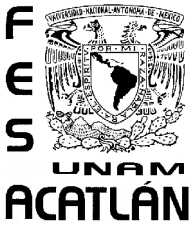
UNIVERSIDAD NACIONAL AUTONOMA
DE
MÉXICO



FACULTAD DE ESTUDIOS SUPERIORES ACATLAN

Bajo la opción de Tesina

Nombre del trabajo:

Identificación, Autentificación de usuarios y seguridad en Internet

Elaborado por**: Fermín Daniel Arazo Saladino**

Asesor: **Guadalupe del Carmen Rodríguez Moreno**

Acatlán, Edo. de México **Septiembre, 2006**

Contenido

Simbología utilizada en los códigos de barras

Lectores ópticos

Los colores permitidos en los códigos de barras

Biometría

Clasificación de técnicas biométricas

Técnica biométrica estática

Técnica biométrica dinámica

Tokens para la seguridad

Capítulo 3 Seguridad en internet

Concepto de redes de computadoras

Componentes Básicos de una Red

Medios de comunicación

Tipos de redes

Topologías de redes de computadoras

Modelo OSI y TPC/IP

Servidor Proxy

Redes VPN

Protocolo de seguridad WEP

Firewall

Conclusiones

Introducción

Actualmente la seguridad computacional es un tema de bastante importancia, ya que los sistemas computacionales corren el riesgo de ser corrompidos, alterados o simplemente destruidos por los conocidos hackers y/o crackers aún cuando cada uno de ellos tienen objetivos diferentes, ambos deben de romper todas las medidas de seguridad, lo cual es un reto para cumplir sus metas.

Es por eso que el objetivo de este trabajo es de informar sobre ciertas medidas de seguridad en cuanto al mundo de la computación e internet se refiere. Así que de inicio para que un sistema comience a ser seguro debe de tener una buena contraseña de acceso, la cual solo puede ser definida por el usuario por medio de ciertas reglas para diseñar la contraseña casi perfecta, pero además el usuario debe ser disciplinado y bastante estricto en cuanto a usar su clave ya que de nada sirve tener una buena contraseña si no es capaz de protegerla de personas ajenas.

Otro aspecto importante además de la contraseña es el uso de hardware y/o software para proteger el equipo y también las instalaciones, éstos por ejemplo en cuanto a hardware son las tarjetas inteligentes que en la actualidad son utilizadas por corporaciones como medio de identificación de sus empleados, pero esto no es suficiente, ya que es fácil falsificar una tarjeta o credencial por lo cual hay que, autentificar ala persona que porta la tarjeta, una de estas técnicas es la biometría dicha técnica se caracteriza por analizar los rasgos característicos de los seres humanos como son la voz, el iris, la forma de escribir, entre otras, ya que es imposible la duplicación de cada uno de estos rasgos, logrando así una seguridad excepcional.

Otra forma de seguridad es el uso del conocido firewall el cual puede encontrarse en formato de hardware y software, se puede usar por separado o en unión para lograr una mayor seguridad, ya que nos permite entrar en la red mundial internet y así evitar el acceso de programas mal intencionados que vayan a perjudicar nuestro sistema.

1 Formas de Identificación y Autentificación de Usuarios

1.- Concepto de username o login

En el aspecto informático, el nombre de usuario el cual es más conocido por la palabra en inglés ***username*** **o** ***login*** tiene el siguiente significado: “es una clave o código compuesto por caracteres sencillos o alfanuméricos el cual tiene como función, el identificar a la persona que utiliza dicha clave junto con una contraseña para poder acceder a los recursos de un sistema computarizado”.

1.1.1.- Username como forma de identificación de un usuario

Una de las formas de identificación más utilizadas actualmente es el uso del username el cual como se definió anteriormente, nos permite el manejo de los sistemas computarizados, además de los recursos con los que cuentan dichos sistemas, y la única forma de verificar la autenticidad del identificador es por medio de la contraseña.

1.2 Concepto de password (contraseña)

Para poder reconocer a un usuario de forma fiable y segura en los sistemas informáticos es necesario la validación de un password (contraseña) la cual se define como “un conjunto de caracteres alfanuméricos que se representa por medio de asteriscos u otros caracteres especiales para enmascarar la clave que es considerada secreta”, estas claves son utilizadas casi exclusivamente para autentificar a los usuarios y permitirles el acceso a los recursos pasivos de los sistemas informáticos.

Es considerada como regla estricta en la actualidad el uso de contraseñas, para evitar que individuos ajenos logren ingresar y así hacer uso mal intencionado de la información, por lo que es aconsejable el uso de algunas reglas para asegurar que usuarios no autorizados no puedan descubrirlas:

- Memorizar las contraseñas.
- Nunca se deben de dejar al alcance donde un usuario no autorizado ó persona ajena pueda encontrarlas (en caso estrictamente necesario de que la contraseña sea escrita en un papel)
- Se deben de guardar en un lugar seguro.

    - Las contraseñas no deben ser muy cortas (debido a que son faciles de memorizar), usar ocho caracteres son suficientes.
- No compartir con familiares o amigos.
- En sistemas computacionales donde la información es de carácter importante, se puede implementar un procedimiento por medio de la programación, para hacer que el sistema lleve una bitácora de registro de las contraseñas que son usadas, qué información se ha accedido, y fecha de en la que se uso.
- Cancelar o deshabilitar temporalmente una contraseña asignada a un usuario al que ha renunciado o suspender por tiempo definido.
- Los administradores del sistema necesitan tener la capacidad
  de reintroducir las contraseñas de los usuarios que las han olvidado.
- Cualquier usuario con contraseña de acceso a un sistema informático (eso incluye a los administradores del sistema), deben contar con un límite sobre la información a la que pueden acceder sin problema.

De este modo podemos asegurar que la información, así como de los recursos de los sistemas se encuentren resguardados de toda persona ajena.

1.2.1 El password como forma de autentificación de usuarios en los sistemas informáticos

Una de las formas de autentificación más sencilla y básica en los sistemas de cómputo es la validación de una contraseña la cual se rige bajo el siguiente protocolo:

- La existencia de entidades (2 o más) las cuales están de acuerdo en la clave que se usará para la autentificación, dicha clave se debe de mantener en secreto si se desea una autentificación más confiable y segura.

- Cuando una de las entidades, en este caso, el usuario desea autentificarse ante el sistema informatico, el usuario debe ingresar una clave (contraseña), y si ésta es correcta se otorga el acceso a un recurso que forma parte del sistema.

- Lo conveniente es que existan roles preestablecidos, con una entidad activa que desea autentificarse (usuario) y otra pasiva que admite o rechaza a la anterior (sistema).

Como se sabe esta forma de autentificación resulta ser muy frágil, debido a que es suficiente con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda; por ejemplo, si el usuario comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado automáticamente esa persona puede autentificarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

Hoy en día el usuario promedio tiene el acceso principalmente a sitios comercializados en internet, donde tiene que registrar sus contraseñas, esto en un principio resultaba difícil ya que debía de crear diferentes contraseñas largas y a veces complicadas de recordar, por lo cual resulto factible el crear una sola cuenta para los diferentes sitios, además una característica que destacaban en esa contraseña era en que se elegía un nombre de algún familiar, o una fecha, etc. Dando como resultado una contraseña que era

demasiado corta, esto fue cómodo pero fue contraproducente ya que otras personas que conocían la clave debido a su sencillez podían acceder a los sitios que sabían que el usuario original frecuentaba para así hacer uso de los recursos a los cuales ya tenia privilegios, por eso se deben de tomar en cuenta ciertas reglas para una buena creación de contraseñas, primeramente se debe de considerar la necesidad de una contraseña que sea de acuerdo al nivel de seguridad del sistema, hay que recordar que el equipo personal (PC) es muy diferente a un equipo en una empresa, después de considerar las necesidades, se utilizarán algunos recursos que nos permitan recordar la clave y así lograr un equilibrio entre la comodidad y la seguridad, evitando claves que tengan relación directa con el usuario, es decir, claves que sean como:

- números telefónicos
- nombre del padre / madre
- nombre de la novia
- nombre de la mascota
- fechas de nacimiento
- personaje favorito de TV

Para lograr una clave imposible de descifrar se recomienda lo siguiente:

- Palabras con sentido para el usuario.
- Usar caracteres como números, signos, mayúsculas y minúsculas que se pueden intercalar en la misma palabra.
- Longitud mínima de 8 caracteres, más de 8 caracteres se considera una buena contraseña.
- Utilizar código ASCII para aquellos que deseen descifrarla les sea más difícil de obtener.

La mayoría de los sitios o sistemas condicionan al usuario al establecer una contraseña con un formato en especial, requisito que está definido por lugar al que se desea ingresar, de ese modo resulta menos complicado ya que existe un estándar para el uso de contraseñas.

Pero hay que recodar asignar una contraseña diferente a cada uno de los sitios a los que se ingresa, porque el crear una sola clave para todos (unificación de contraseña) hace más vulnerable la seguridad, a lo cual podemos establecer un diferente nivel de contraseña a los distintos tipos de sitios a los que se accede, la siguiente tabla muestra el nivel a que se debe de seguir:

Servicio	Nivel	Ejemplo Password
Equipo.	**Nivel de seguridad alto. 15 ó más caracteres.**	**Cr@ckeal@ si Puede5**
Correo.	**Nivel de seguridad alto. 15 ó más caracteres.**	**C@rtas@miYahoo88** **C@rtas@miHotmail99**
Cuentas en servidores.	**Nivel de seguridad alto. 15 caracteres.**	**MiP@ginaWEBServer9**
Cuentas FTP.	**Nivel de seguridad medio. 10 caracteres.**	**Cuen7aF7P5**
Documentos, archivos.	**Nivel de seguridad medio. 10 caracteres.**	**Fi6hero#99** **W0rDTema#56**
Foros/Sites Web.	**Nivel de seguridad medio. 10 ó más caracteres.**	**PaseParaFor0** **PaseParaSit6**
Otros servicios.	**Nivel de seguridad bajo. 8 caracteres.**	**Sombrer0**

Otro aspecto esencial es el de periodo de vida de las contraseñas o vigencia el cual es recomendable a un máximo de 5 meses dependiendo del sistema, en un aspecto donde la seguridad es bastante grande se puede considerar el renovar las contraseñas en periodos de tiempo más largos, de no ser así entonces se tendrá que tomar la medida de cambiarlas en tiempos más cortos.

1.3 Contraseña

Como se habló en el punto anterior el tener un buen hábito en el uso de contraseñas permite mantener la seguridad de los sistemas informáticos, pero el verdadero reto es para aquellas personas que cuentan con altos conocimientos en informática, ya que aplican sus conocimientos y habilidades para descifrar dichas contraseñas, este tipo de gente son conocidos como hackers cuyo único fin, es el de penetrar sistemas violando toda seguridad, las formas en la que los hackers logran obtener las claves, es por medio de técnicas y de programas que muchas veces son de su propia creatividad a este último método también se le denomina fuerza bruta, por mencionar otra de las técnicas más usadas es la conocida como ***ingeniería social***, donde el atacante quien esta interesado no sólo en obtener la clave del usuario, sino saber mas acerca de él para utilizar esa información, primeramente elige un medio donde encontrar una victima, este medio es a través de un chat, que resulta ser el más común, después adopta una personalidad distinta (si es hombre se hace pasar por mujer) comienza el trato con cualquier persona que obviamente tendrá contacto, después de una larga platica el atacante le advierte que le mandará una “foto” esperando que la otra persona acepte, al tener respuesta favorable, lo único que falta es esperar a que la otra persona abra la fotografía, para que así el “programa” que se oculto con la foto comience a funcionar y obtener la información que el atacante necesita. La otra forma es a través del uso de programas decodificadores capaces de descifrar la contraseña ya que cuentan con un diccionario de palabras comunes que un usuario promedio utiliza para sus contraseñas, por eso si se tiene la sospecha de que alguien tenga alguna de sus contraseñas debe:

- Cambiar inmediatamente esa contraseña.
- Revisar sus cuentas on-line con frecuencia para detectar alguna transacción que no haya autorizado, como son los cargos a las tarjetas de crédito, retiros de cuentas de banco, transferencia de fondos.

- Revisar las bitácoras de eventos en los sistemas operativos, para detectar accesos extraños a sitios en internet.
- Protéjase utilizando contraseñas poco probables y más seguras.
- Evitar aceptar propaganda de Internet que llega por medio del correo electrónico.
- Si se procura mucho los chats, evite aceptar fotos u otros tipos de archivos.

Además de otras aficiones que tienen los hackers después de haber entrado al sistema es la de cambiar las contraseñas de algunas cuentas o en el peor de los casos eliminarlas por completo.

