAFÍA

BIBLIOGRAFÍA

*** Novell Netware 386, Tom Sheldon**
Editorial Mc Graw Hill

*** Manual de Windows**
Para Trabajo en Grupo

*** Revista Personal Computing**
Edición: Nov. 95, Dic. 95, Ene. 96.

***Audotoría de Informática**
Ayala Rodiles, Sara Isabel