1.4 Autentificación de Usuarios con PAM

PAM (Pluggable Authentication Modules), es un mecanismo que funciona para la autentificación de usuarios, que fue implementado por SUN microsystem, en los primeros sistemas UNÍX, Linux no fue la excepción ya que cuenta con este mecanismo en sus versiones de ***Red Hat***

PAM y gracias a su flexibilidad, permite que se desarrollen programas o aplicaciones adicionales para hacer uso de este mecanismo de autentificación, como por ejemplo, lectores de huellas digitales.

Cabe mencionar que PAM no tiene como único objetivo la autentificación de usuarios, otras tareas se explican en los siguientes cuatro grupos que se encuentran dentro del mecanismo PAM, los cuales son:

- ACCOUNT.
- AUTHENTICATION.
- PASSWORD.
- SESION.

ACCOUNT (cuenta)

En este grupo se encuentran ciertas tareas que permiten o niegan el acceso de los recursos con los que cuenta la computadora, por ejemplo: *manipulación de la hora*, *fecha*, entre otros, ya que verifica las cuentas de usuario existentes, un ejemplo descriptivo de este grupo es, cuando el usuario tiene o no acceso al disco duro, puede usar la impresora, u otros dispositivos con los que cuente la máquina, y eso se debe a que su cuenta de usuario no esta habilitada con ciertos “privilegios” que le permite hacer uso de los recurso ya mencionados, además el grupo **ACCOUNT** determina si algunas cuentas ya han caducado, permitiendo una mejor administración de los mismos usuarios.

AUTHENTICATION (autenticación / autentificación)

La actividad que realiza esta tarea es la de verificar que en realidad es el usuario quien dice ser.

PASSWORD (contraseña)

La tareas primordial es de mantener actualizada la contraseña que se ha asignado a cada uno de los usuarios que tienen posibilidades de utilizar el equipo.

SESION (sesión)

Proporciona los servicios a los cuales el usuario esta destinado a utilizar, una vez que el ***modulo**** de cuenta haya permitido al modulo de autentificación comprobar la identidad del usuario.

Los módulos con los que cuenta el mecanismo PAM* son los siguientes:

- pam console.so.
- pam_cracklib.so
- pam_deny.so
- pam_env.so
- pam_limits.so
- pam_nologin.so
- pam_permit.so

---

modulo grupos de tareas que se unen para una misma operación o función,
PAM ver 0.77

- pam_rootok.so
- pam_securetty.so
- pam_stack.so
- pam_wheel.so
- pam_xauth.so

La siguiente tabla (Tabla 1) describe al grupo que pertenece cada modulo y función que desempeña:

MODULO	GRUPO AL QUE PERTENECE	FUNCION ESPECIFICA
pam_console.so.	SESSION Y AUTH	Cambios de permisos y propietarios de los ficheros
pam_cracklib.so	PASSWORD	Notificar al usuario la debilidad de su clave de acceso
pam_deny.so	ACCOUNT, AUTHENTICATION, PASSWORD Y SESSION	Función, de producir un fallo al no cumplir con las reglas establecidas de autentificación del usuario
pam_env.so	AUTHENTICATION	Establece las variables de entorno o sustituirlas cuando un usuario se registra en el sistema

MODULO	GRUPO AL QUE PERTENECE	FUNCION ESPECIFICA
pam_limits.so	SESSION	Controla y limita los recursos del sistema a un usuario, un grupo, o a todos los usuarios
pam_nologin.so	ACCOUNT Y AUTHENTICATION	Permite la entrada al sistema a usuarios siempre y cuando no exista el fichero **/etc/nologin**
pam_permit.so	ACCOUNT,AUTHENTICATION, PASSWORD Y SESSION.	
pam_rootok.so	AUTHENTICATION	Permite la entrada al sistema al usuario root sin problemas, lo cual genera cierto problema.
pam_securetty.so	AUTHENTICATION	Limita las consolas en las que se puede autentificar el usuario root
pam_stack.so	ACCOUNT, AUTHENTICATION, PASSWORD Y SESSION	Permite la asociación de modulos PAM, devolviendo un error si algún modulo falla
pam_wheel.so	AUTHENTICATION,	Limita la autentificación como root a usuarios del grupo wheel

MODULO	GRUPO AL QUE PERTENECE	FUNCION ESPECIFICA
pam_xauth.so	SESSION	Redirecciona las cookies de autentificación de un usuario en el sistema X-Windows

Tabla1
Módulos Ver. 0.77 de PAM-Linux

Los módulos, permiten en conjunto acceder de manera segura al sistema ya que a través de la autentificación de los usuarios, evita intrusos no autorizados protegiendo la información, además por su flexibilidad los desarrolladores de aplicaciones no necesitan crear un programa que les permita usar un determinado esquema de autentificación.

En su lugar, pueden concentrarse únicamente en los procesos que realiza
su programa evitándose recompilar todo el código.

2 Tecnologías Aplicadas en la Seguridad Computacional

2.1 Tarjetas inteligentes (smartcards)

Son tarjetas con un chip integrado, las cuales son mejor conocidas como tarjetas inteligentes, pueden almacenar y procesar grandes cantidades de información, entre sus características más importantes se encuentran la lectura y escritura de datos, mediante el uso de programas o aplicaciones. Entre algunas de sus utilidades se encuentra el, poder autorizar o controlar transacciones bancarias y comerciales, permitir el acceso autorizado a zonas

restringidas en edificios inteligentes, almacenar información de modo digital, conservar y utilizar boletos para viajes o eventos, almacenar de manera segura información médica o legal del usuario, pero las aplicaciones se verán más adelante.

2.1.1 Breve historia de las tarjetas inteligentes

En marzo de 1970, el japonés Kunitake Arimura presenta la primera tarjeta de plástico con un circuito integrado, planteando así las bases para la que hoy se conoce como tarjeta inteligente (smartcard)

En 1974, el francés Roland Moreno registró el concepto original de las tarjetas IC (Circuito Integrado). Moreno fijó su atención en aspectos funcionales tales como "el PIN en la tarjeta". Fundó Societé Internationale pour l'Innovation (Innovatron).

En 1979, Michael Ugon de Bull en colaboración con Motorola entregaron la primera tarjeta que contenía un microprocesador, conocida después como "Tarjeta Inteligente".

Bull CP8, Schlumberger y Philips fueron, a principios de los 80, los tres primeros fabricantes de tarjetas inteligentes.

La filosofía que ha seguido es muy sencilla, se trata de almacenar información con cierta autonomía.

Aunque la cantidad de información que puede almacenar es relativamente pequeña por la cantidad de memoria utilizada, su autonomía es lo suficientemente importante como para haber producido la expansión de este tipo de tarjetas y llegar a ser lo que es hoy.

Al igual que una computadora personal, el chip puede programarse para ejecutar algunas tareas específicas y tomar decisiones al comunicarse con una terminal (computadora) o un lector de chip.

2.1.2 Características Generales

La tarjeta inteligente es básicamente un chip, el cual se encuentra encapsulado en un rectángulo de PVC de aproximadamente 85´ 54mm. Las tarjetas se encuentran por lo regular en color blanco, pero su superficie puede ser impresa utilizando diferentes medios (*Figura 2.1.2.1*). El chip que contiene dispone de unos contactos exteriores que son los que le permiten mantener una comunicación con él, y de esta forma acceder a la información que contiene o grabar nueva información. Estos contactos tienen un recubrimiento en oro o también de otro material, para que la tarjeta sea resistente al uso diario, y en cualquier tipo de entorno como es: la alta humedad, agentes químicos, trato excesivamente rudo, etc. Su pequeño formato hace que sea ideal como sistema de identificación personal. Además, su medida no está limitada por razones técnicas, sino por razones de estandarización, es decir, técnicamente se podrían producir y utilizar tarjetas que fuesen la cuarta parte de tamaño y con capacidades mucho más grandes que las tarjetas actuales.

(*Figura 2.1.2.1*)

E*jemplos de tarjetas inteligentes*

2.1.3 Las tarjetas inteligentes y el estándar ISO 7816

La ISO (International Standard Organization) ha establecido un formato especial para las tarjetas inteligentes en el estándar 7816.

La descripción de cada una de las partes del estándar **7816** es:

- **7816-1**: Características Físicas.
- **7816-2**: Dimensiones y ubicaciones de los contactos
- **7816-3**: Señales Electrónicas y Protocolo de Transmisión

ISO 7816-1: Características Físicas

La característica que define una tarjeta es sin duda alguna su aspecto físico. Otro detalle el cual podemos percibir a simple vista es la presencia o no del área de contactos (*Fig. 2.1.3.1*), la cual tiene la forma de un cuadrado dorado o plateado, y que esta se ubica en la superficie de la tarjeta. En algunos casos esta área no existe por lo que se denominan tarjetas sin contacto (*Fig. 2.1.3.2*).

Existe una estrecha relación entre el cuerpo de la tarjeta y el chip que lleva implantado dentro, de nada sirve que el cuerpo de la tarjeta sea capaz de soportar temperaturas extremas, si el chip no comparte esa característica. Ambos componentes deben de satisfacer todos los requisitos tanto por separado como conjuntamente.

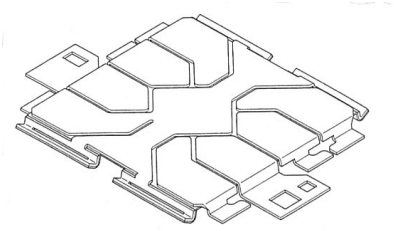


Fig. 2.1.3.1

Contacto de la tarjeta

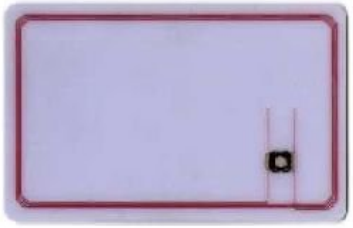


Fig. 2.1.3.2

Tarjeta sin contacto

Es por eso que la tarjeta debe:

- Resistir ataques con rayos X y luz ultravioleta
- Tener superficie plana
- Permitir cierto grado de torsión
- Resistir altos voltajes, campos electromagnéticos, electricidad estática
- No disipar más de 2,5 W

Formatos utilizados en las tarjetas:

- **ID-1**: Este formato es el más utilizado en la producción de tarjetas inteligentes (*Fig. 2.1.3.3*) con las siguientes medidas :
  - 85.6mm de ancho
  - 53.97mm de altura
  - 0.76mm. de espesor
- **ID-00**: Es formato al igual que el ID-000 se utiliza en la tecnología celular, con las siguientes dimensiones:
  - 66mm de ancho
  - 33mm de alto
- **ID-000** : Este formato es utilizado en la telefonía celular con tecnología de comunicación **GSM** (Global System for Mobile Communication)
  - 25mm de alto
  - 15mm de ancho
  - 3mm de corte rectanguar ubicado en el lado inferior derecho de la tarjeta

con un corte rectangular del lado derecho con una medida de 3mm, dicho corte permite una mayor facilidad de inserción de la tarjeta dentro del teléfono celular

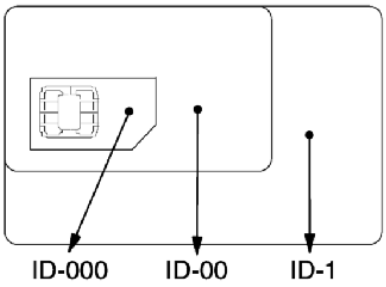


Fig. 2.1.3.3

Tamaños utilizados en las tarjetas inteligentes

ISO 7816-2: Dimensión y localización de los contactos

Dado que el microprocesador que se encuentra en la tarjeta requiere de algún medio por donde pueda tomar la alimentación de corriente eléctrica para sus circuitos o para llevar a cabo la transmisión de datos, es necesaria una superficie física de contacto que haga de enlace entre el lector y la tarjeta. Esta superficie consiste en 8 contactos que se encuentran en una de las caras de la tarjeta. El tamaño de los contactos no deber ser nunca inferior a 1,7mm de alto y 2mm para el ancho, el valor máximo de estas medidas no está especificado, además la ubicación de estos contactos en una tarjeta inteligente (*Fig. 2.1.3.4*) debe de ser a las siguientes medidas, tomando como referencia la esquina superior izquierda

- 10.25mm a lo ancho de la tarjeta
- 19.23mm a lo alto de la tarjeta

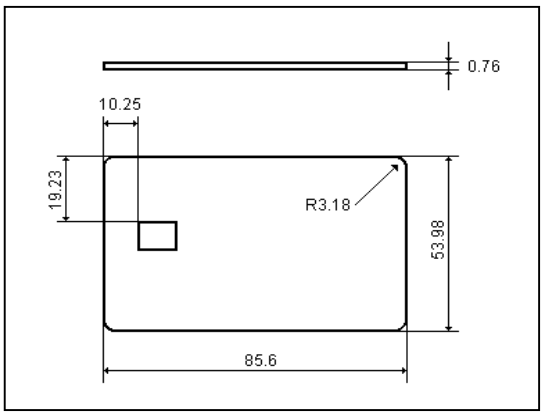


Fig. 2.1.3.4
Localización de los contactos en una tarjeta inteligente convencional

Los 8 contactos están diseñados para cumplir cierta función y así permitirle al microprocesador comunicarse e intercambiar información con los lectores. Algunos de estos contactos no tienen definida ninguna función (*Fig. 2.1.3.5*).

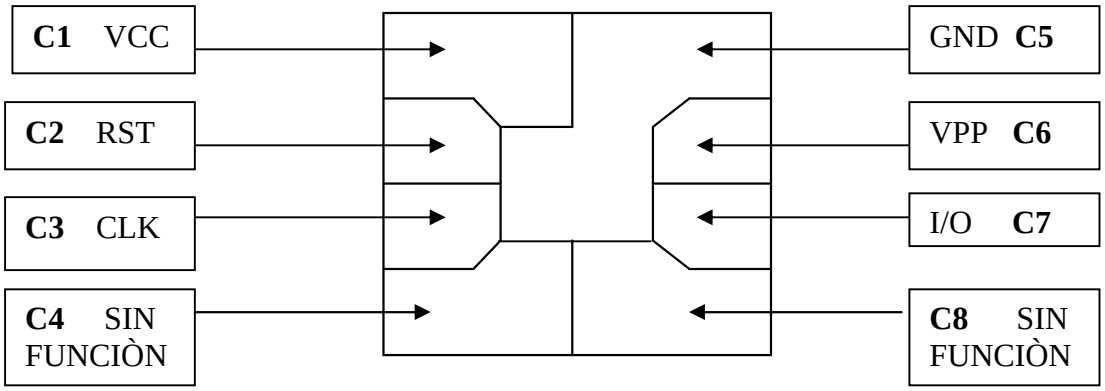


Fig. 2.1.3.5
Funciones desempeñadas de los contactos

Contacto 1 (c1) Vcc

El chip al igual que una computadora necesita de energía para poder funcionar. El contacto *Vcc* es el encargado de suministrar corriente eléctrica del chip. La energía

o corriente eléctrica es proporcionada por el dispositivo (hardware) con el que la tarjeta interactúa en cada operación.

Contacto 2 (c2) RST "RESET"

Es el mecanismo que pone en funcionamiento la interrelación entre una tarjeta inteligente y cualquier elemento externo adecuado con el que se ponga en contacto

Contacto 3 (c3) CLK "CLOCK"

La tarjeta debe suministrar una señal de reloj, que será utilizada para el funcionamiento de los circuitos contenidos en ella. La frecuencia determina la velocidad de comunicación entre lectora y tarjeta. El estándar fija una frecuencia de reloj de 372 veces la velocidad de transmisión deseada, aunque esta cantidad puede variar en función de la tarjeta. El rango normal de operación de una tarjeta suele estar entre 1 MHz y 5 MHz.

Contacto 4 (c4)

No tiene asignadas funciones por el momento **.

Contacto 5 (c5) GND "TIERRA**"**

La única función de este contacto es de "hacer tierra" .

Contacto 6 (c6) VPP

Este contacto se utilizaba con antiguas tarjetas donde se requería de cierto voltaje externo para programar la memoria de la tarjeta, en la actualidad este contacto ya no se utiliza .

Contacto 7 (c7) I/O "ENTRADA Y SALIDA"

A través de este contacto permite la entrada y salida de la información, pero no es posible hacer las dos funciones al mismo tiempo.

Contacto 8 (c8)

No tiene asignadas funciones por el momento **

******** *Algunas tarjetas utilizan este contacto en combinación con el "c7 I/O" para realizar una comunicación completa, es decir un contacto se encarga de la entrada de datos y el otro de salida de datos teniendo así un mejor rendimiento*

ISO 7816-3: Señales electrónicas y protocolos de transmisión

Reset y ATR

Antes de poder establecer la comunicación con la tarjeta, debe proceder a su inicialización. Una vez se le ha aplicado alimentación y la señal de reloj apropiada, debe activar la señal de Reset. Una vez la tarjeta detecta esta señal, procede a enviar a la lectora una serie de bytes, conocidos como *Answer To Reset* (o ATR), que son la respuesta que genera la tarjeta a la señal de Reset. El ATR contiene información como:

- Frecuencia de reloj máxima a la que trabaja la tarjeta y factor por el que hemos de dividir esta para obtener la velocidad de transmisión. Por supuesto, en el inicio, la frecuencia y el factor está prefijada (3,5712 MHz y 372 respectivamente, para obtener una velocidad de transmisión de 9600 bps). Esto quiere decir que el ATR es enviado a una velocidad de 9600 bps, pudiendo variar la frecuencia y velocidad de transmisión utilizada después, tras una negociación entre Terminal y tarjeta.
- Se indica el orden de envío de los bits (los más significativos enviados primero o no) y si cada bit es enviado negado o no.
- Tiempo de espera entre carácter y carácter.
- Tensión de programación necesaria (Vpp), en caso de necesitarla.
- Protocolo utilizado por la tarjeta.
- Información relativa a la tarjeta o al fabricante, como número de serie de la tarjeta, versión del sistema operativo, etc.

Una vez la tarjeta ha enviado la respuesta al Reset (ATR), la Terminal ya conoce las características de la misma, y ya puede dialogar con ella, siempre con la línea de Reset activada. Una vez ha finalizado de dialogar con la tarjeta, desactivará la señal de Reset, no pudiendo comunicarse más con la tarjeta hasta volver a activar la señal, mediante la cual se volverá a recibir el ATR, repitiéndose el proceso.

Siendo el chip integrado el componente más importante de toda la tarjeta, estas serán clasificadas según el tipo de circuito que tengan.

2.1.4 Clases de Tarjetas inteligentes

Tarjeta Inteligente de Contacto

Estas tarjetas son las que se insertan en una terminal con lector inteligente para que por medio de contactos pueda ser leída. A su vez existen dos tipos de tarjeta inteligente de contacto: **Las sincrónicas y las asincrónicas.**

Tarjetas Inteligentes Sincrónicas o Tarjetas de Memoria (memory card)

Son tarjetas con solo memoria y la presentación de esta tarjeta inteligente y su utilización se concentra principalmente en tarjetas prepagadas para hacer llamadas telefónicas.

Estas tarjetas son desechables, cargadas previamente con un monto o un valor que va decreciendo a medida que se utiliza y una vez que se acaba dicho monto se vuelve prácticamente inservible y por lo cual hay que desechar. Las tarjetas contienen un chip de memoria que se utiliza generalmente para el almacenamiento de datos, dentro de esta categoría existen dos tipos de tarjeta las cuales son aquellas con:

- **Memoria Libre:**

Carece de mecanismos de protección para acceder a la información. Las funciones que desempeñan están optimizadas para aplicaciones particulares en las que no se requieren complejos mecanismos de seguridad. Como por ejemplo se utilizan para el pago de peajes, teléfonos públicos, máquinas dispensadoras y espectáculos, etc.

- **Memoria Protegida:**

Poseen un circuito de seguridad que proporciona un sistema para controlar los accesos a la memoria frente a usuarios no autorizados. Este sistema funciona mediante el empleo de un código de acceso que puede ser de 64 bits o más. Se utilizan en tarjetas bancarias las cuales necesitan de un Numero de Identificación Personal (NIP),

Tarjetas Inteligentes Asincrónicas:

Son tarjetas inteligentes con microprocesador (Fig.2.1.4.1), esta es considerada como la verdadera tarjeta inteligente, sus características físicas no cambian tiene el mismo tamaño y grosor de una tarjeta de crédito, pueden tener o no una cinta magnética en la parte posterior. Dentro del plástico se encuentra un elemento electrónico junto con la memoria RAM, ROM y EEPROM en el mismo chip la cual le permite tomar decisiones, además de que puede guardar información así como también el poder borrarse, esta tarjeta tiene muchas ventajas a diferencia de la sincrónica la cual es simplemente una memoria. La memoria ROM (Read Only Memory) enmascarada contiene el sistema operativo de la tarjeta, y se graba durante el proceso de fabricación. La EEPROM es la memoria no volátil del microprocesador, y en ella se encuentran datos del usuario o de la aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre del usuario, número de identificación personal o PIN (Personal Identification Number).

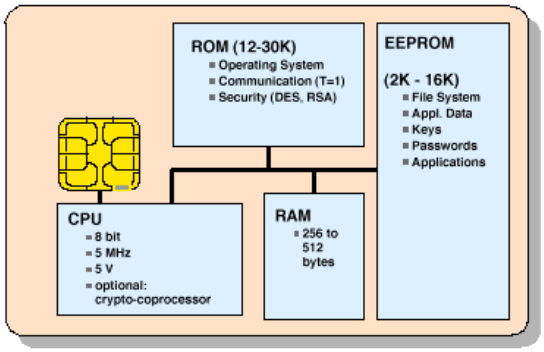


Fig. 2.1.4.1
Tarjeta inteligente asíncrona

La memoria RAM (Rand ; volátil, es decir que solo funciona al existir corriente eléctrica que alimente al chip esta memoria, es la

que utiliza el microprocesador para realizar sus trabajos. Al ocurrir algún fallo en el suministro de energía toda la información contenida en ella a alimentación.

El puerto de entrada y salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit.

Tarjetas Inteligentes sin Contacto

Son similares a las tarjetas de contacto con respecto a las funciones que pueden hacer, pero estas tarjetas carecen de contacto como las tarjetas anteriores (Fig. 2.1.4.2).

Poseen además del microprocesador, una antena de la cual se valen para realizar transacciones que tienen que ser realizadas muy rápidamente.

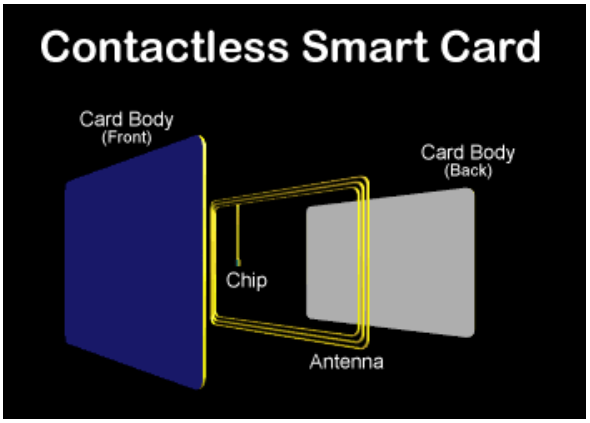


Fig. 2.1.4.2
Tarjeta inteligente sin contacto

Esta tecnología ofrece ventajas con respecto a la de las tarjetas de contacto. Cuando en una tarjeta de contactos se producen fallos de funcionamiento, casi siempre se deben al deterioro en la superficie del contacto o a la suciedad que se ha pegado al mismo. Una de las ventajas de las tarjetas sin contactos es que los problemas técnicos antes mencionados no ocurren, Otra de las ventajas es la de no tener que introducir la tarjeta en un lector. Esto es una gran cualidad y ventaja

en sistemas de control de accesos donde se necesita abrir una puerta u otro mecanismo, ya que la autorización de acceso puede ser revisada sin que se tenga que sacar la tarjeta del bolsillo e introducirla en un lector para su uso.

Este tipo de tarjetas se comunican por medio de radiofrecuencias. Dependiendo de la cercanía entre la tarjeta y el lector, existen dos tipos:

Tarjeta cercana: Para que esta tarjeta funcione debe estar a unos pocos milímetros del lector para que sea posible la comunicación.

Tarjeta lejana: la distancia varía entre centímetros y unos pocos metros.

2.1.5 Periodo (etapas) de vida de la tarjeta inteligente

Se tienen las siguientes etapas:

1.-Fabricación:

-Desarrollo del SO y su implementación como mascara ROM.

-Producción industrial del chip.

2.-Preparación:

- Inicialización y pre-personalización de la tarjeta según uso futuro.
- Envío al expendedor de la tarjeta.

3.-Personalización.

4.-Uso.

5.-Fin de la vida activa.

2.2 Código de barras

El código de barras es un método muy eficiente para asignar una clave única de identificación a una persona como por ejemplo su nombre, dirección, código postal, entre otros datos. Puede agregarse un código de barras a una tarjeta adicionalmente de la fotografía y de una banda magnética obteniendo así otro tipo de tarjeta inteligente pero no tan precisa como lo es aquella que tiene un chip integrado, ya que el código de barras puede recibir algún daño y así estropear la tarjeta en su totalidad.

2.2.1 Definición de código de barras

El código de barras (Fig. 9) consiste en una serie de barras paralelas negras y espacios en blanco de diferentes anchos, y los cuales están impresos en una etiqueta, su uso es principalmente para almacenar información. El código de barras representa un método sencillo y fácil para la codificación de información que puede ser leída por medio de un scanner (unidad lectora por medio de un láser), el cual mide la luz reflejada e interpreta la clave en números y letras, estos son enviados como información a una computadora para su manejo. Los códigos de barras se consideran como la versión impresa del código Morse.

Para codificar datos dentro de un ***símbolo**** impreso, se usa una barra predefinida y patrones de espacios o ***simbología**** para así obtener un patrón que permita crear las barras

Fig. 9
Ejemplos de códigos de barras

---

*__Un símbolo__ *de código de barras es la* __visualización__ *física, es la impresión* __de un código de barras.__

**__Una simbología__ *es* __la forma__ *en que se codifica la información en las barras y espacios del símbolo* __de código de barras__

El código de barras representa la clave esencial para realizar el vínculo a un registro de alguna base de datos que es en donde realmente se guarda toda la información.

2.2.2 Historia de los códigos de barras

1961, Año de la aparición del primer escáner fijo de códigos de barras instalado por Sylvania General Telephone. Este aparato leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles.

1967, La Asociación de Ferrocarriles de Norteamérica (EEUU) aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de adecuado mantenimiento de las etiquetas conteniendo los códigos.

1967, La sucursal de supermercados Kroger de Cincinnati (Ohio, EEUU) instala el primer sistema basado en códigos de barras. Al cliente que encontraba un código que no se podía escanear correctamente se le ofrecía cupones de compra gratis

1969, El láser hace su aparición. Usando luz de gas de Helio-Neón, el primer escáner fijo es instalado. Su costo fue de: $10 000, dólares en la actualidad él mismo tipo de escáner tendría un precio menor de $ 2 000 dólares.

Finales de los años **60`s** y principios de los **70`s** aparecen las primeras aplicaciones industriales pero únicamente para manejo de información. En **1969,** Rust-Oleum fue el primero en interactuar un lector de códigos con un computador (ordenador). El programa ejecutaba funciones de mantenimiento de inventarios e impresión de reportes de embarque.

1970, Aparece la primer terminal portátil de datos fabricado por Norand. Este utilizaba un "wand" o lápiz de contacto.

1971, El código Plessey aparece en Inglaterra (The Plessey Company, Dorset, Inglaterra), es usado para el control de archivos en organismos militares. Su aplicación se utilizo para control de documentos en bibliotecas.

1971, Codabar aparece y encuentra su mayor aplicación en los bancos de sangre, donde un medio de identificación y verificación automática eran indispensables y necesarios.

Buick (la fábrica de automóviles) utilizó identificación automática en las operaciones de ensamble de transmisiones, también por la década de los **70`s**. El sistema era utilizado para conteo de los diferentes tipos de transmisión ensamblados diariamente

1972, ITF aparece, creado por el Dr. David Allais, en aquel entonces de Intermec.

1973, Se anuncia el código U.P.C. (Universal Product Code) que se convertiría en el estándar de identificación de productos. De esta forma la actualización automática de inventarios permitía una mejor y más oportuna compra y reabastecimiento de bienes. Europa se hace presente con su propia versión de U.P.C. En **1976**, el código EAN (European Article Number).

1974, nuevamente el Dr. Allais conjuntamente con Ray Stevens de Intermec inventan el codigo 39, el primero de tipo alfanumérico .

1978, El primer sistema patentado de verificación de códigos de barras por medio de láser aparece en el mercado en.

1980, PostNet, aparece siendo usado por el Servicio Postal de los EEUU. El cual utilizaría el siguiente estilo

1981, La tecnología de CCD (Charge Coupled Device) es aplicada en un escáner. Este tipo de tecnología tiene bastante difusión en el mercado asiático, mientras que el láser domina en el mundo occidental. En ese año también aparece el código 128, de tipo alfanumérico.

Aparece la norma ANSI MH10.8M que especifica las características técnicas de los códigos 39, Codabar, e ITF (Interleaved Two of Five).

1987, El Dr. Allais desarrolla el primer código bidimensional, el código 49.

1987, Ted Williams (Laser Light Systems) con el código 16K

1990, Se publica la especificación ANS X3.182, que regula la calidad de impresión de códigos de barras lineales. En ese año, Symbol Technologies presenta el código bidimensional PDF417.

2.2.3 Estructura representativa del código de barras

En general un código de barras común tiene la siguiente estructura (Fig. 10), la cual se representa por los siguientes puntos:

1. **Quiet zone**

Se le llama así a la zona libre de impresión que rodea al código y permite al lector óptico distinguir entre el código y el resto de información contenida en el documento o en la etiqueta del producto.

2. **Caracteres de inicio y terminación**.

Son marcas predefinidas de barras y espacios específicos para cada simbología. Como su nombre lo indica, marcan el inicio y terminación de un código. En el ejemplo que se muestra son iguales, pero en otras simbologías pueden diferir uno de otro.

3. **Caracteres de datos**.

Contienen los números o letras particulares del símbolo.

4. **Checksum**

Es una referencia incluida en el símbolo, cuyo valor es calculado de forma matemática con información de otros caracteres del mismo código. Se utiliza para ejecutar un chequeo matemático que valida los datos del código de barras. Aunque puede ser importante en cualquier simbología, no son requeridos en todas ellas.

Fig. 10
Estructura del código de barras

Otras características que se deben de mencionar como:

Densidad:

Es la anchura del elemento (barra o espacio) más angosto dentro del símbolo de código de barras. Está dado en mils (milésimas de pulgada). Un código de barras no se mide por su longitud física sino por su densidad.

WNR: (Wide to Narrow Ratio)

Es la razón del grosor del elemento más angosto contra el más ancho. Usualmente es 1:3 o 1:2.

2.2.4 Simbología utilizada en los Código de Barras

La "simbología" es considerada como la forma en que se codifica la información en las barras y espacios para así tener el símbolo de código de barras. Cuando un código de barras es digitalizado, es la simbología la que permite que la información se lea de manera precisa. Y cuando un código de barras se imprime, la simbología permite a la impresora comprender la información que necesita ser turnada dentro de una etiqueta. Pero existen diferentes simbologías, estas dependen de la aplicación donde va a emplearse el código de barras.

El tipo de carácter, numérico o alfanumérico, la longitud de los caracteres, el espacio que debe ocupar el código o la seguridad, son algunos de los factores que determinarán la simbología a emplear.

Existen diferentes simbologías para diferentes aplicaciones, cada una de ellas con diferentes características.

- Numéricas o alfanuméricas
- De longitud fija o de longitud variable
- Discretas o continuas
- Número de anchos de elementos
- Auto verificación.
- Quiet Zone (es el área blanca al principio y al final de un símbolo del código de barras)

EAN / UPC

Universal Product Code (U.P.C.)

UPC es la simbología más utilizada (Fig. 11) en el comercio minorista de EEUU, la cual solo puede codificar únicamente números. El estándar UPC (denominado **UPC-A)** es un número de 12 dígitos.

- El primer digito es llamado "número del sistema". La mayoría de los productos tienen un "1" o un "7" en esta posición. Esto indica que el producto tiene un tamaño y peso determinado, y no un peso variable.
- Los dígitos del segundo al sexto representan el número del fabricante. Esta clave de 5 dígitos (adicionalmente al "número del sistema") es única para cada fabricante, y la asigna un organismo rector evitando códigos duplicados.
- Los caracteres del séptimo al onceavo son un código que el fabricante asigna a cada uno de sus productos, denominado "número del producto".
- El doceavo carácter es el "dígito verificador", resultando de un algoritmo que involucra a los 11 números previos.

  Desde su creación se ha usado entonces en la venta al detalle y la industria alimenticia.

El sistema de codificación EAN es usado tanto en supermercados como en comercios. Es un **estándar internacional**, creado en Europa y de aceptación mundial. Identifica a los productos comerciales por intermedio del código de barras, indicando país-empresa-producto con una clave única internacional. Hoy en día es casi un requisito indispensable tanto para el mercado interno como internacional.

El **EAN-13** es la versión más difundida del sistema EAN y consta de un código de 13 cifras (uno más que el UPC) en la que:

- Los 3 primeros dígitos identifican al país.
- los seis siguientes a la empresa productora.
- los tres números posteriores al artículo,
- finalmente un dígito verificador, que le da seguridad al sistema. Este dígito extra se combina con una o dos de los otros dígitos para representar un código de para, indicando el origen de la mercancía.

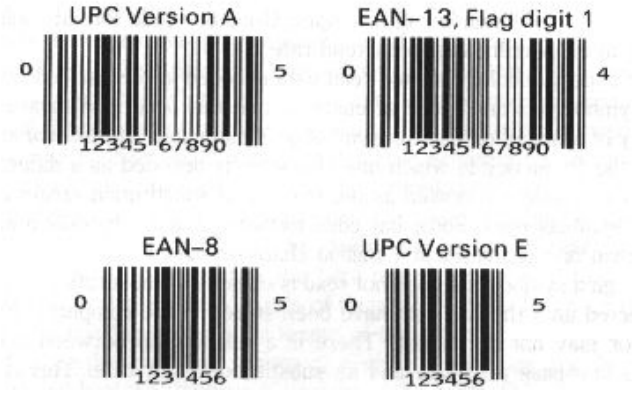


Fig. 11
Simbologías UPC/EAN-13

Código 39

Algunas industrias necesitaban codificar el alfabeto así como también números en un código de barras. Este tipo de simbología (fig.12) no se utiliza para la industria alimenticia. Su uso se aplica para la identificación de inventarios y para

propósitos de seguimiento en las industrias, es por hoy que esta simbología es la más usada para aplicaciones industriales y comerciales para uso interno, ya que entre sus características están la de permitir la codificación de caracteres numéricos, letras mayúsculas y algunos símbolos como -, . $, /, +, % y "espacio". Se utilizan sólo dos grosores tanto para barras como para espacios.

Fig. 12
Simbología código 39

Codabar

Es una simbología de longitud variable que codifica solo números (Fig. 13). Utiliza dos tipos de grosores para barras y espacios y su densidad es similar a la del Código 39 su uso esta enfocado a Bancos de sangre, bibliotecas, librerías.

Fig. 13
Simbología codabar

Código 128

Se utiliza cuando es necesaria una amplia selección de caracteres más de lo que puede proporcionar el Código39. El Código 128 (Fig. 14) utiliza 4 diferentes grosores para las barras y los espacios y tiene una densidad muy alta, ocupando

en promedio sólo el 60% del espacio requerido para codificar información similar en Código 39. Puede codificar los 128 caracteres ASCII.
Cuando la dimensión de la etiqueta es importante, el código 128 es una buena alternativa porque es muy compacta lo que resulta en un símbolo denso. Esta simbología se usa a menudo en la industria de envíos donde el tamaño de la etiqueta es importante.

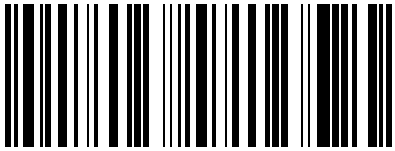


Fig. 14
Simbología código 128

Simbologías bidimensionales

Los datos se encuentran codificados en la altura y longitud del símbolo, y en éstos se puede almacenar gran cantidad datos. La ventajas de utilizar códigos de 2 dimensiones es que el código contiene una gran cantidad de información que puede ser leída de manera rápida y eficaz, sin necesidad de acceder a una base de datos que es en donde se almacena la información La seguridad que son capaces de incorporar éstos códigos los hace casi invulnerables. Con el caso de los códigos unidimensionales para poder estropear la legibilidad de un código de este tipo, basta con agregar otra barra al inicio o final del símbolo o trazar una línea paralela a las barras en cualquier lugar dentro del código. Los códigos de 2D se pueden construir con muchos grados de redundancia, duplicando así la información en su totalidad o sólo los datos vitales. La redundancia aumenta las dimensiones del símbolo pero la seguridad del contenido se incrementa notablemente.

Se han realizado pruebas de resistencia a códigos bidimensionales como el perforándolos, marcándolos con tinta y maltratándolos, antes estas situaciones tan extremas el símbolo es legible aún después de todos estos abusos.

PDF 417

Es un código de dos dimensiones (Fig. 15), la simbología es de alta densidad cuya característica representativa es por ser no lineal. La diferencia entre éste y los otros tipos de **código de barras**, radica en que el PDF417 es en realidad un Portable Data File (Archivo de Información Portátil, PDF) es decir, contiene toda la información, ya que tiene una capacidad de hasta 1800 caracteres numéricos, alfanuméricos y especiales. Un documento como éste tiene un espacio suficiente para incluir información como: nombre, foto, tipo de sangre, rfc, historial del comportamiento y alguna otra información importante.

.

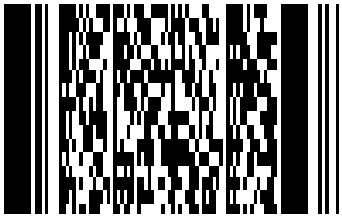


Fig. 15
Simbología PDF 417

Maxicode

Es una simbología de alta densidad creada por UPS (United Parcel Service) está especificada bajo las normas ANSI (MH10.8.3M-1996), la cual es utilizada para procesamiento de información a alta velocidad (Fig. 16).
Su estructura consiste de un arreglo de 866 hexágonos los cuales se utilizan para el almacenamiento de datos en forma binaria. Estos datos son almacenados en forma seudo-aleatoria. Posee un blanco o "bull_eye" utilizado para localizar a la etiqueta en cualquier orientación.
Es posible codificar hasta 100 caracteres en un espacio de una pulgada cuadrada. Este símbolo puede ser decodificado sin importar su orientación con respecto al lector óptico. La simbología utiliza el algoritmo de Reed-solomon para corrección de error. Esto permite la recuperación de la información contenida en la etiqueta cuando hasta un 25 por ciento de la etiqueta este dañado.

Fig. 16
Simbología Maxicode

2.2.5 Lectores ópticos

Los lectores ópticos o scanners son los encargados de captar la información contenida en el código de barras. En general, emiten una línea de luz roja que se refleja en los patrones de luz clara y obscura contenidos en las barras y los espacios.

Dichos reflejos son tomados por un transductor del scanner que los convierte en una señal eléctrica, que a su vez es transformada por el decodificador del scanner en ceros y unos, es decir, al lenguaje binario de las computadoras. Existen en el mercado lectores ópticos de diferentes formas y tamaños:

En forma de pluma o rastrillo (que requieren hacer contacto con el código), de tipo pistola láser, que pueden hacer la lectura a distancia.

2.2.6 Los colores en los códigos de barras

En aplicaciones de código de barras se utilizan distintos tipos de lectores. La fuente de emisión de luz puede producir luz de distintas longitudes de onda. Por esta

razón hay símbolos que son legibles por un tipo de lector y que puede no ser legible si se utiliza otro. Las barras impresas en colores:

- Rojo.
- Amarillo.
- Naranja.
- Púrpura-rojizo u ocre.

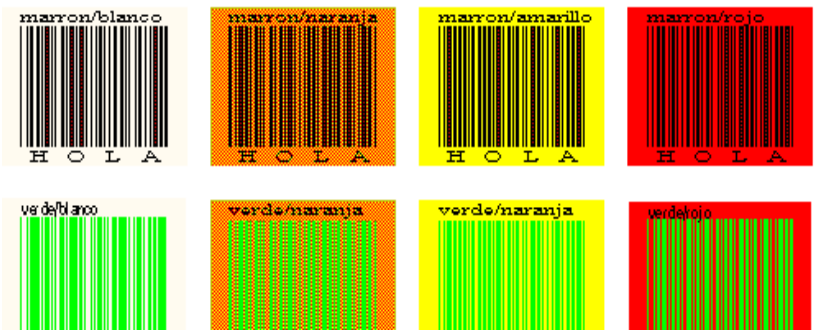
Son ejemplos donde se presentan dificultades para la lectura mediante un lector que emite luz láser roja. Al utilizar tintas con alto componente rojizo para la impresión de barras, se tiene un bajo contraste que afecta la lectura.

Los siguientes colores pueden ofrecer una lectura aceptable:

- Negro, azul, verde y marrón oscuro para las barras**.**
- Blanco, amarillo, naranja y rojo para los espacios.

No significa que los colores ya mencionados (Fig. 2.2.6.1) ofrezcan resultados aceptables. También hay que considerar detalles tales como que el color azul debe tener alto contenido de ciano, el color verde debe tener bajo componente de color amarillo, etc.

Para una mejor información al respecto:
Distribution Symbology Study Group. "Recommended Practices for Uniform Container Symbol/UCS Transport Case Symbol/TCS" Sept. 1981, esta referencia presenta un listado de colores que proporcionan valores de contraste aceptables. Las especificaciones EAN recomiendan combinaciones de colores que proporcionan un contraste de 63 % o más según normas.



Colores aceptables

Colores aceptables

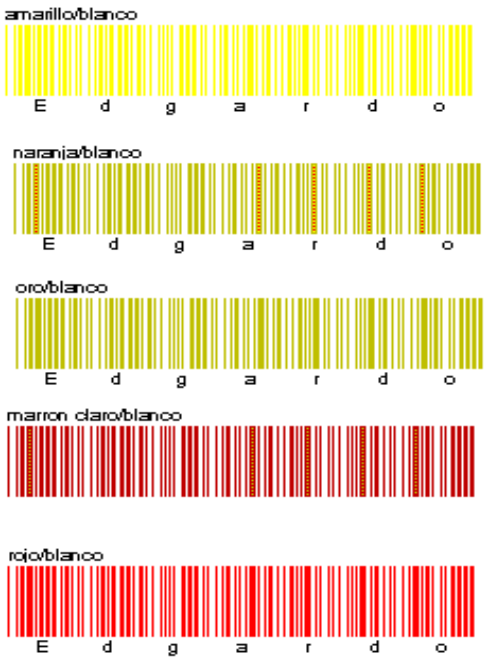


Fig. 2.2.6.1
Colores aceptables en la elaboración de códigos de barras

2.3 Biometría

La biometría tiene el siguiente significado:

> "*Aplicación automatizada de técnicas biométricas utilizadas para medir características corporales o de comportamiento para la autentificación e identificación de personas en sistemas de seguridad*"

Estas técnicas biométricas como se menciona permite la verificación de información contenida en una base de datos por medio de mecanismos como son lectores ópticos para la retina y el iris del ojo, escáner de huella digital, censores verificadores de voz, y entre otros es posible comprobar la autenticidad del individuo y así tener un 100% de seguridad de acceso en cualquier sistema computacional o complejo industrial (Fig. 17).

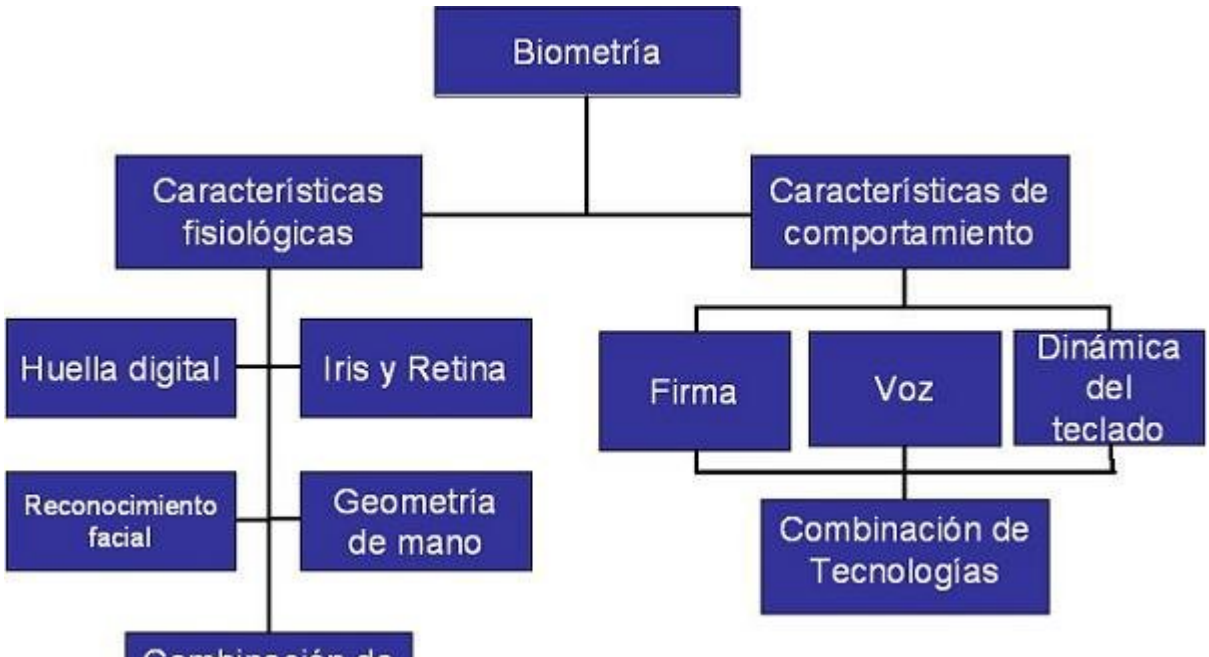


Fig. 17
Biometría como método de identificación y autentificación

En el siglo XIX se da comienzo las primeras investigaciones científicas acerca de la biometría con el fin de buscar y utilizar un sistema de identificación de personas con fines judiciales.

Con estas investigaciones se producen importantes avances y se comienzan a utilizar los rasgos morfológicos únicos en cada persona para la identificación.

Ya en el siglo XX, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación de las personas. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como alternativas de identificación, como por ejemplo el iris del ojo, el calor facial o la voz.

La biometría y la seguridad informática

Como se mencionó la biometría se refiere a la aplicación de técnicas las cuales son capaces de analizar aspectos físicos de una persona para la certificación, autentificación e identificación, en el aspecto computacional esta herramienta es de gran ayuda por el uso de estas técnicas, ya que las características corporales o de comportamiento de las personas permiten establecer una identidad.

Las computadoras o sistemas automatizados no evalúan ningún otro factor al tomar una decisión, sólo se evalúa la identidad. Esto elimina o reduce cualquier factor que pueda comprometer la seguridad.

Ahora con la biometría los sistemas de seguridad utilizan tres métodos de autentificación:

- Algo que la persona sabe: una contraseña, un número de identificación (PIN), etc.
- Algo que la persona tiene: una llave, tarjeta con código de barras, *smart car*d, etc.

Con la biometría podemos agregar otra particularidad además de una contraseña o una tarjeta y es:

- Quién es la persona: seguridad biométrica (identificación del individuo).

De los tres métodos, la biométrica es la más segura y conveniente, ya que permite identificar a un individuo con una exactitud del 100%. Una contraseña puede ser traspasada, robada, descifrada o alterada, una tarjeta puede ser duplicada, se puede alterada pero la identidad de una persona es muy difícil de duplicar o imitar a tal grado que permita engañar a los sistemas automatizados.

2.3.1 Clasificación de técnicas biométricas

Hay ciertos aspectos que se deben de considerar al momento de usar técnicas biométricas, por ejemplo cuando se utiliza la huella digital influye mucho la forma de cómo colocar el dedo para la verificación de la huella, la manera de hablar, si se usa un reconocedor de voz, de ahí que se dividan las técnicas biométricas para entender mejor el funcionamiento de estas y aplicarlas correctamente, las técnicas serán:

- Biometría estática.

- Biometría dinámica.

La biometría estática

Está basada en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen otras también, pero son menos utilizadas, las técnicas basadas en cuanto a la forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La biometría dinámica

La forma de medir las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual.

2.3.1.1 Técnicas biométricas estáticas

Medición de huellas digitales

Las huellas digitales constituyen una de las características del ser humano más singular. La probabilidad de que dos personas tengan la misma huella digital es 1/67 billones. La medición automatizada de la huella digital requiere un gran poder de procesamiento y alta capacidad de almacenamiento. Por esto, los productos biométricos basados en huella digital se basan en rasgos parciales, lo cual aumenta la posibilidad de que dos personas resulten con plantillas similares a valores entre 1/100,000 a 1/1, 000,000, de los más seguros entre los dispositivos

biométricos de seguridad. Los dispositivos biométricos de huella digital son los más usados, son productos de buen precio, mayor cantidad de fabricantes y mayores ventas. Son convenientes y fáciles de usar.

Geometría de la mano

Los biométricos basados en la geometría de la mano miden la forma de la mano por medio de una cámara infrarroja o visual. Ofrecen un buen balance entre la velocidad del análisis de las plantillas y facilidad de uso. Son ideales para uso masivo, como control de asistencia y acceso de entradas. Su uso se ha incrementado en los últimos años.

Retina

Los lectores biométricos de retina analizan los capilares que están situados en el fondo del globo ocular. El usuario debe acercar el ojo al lector y fijar su mirada en un punto. Una luz de baja intensidad examina los patrones de los capilares en la retina. Este procedimiento es intimidante para algunos y hace de los lectores de retina los biométricos más impopulares, es normal que el usuario tenga ciertas dudas acerca del uso de esta técnica, ya que cree que el haz de luz utilizado puede dañar su vista. Para que el lector pueda realizar su trabajo, el usuario no debe tener lentes puestos.

El iris

Los lectores de iris analizan las características del tejido coloreado que se encuentra alrededor de la pupila. Estos biométricos son los menos incómodos de usar de los lectores de ojo, porque no se realiza un contacto cercano con el lector. Además, es una de las tecnologías biométricas más exactas y el usuario puede usar los lentes al momento de la lectura. La facilidad de uso y la integración con otros sistemas no han sido puntos fuertes de los lectores de iris, pero se espera que mejoren con los avances técnicos.

Reconocimiento de cara

Los biométricos que realizan el reconocimiento de cara, analizan las características faciales. Por medio de una cámara digital captura una imagen de la cara, a partir de la cual se crea la plantilla. El uso de esta tecnología es muy enfocado en Europa. Es utilizada principalmente en aplicaciones de identificación. Los casinos los utilizan para identificar estafadores. Complejos comerciales y edificios los utilizan para identificar delincuentes y personas *no gratas.*

2.3.1.2 Técnicas Biométricas Dinámicas

Lectura de firma

La técnica de verificación de firma analiza la manera que el usuario realiza su firma personal. Factores diversos, como la rapidez y presión, son cuantificados, así como la forma de la firma. La verificación tiene uno de los niveles más bajos de exactitud entre los lectores biométricos.

Sin embargo, su familiaridad con los actuales procesos de verificación manual la hace una de las técnicas más fáciles de introducir al usuario.

Reconocimiento de voz

Los biométricos de reconocimiento de voz están basados en la verificación del patrón de voz.

Su implementación puede ser económica si es realizada en computadoras, ya que la mayoría trae el *hardware* necesario: micrófonos y bocinas. Sin embargo, factores ambientales, como el ruido, pueden afectar la verificación. Además, el patrón del reconocimiento de voz es el que más espacio ocupa de todas las tecnologías biométricas, pudiendo llegar hasta 1 MB. Por estas razones, los biométricos de voz son percibidos por los usuarios como dispositivos poco amigables. La tecnología está siendo mejorada y se espera que en el futuro gane popularidad.

Dinámica del tecleo

Se añade la dinámica del tecleo para descubrir cómo se ejerce presión sobre las teclas y con qué velocidad. Estas técnicas combinadas ofrecen una alternativa bastante aceptable ya que un sistema con varias técnicas permiten mayor grado de seguridad, porque se debe de cumplir con cierto orden de identificación, por ejemplo un sistema que esta compuesto de:

- Una identificación por medio de una tarjeta inteligente (incluido un código de barras)
- Lector óptico de huellas digitales
- Lector de retina

permite una mayor autentificación del personal para ingresar a diferentes sistemas, poder acceder a complejos industriales donde la seguridad es la mayor prioridad.

2.3.2 Tokens para la seguridad

Un Token de seguridad, también llamado token de autentificación, el cual es un dispositivo electrónico pequeño que los usuarios llevan consigo mismos para tener el permiso o el acceso a un servicio de red o en una computadora. Dicho dispositivo puede asumir cierta forma:

- De una tarjeta inteligente.
- Puede estar dentro de un llavero.

Los token de seguridad además proporcionan otro aspecto de seguridad utilizando el método conocido como de autentificación de dos factores el cual funciona de la siguiente forma:

El usuario tiene en su poder una identificación personal (PIN), dicha identificación lo acredita como el propietario del dispositivo (computadora); después de comprobar al dueño, el dispositivo despliega un número que identifica en forma única al usuario ante el sistema, permitiéndole ingresar.

El número de identificación de cada usuario es cambiado con frecuencia, (cada cinco minutos). A diferencia de una contraseña, un token de seguridad es un objeto físico. Una de sus ventajas de éste objeto, es que al ser robado, perdido o usado por otra persona, no se puede funcionar para acceder a la red o a cualquier computadora o sistema, ya que necesita el PIN o identificación personal.

3 Seguridad en Internet

3.1 las redes de computadoras

Una red de computadoras son una serie de equipos conectados entre si (desde dos computadoras conectadas directamente una de otra se considera una red) a través de un cable o una señal (láser, microonda, satélite), las cuales tienen como función el comunicarse con otras computadoras y compartir archivos y periféricos. (Fig.3.1.1)

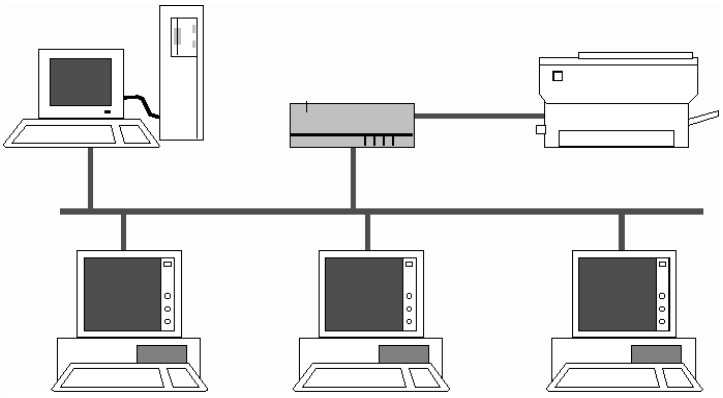


Fig. 3.1.1
Red de computadoras

Las redes están diseñadas para cumplir ciertos objetivos:

- Lograr que todos sus programas, datos y equipo (periféricos que estén conectados y compartidos) estén disponible para cualquiera de las computadoras de la red que lo solicite, sin importar la ubicación o localización física del recurso
- Proporcionar una alta fiabilidad, al contar con otras fuentes que suministran información, es decir que todos los archivos pueden duplicarse en dos o tres máquinas, de modo que si una de ellas no se encuentra disponible o llegara a fallar, se pueda utilizar alguna otra de las otras copias.
- La presencia de varios CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque el rendimiento en general llegue a ser menor.
- El ahorro económico debido a que los ordenadores pequeños tiene una mejor relación costo / rendimiento, en comparación con la que ofrece las máquinas grandes.
- Proporciona un gran y poderoso medio de comunicación entre computadoras que se encuentran en lugares distantes.

3.1.1 Componentes Básicos de una Red

Servidor

Se le llama servidor a la computadora utilizada para controlar todo el sistema de archivos de la red, es decir permite la transmisión de datos (información) a otras computadoras que se encuentran en la red, proporciona servicio de impresoras, también puede ser capaz de compartir el Internet a todas aquellas computadoras que se encuentren en la red interna convirtiéndose así en un servidor proxy.

Entre las funciones que debe de realizar un servidor se encuentran las siguientes:

Procesar las peticiones realizadas por la estación de trabajo (computadora que se encuentra en red) desde:

- El acceso a disco duro del servidor (con previa autorización del mismo).
- Petición de impresión al dispositivo que se encuentra conectado al servidor (impresora).
- Solicitud de algún programa o aplicación que reside en el disco del servidor.
- Comunicación a otra computadora a través del servidor.

Como el servidor es el encargado de gestionar las peticiones de todas las computadoras, su carga de trabajo puede ser muy pesada. Se puede entonces llegar a una congestión de datos, el tráfico puede ser tan grande que puede impedir la recepción de algunas peticiones enviadas desde cualquier otra PC.

Así que cuanto mas grande sea la red, resulta más importante tener un servidor con características mas adecuadas para que logre realizar su trabajo algunas de estas características son:

- Grandes cantidades de memoria RAM para optimizar los accesos a disco y mantener las colas de impresión.
- Un procesador con mayor velocidad.
- El factor de estados de espera.
- El tamaño del canal.
- El tamaño del bus.
- La memoria caché así como de otros factores.

Estaciones de Trabajo (computadoras)

A diferencia de el servidor, las estaciones de trabajo son computadoras con características básicas en cuanto a memoria RAM, velocidad de procesador, espacio en disco duro. Estas estaciones se pueden conectar a través de tarjeta de red u otro medio como es por los puertos serial o paralelo,

Sin embargo las estaciones de trabajo son, generalmente, sistemas inteligentes, que se encargan de sus propias tareas de procesamiento.

Tarjetas de Conexión de Red (Network Interface Card)

Para que exista comunicación entre computadoras es necesario contar con una tarjeta de red (NIC) el cual es el "hardware" utilizado para transmitir y recibir información.

La tarjeta de red un dispositivo de expansión de la computadora y proporciona un puerto en la parte trasera de la PC (conector del tipo RJ45) al cual se conecta el cable de la red. Actualmente los equipos ya tienen integrada una interfaz de red, además de la tarjeta de red, es necesario otro dispositivo, el cual se conecta al medio de comunicación (cable de red) y a la tarjeta,

3.1.2 Medios de comunicación (cableado)

La forma en la que las computadoras logran establecer una comunicación es a través de un medio (cable), el cual permite la transmisión de los datos a otras computadoras en la red. Existen algunos tipos de cable los cuales son:

- Par trenzado.
- Cable coaxial y
- Fibra óptica.

De acuerdo al tipo de cable o método que se vaya a utilizar, es conveniente tener en cuenta sus ventajas y desventajas.

Algunos son propensos a interferencias, mientras que otros no pueden usarse por razones de seguridad.

La velocidad y longitud del tendido son otros factores a tener en cuenta el tipo de cable a utilizar.

Par Trenzado

Consiste en dos hilos de cobre trenzado, aislados de forma independiente y trenzados entre sí. Está cubierto por una capa aislante externa. Sus principales ventajas son:

- No se requiere de conocimientos amplios para su instalación
- La instalación es rápida y fácil
- La emisión de señales al exterior es mínima.
- Ofrece alguna inmunidad frente a interferencias, modulación y corrosión.

Algunas de sus desventajas son:

- Si se encuentra cerca de una conexión eléctrica provoca perdida de información
- Un mal ponchado de cable provoca que la computadora se desconecte de la red
- a una distancia de más de 100mts. ocasiona una comunicación lenta o perdida total de datos

Cable Coaxial

Esta formado de un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra. Entre el hilo conductor y la malla hay una capa gruesa de material aislante, y todo el conjunto está protegido por una cobertura externa. El cable está disponible en dos espesores: **grueso y fino**.

- El cable **grueso** soporta largas distancias, pero es más caro.
- El cable **fino** puede ser más práctico para conectar puntos cercanos.

Las ventajas del cable coaxial son:

- Soporta comunicaciones en banda ancha y en banda base.
- Es útil para varias señales, incluyendo voz, video y datos.

Las desventajas del cable coaxial son:

- Se necesita tener una topología en anillo.
- Si se desconecta una computadora de la red provoca que todas las demás computadoras no se puedan comunicar entre si.
- Es un medio obsoleto que ya no se usa

Conexión fibra óptica

Este tipo de cable es bastante caro, pero una de sus características excepcionales es que permite transmitir la información a gran velocidad e impide la intervención de las líneas.

Como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctricas o emisión de señal.

El cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta.

La fibra está encapsulada en un cable protector. Sus ventajas son:

- Alta velocidad de transmisión
- No emite señales eléctricas o magnéticas, lo cual redunda en la seguridad
- Inmunidad frente a interferencias y modulación cruzada.
- A mayores distancias no se pierde la señal.

Sus desventajas son:

- Es un medio que resulta un poco costoso.
- Se necesita de equipo especializado para la creación de cables
- Si se llega a crear un cable que sea inútil para la comunicación es un cable que se desecha.

3.1.3 Tipos de redes

Las redes de computadoras se pueden clasificar según su extensión y su topología. Una red puede comenzar siendo red pequeña para crecer junto con la organización o institución.

Los diferentes tipos de red son:

- Red de área local (LAN)
- Red Campus
- Red de Área Metropolitana (MAN)
- Red de Área Extensa (WAN y redes Globales)

Red de área local (LAN)

Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.

Red de Campus

Una red de campus se extiende a otros edificios dentro de un campus o área industrial. Los diversos segmentos o LAN de cada edificio suelen conectarse mediante cables de la red de soporte.

Red de área metropolitana (MAN)

Una red MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

Red de área extensa (WAN y redes globales)

Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

3.1.4 Topologías de redes de computadoras

La topología o forma lógica de una red se define como la forma de conectar las computadoras por medio del cable; por muros, suelos y techos del edificio.

Existe un número de factores a considerar para determinar cual es la topología más apropiada.

Las topologías más comunes son:

Anillo

Las computadoras están unidas unas con otras formando un círculo por medio de un cable común (utilizado mas el cable coaxial como medio de comunicación). El último nodo de la cadena se conecta al primero cerrando el anillo (Fig. 3.1.4). Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. Esta topología tiene una gran desventaja, si se rompe una conexión, ocasiona que la red se caiga por completo.

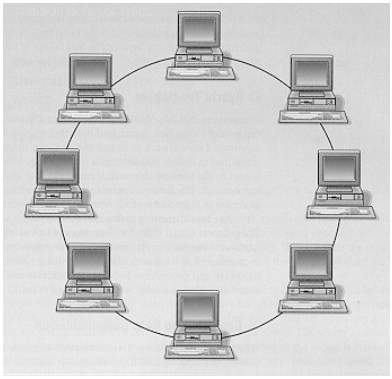


Fig. 3.1.4
red anillo

Estrella

La red se une en un único punto, normalmente con un panel de control centralizado (Fig. 3.1.4.1), como un concentrador (switch, Hub, Router, etc.). Los bloques de información son dirigidos a través de este concentrador hacia sus destinos. Este esquema tiene una ventaja al tener un punto de concentración ya que este monitorea el tráfico y evita las colisiones, y si alguna de las computadoras se desconecta o falla esta no afecta al resto de la red.

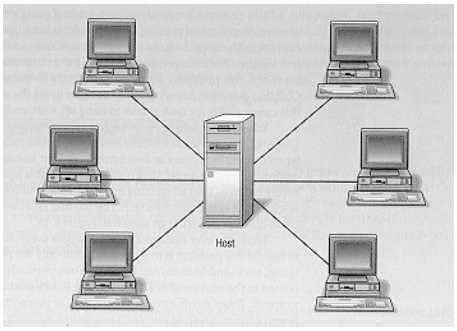


Fig. 3.1.4.1
red estrella

Bus

Las estaciones están conectadas por un único segmento de cable (Fig. 3.1.4.2). A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

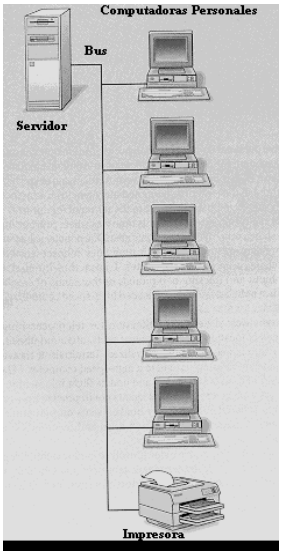


Fig. 3.1.4.2
red bus

Híbridas

Las redes bus, estrella y el anillo se combinan algunas veces para formar redes llamadas redes híbridas (Fig. 3.1.4.3). Algunos ejemplos son:

Anillo en estrella

Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

Bus en estrella

El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Estrella jerárquica

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

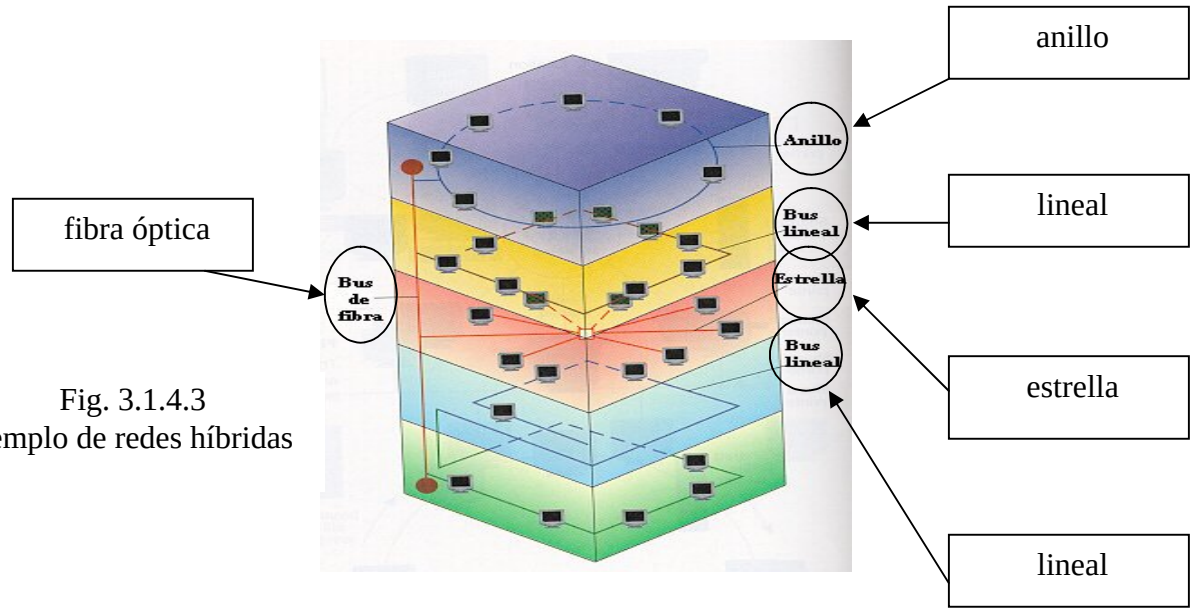


Fig. 3.1.4.3
Ejemplo de redes híbridas

3.1.5 Modelo OSI y Protocolo TCP/IP

El modelo OSI (Open System Interconection) es el modelo más utilizado por la todas las redes utilizadas en el mundo, creado por el ISO (Organización Internacional de Normas). El modelo OSI esta formado por siete niveles o capas donde cada una de ellas estan establecidas las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas o redes que necesiten comunicarse. Cada nivel o capa depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores para tener un control total de los datos que se manejan.

Las capas o niveles que forman al modelo OSI son los siguientes:

1.- Capa física

Esta capa (nivel) es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión (cableado),a través de impulsos los cuales pueden ser:

- eléctricos (transmisión por cable).
- electromagnéticos (transmisión inalámbrica).
- luminosos (transmisión óptica).

Otro aspecto que el cual se encarga la capa de física es el de la interpretación de las señales eléctricas.

Cuando actúa en modo de receptor el trabajo se realiza a la inversa; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

2.- Capa de enlace

Esta capa traslada los mensajes desde la capa física a la capa de red y viceversa. Especifica la forma de como se organizan los datos cuando se transmiten en un medio particular (ya mencionados). Además se encarga de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques ("Frames"), e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad.

Los datagramas recibidos son comprobados por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío.

La capa de enlace esta dividida en dos subcapas:

- **Control lógico de enlace LLC** ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.
- **Control de acceso al medio MAC** ("Medium Access Control"). Esta subcapa actúa como controladora del hardware utilizado para la comunicación (el adaptador de red). El controlador de la tarjeta de red es denominado a veces como "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección MAC ("MAC address"). Su principal tarea (que le proporciona el nombre -control de acceso-) consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte.

3 Capa de Red

Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada ("Routing"), esta capa no se ocupa de los errores o pérdidas de paquetes. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. Esta capa puede subdividirse en dos:

- **Transporte**. Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. En esta categoría se encuentra el protocolo **IP**
- **Conmutación** ("Switching"): Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario). Los routers son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. Aquí se encuentra el protocolo **ICMP** ("Internet Control Message Protocol"), responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante PING

4 Capa de Transporte

La función que desempeña esta capa es la de garantizar la fiabilidad del servicio. Además define cuando y como debe utilizarse la retransmisión para asegurar la llegada de loa paquetes, para que esta función se lleve acabo divide el mensaje recibido de la capa de sesión en partes (datagramas), los enumera y los entrega a la capa de red para su envío. Durante la recepción, si la capa de red utiliza el protocolo IP, la capa de transporte es responsable de reordenar los paquetes recibidos fuera de secuencia.

5 Capa de Sesión

Es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, pero son pocas las aplicaciones que hacen uso de ella. Por ejemplo, las comunicaciones de Internet no la utilizan.

6 Capa de Presentación

Esta capa se ocupa de la semántica de la comunicación (describe la sintaxis de los datos a transmitir), estableciendo los arreglos necesarios para que se puedan comunicar entre si máquinas que utilicen diversa representación interna para los datos.

Un ejemplo: describe como pueden transferirse números de punto flotante entre equipos que utilizan distintos formatos matemáticos. Esta capa es considerada para la mejor para implementar aplicaciones de criptografía.

7 Capa de Aplicación

En esta capa se describe la forma en el como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia de ficheros etc.).

Protocolo TCP/IP.

Éste protocolo se diseño a finales de los años 60's como base de la red ARPANET la cual conectaba las computadoras de oficinas gubernamentales y universitarias. Funciona bajo el concepto de cliente servidor, lo que quiere decir que alguna computadora solicitaba los servicios de otra; de las cuales la primera era el cliente y la segunda el servidor.

ARPANET evolucionó para lo que ahora se conoce como INTERNET y con ello también evolucionó el protocolo TCP/IP. El cual se organiza en sólo tres niveles: el de red, transporte y aplicación.

En comparación con el protocolo OSI la capa de red de TCP/IP equivale a la capa de red de OSI.

La capa de transporte de TCP/IP equivale a la capa de transporte de OSI y la capa de aplicación de TCP/IP equivale a las capas de sesión, presentación y aplicación todas en conjunto del protocolo OSI.

El protocolo TCP/IP no especifica nada a cerca del hardware de red por lo que las capas de enlace de datos y físicas no existen.

1.-Capa de Red de TCP/IP.

La capa de red se encargan de encaminar (ruteo) la información a través de una red de área amplia. Existen dos protocolos en este nivel, uno de ellos conocido como **IP** (Internet Protocol) que es probablemente el protocolo de routing más utilizado; también existe una versión más simplificada de IP conocida como ICMP que se encarga de encaminar paquetes sin ningún esquema de seguridad pero a mayor velocidad, se utiliza en particular para transmisión de correos electrónicos.

2.-Capa de Transporte.

La capa de Transporte de TCP/IP ofrece dos protocolos:

- TCP para redes orientadas a conexiones
- UDP para redes no orientadas a conexión.

Otra característica de la capa de transporte es que a diferencia del modelo OSI pueden trabajar a nivel local sin necesidad de enrutamientos ni partición o segmentación de paquetes.

También es importante hacer notar que en el nivel capa de transporte no existe control de flujo ni verificación de errores para administrar los paquetes que circula por la red. Sin embargo, algunas implementaciones particulares del TCP/IP como la de Windows si contempla esquemas de verificación de errores.

3.-Capa de Aplicación para TCP/IP.

La capa de aplicación de TCP/IP cuenta con funciones idénticas a los que cuenta el modelo OSI pero incluyen ciertas características, que en el protocolo del modelo OSI corresponden a las capas de presentación y de sesión. Entre ellos se encuentran:

- **Telnet:** servicio de terminal remota para permitir a un usuario remoto acceder a los servicios de un servidor como si tuviera conexión directa.
- **FTP:** protocolo para transferencia de archivos y servicios de directorio entre terminales remotas.
- **SMTP:** protocolo para correo electrónico.
- **Kerberos:** protocolo que ofrece servicios de encriptación y codificación de información y otros esquemas de seguridad para aplicaciones de usuario.
- **TNS:** este protocolo permite mapear las direcciones lógicas de una terminal a un nombre simbólico más fácilmente identificable pro los usuarios de la red. Ese servicio a su vez es utilizado por otros servicios como el de correo electrónico y FTP.

Todos estos servicios están basados en TCP/IP a nivel capa de transporte y aunque son más simples de usar no son tan seguros, entre ellos están:

- **RCP:** Este protocolo se utiliza para que los programas de usuario estén accesibles a otros usuarios en la red ofreciendo a estos últimos una interfaz con el primero.
- **TFTP**: Idéntico a ftp pero sin verificación de errores.

Existe además un servicio orientado a los administradores de red, conocido como SNMP que permite monitorear a las terminales en red, a los usuarios, a los servicios y finalmente a los recursos existentes en la red.

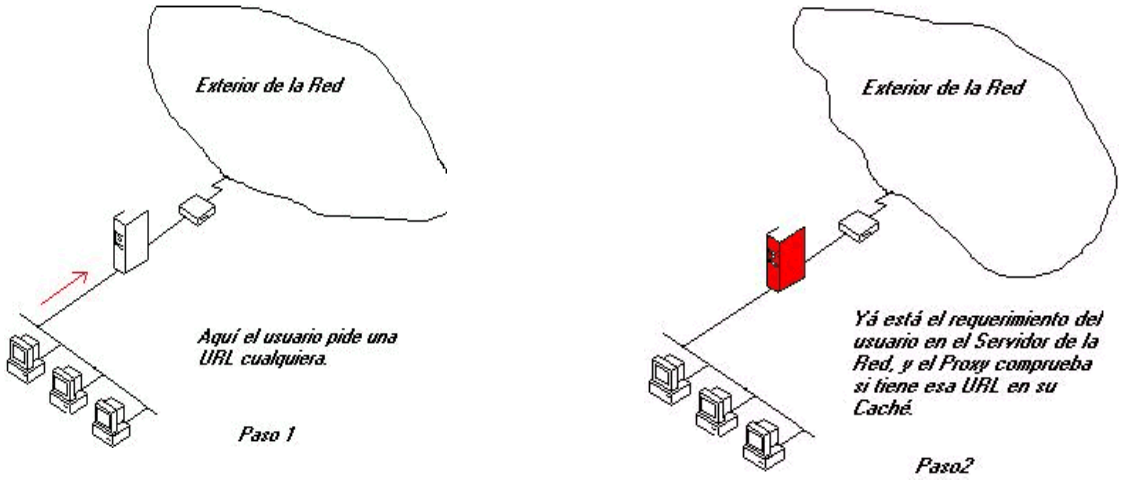
3.2 Servidor Proxy como medio de conexión a internet

Es el encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

Funcionan abriendo un socket (puertos) en el servidor y permitiendo la comunicación con la internet a través de él.

Un servidor Proxy bien configurado, es completamente seguro. No dejan que nadie entre a través de ellos.

Las siguientes figuras muestran como ejemplo el funcionamiento del servidor proxy en una red interna. (fig.3.2.1)



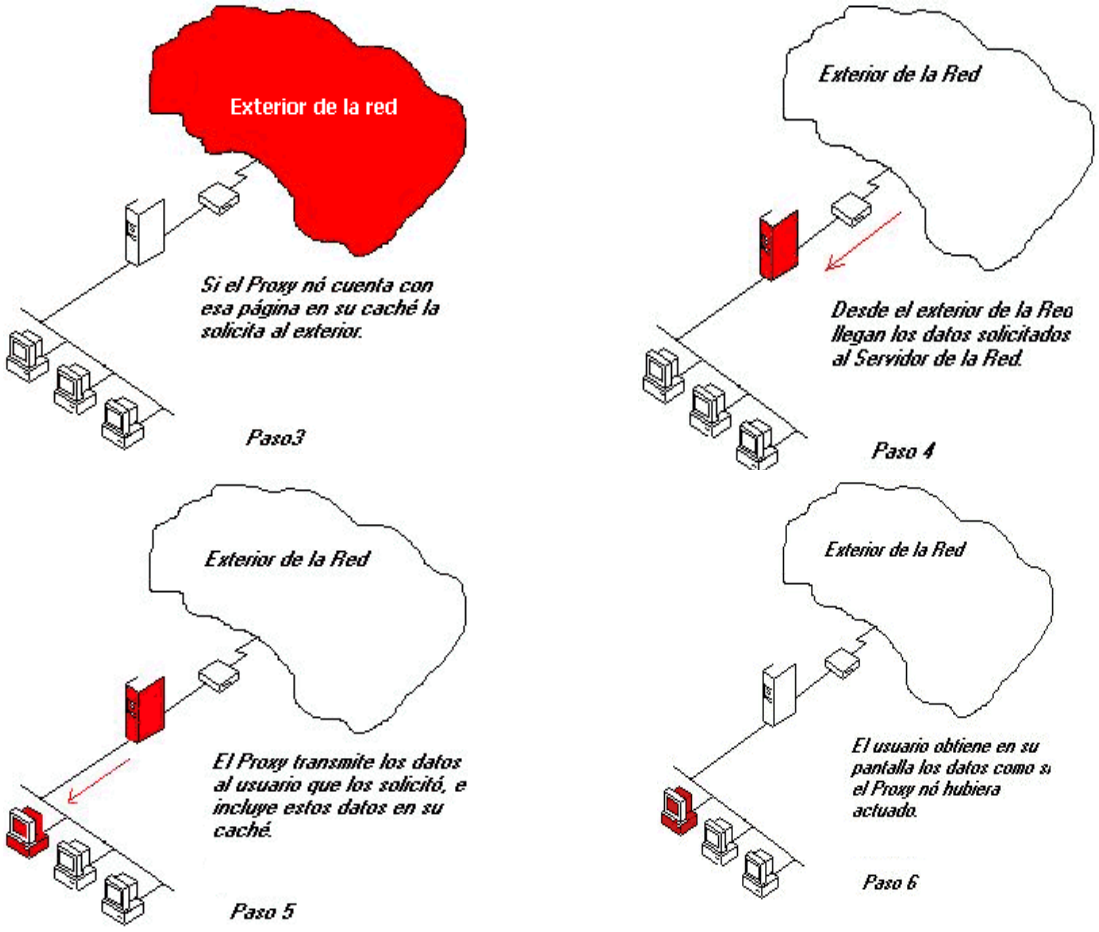


Fig. 3.2.1
Funcionamiento del servidor proxy

Ventajas de un servidor Proxy:

Las ventajas que ofrece la utilización de un Proxy en una red local son las siguientes:

- **Bajo costo**: El programa y la instalación tienen un precio menor que cualquier R*outer**.
- La utilización de **una** sola **línea telefónica**: Sólo es preciso disponer de una línea telefónica normal u otras como conexión ADSL, Cable, RDSI, etc.

Router
Son equipos de interconexión que permite enlazar dos redes mejorando el rendimiento de la transmisión entre las redes conectadas.

- **Fácil instalación**: La instalación emplea los dispositivos de la propia red local, por lo que se reduce a la configuración de los programas.
- **Seguridad**: El servidor Proxy también actúa como una barrera (*firewall*) adicional para limitar el acceso a la red local desde el exterior.
- **Dirección IP única**: El número IP es el que identifica a un ordenador en internet. Si se utiliza un Proxy basta un IP para toda la red local en lugar de un IP para cada uno de los ordenadores.
- **Conexión automática** (*autodialing)*: No es necesario que la computadora que actúa como Proxy esté conectado permanentemente internet. Con esta función cada vez que un usuario desea entrar a internet, el servidor Proxy establece la conexión. Del mismo modo el Proxy la desconecta cuando no hay ninguna petición de conexion, todo ello automáticamente

Servicios que ofrece un Servidor Proxy:

El Proxy puede ofrecer a los equipos que forman de la red local la mayoría de los servicios de Internet. Entre los más comunes se encuentran:

- Correo electrónico.
- World Wide Web.
- Transmisiones FTP.
- Telnet.
- News.

3.3 Redes V.P.N.

Una VPN (Virtual Private Network) red privada virtual, es un grupo de dos o mas computadoras conectados a una red privada (conexión que la provee una organización independiente) proporcionando acceso restringido, comunicación "con seguridad" sobre una red publica (Fig. 3.3.1) utilizando métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas computadoras. Usando una VPN, se crea una conexión privada segura a través de una red publica como internet.

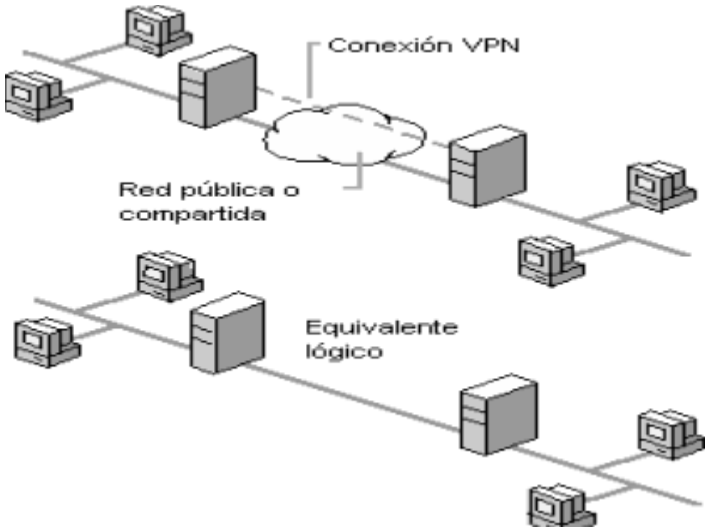


Fig. 3.3.1
V.P.N.

En un principio existían dos tipos de VPN las cuales sentaron las bases para los que hoy es la V.P.N. y son :

- **V.P.N. confiable**
- **V.P.N. segura**

VPN confiable

Anteriormente, una VPN consistía en uno o más circuitos (dispositivos) rentados a un proveedor de comunicaciones. Cada circuito rentado actuaba como un cable independiente, el cual era manejado por el cliente. La idea básica era que el cliente usara el circuito de la misma manera en que usaba los cables físicamente en su red local.

La única privacidad que contaban estas redes VPN era manejada por el proveedor del servicio de comunicación; ya que nadie más podía usar el mismo circuito, esto permitía a los clientes tener su propia dirección IP y políticas de seguridad independientes. Un circuito rentado corría sobre uno o más de un switch de comunicación, de los cuales, cualquiera podía ser alterado por alguno de los operadores que tratara de monitorear el tráfico de las líneas.

El cliente VPN tenía que confiar la integridad de los circuitos y de la información en el proveedor de servicio VPN; por este motivo este tipo de redes era llamada VPN confiable.

Existen ciertos requerimientos de las VPN confiables:

- Nadie más que el proveedor VPN puede afectar o modificar el canal en la VPN.
- El direccionamiento y el enrutamiento usado en una VPN confiable, deberán ser establecidos antes que la VPN sea creada.

VPN segura

Después de que internet se convirtió en el medio más popular como forma de comunicación a nivel empresarial, la seguridad tomo mayor importancia. Con el antecedente de las VPN confiables, se decidió mejorar aspectos que no afectaran la privacidad de la información y que además se mantuviera la integridad de los datos enviados.

Se empezaron a crear protocolos (reglas) que permitieran la encriptación del tráfico en algún extremo de la red, que se moviera a través de la Internet como

cualquier otra información, para luego ser descifrado cuando alcanzara la red de la corporación o al destinatario.

El tráfico cifrado o encriptado actúa como si estuviera en un túnel entre dos redes. Aún cuando un atacante pudiera ver o interceptar el tráfico, no podría leerlo y no le haría cambios sin que el destinatario lograra enterarse de dichos cambios.

Las redes que eran construidas usando elementos de encriptación se llamaban VPN seguras. La razón principal por la que las empresas usan VPN seguras es que de esta forma pueden transmitir información sensible a través de internet, sin preocuparse de que personas ajenas puedan ver los datos que fluyen sobre la VPN. Por este motivo las VPN seguras deben de cumplir con ciertos requerimientos:

- Todo el tráfico que circula en una VPN segura debe estar encriptado y autentificado.
- Las propiedades de seguridad deben de estar en común acuerdo por las partes de la VPN (cliente/servidor).
- Nadie fuera de la VPN puede afectar las propiedades de la VPN. Debe ser imposible para un atacante cambiar las propiedades de seguridad de cualquier parte de la VPN.

VPN híbrido

Una VPN segura podía ser el complemento de una VPN confiable, creando así un tercer tipo llamado VPN híbrido. Las partes que dan lugar a la seguridad de una VPN híbrida pueden ser controladas por los clientes o por el proveedor, siendo el último quien maneja la parte confiable de la VPN o para efectos de entendimiento la conexión hacia la Internet.

Requerimientos para las VPN híbridas:

Ventajas de las redes VPN

- **Reducción de costos**: El costo total de conectividad se reduce debido a la eliminación de servicios como son pagar renta en una o varias líneas telefónicas, y equipo de acceso dial-up (marcado telefónico).
- **Escalabilidad**: Las VPN son arquitecturas de red más escalables y flexibles que las WAN tradicionales, debido a que permiten a las corporaciones agregar o eliminar sus sistemas localizados remotamente, trabajadores a distancia (vendedores) o aliados comerciales de forma fácil y poco costosa en función de las necesidades del negocio.
- **Seguridad**: La conexión a través de Internet es cifrada (codificada). El servidor de acceso remoto exige el uso de protocolos de autentificación y cifrado. Los datos confidenciales quedan ocultos a los usuarios de Internet, pero los usuarios autorizados pueden tener acceso a ellos a través de la VPN.
- **Diseño de red simplificado**: Un diseño de red con tecnología VPN se simplifica en términos de diseño de arquitectura, flexibilidad y mantenimiento, debido a que se reducen los costos asociados a la gestión de red.
- **Compatibilidad**: Como se aceptan la mayor parte de los protocolos de red más comunes (incluidos TCP/IP, IPX y NetBEUI), las VPNs puede ejecutar de forma remota cualquier aplicación que dependa de estos protocolos de red específicos.
- **Administración centralizada**: Algunos proveedores soportan la característica de administración centralizada de sus productos VPN. Esto representa una fuerte característica de seguridad y un buen mecanismo para la resolución de problemas.
- **Prioridad de Tráfico**: Algunos proveedores ofrecen la funcionalidad de priorizar tráfico en sus productos VPN. Esto agrega gran flexibilidad a la corporación en cuanto a la utilización de los enlaces de Internet, debido a

que se puede decidir en qué orden se preserva el ancho de banda según el tipo de tráfico permitido y de acuerdo a su importancia.

Tecnología de túnel

Las redes privadas virtuales (VPN) crean un túnel de un origen a un destino (Fig. 3.3.2) para poder transferir datos, a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos e información sean casi invisibles para los extraños.

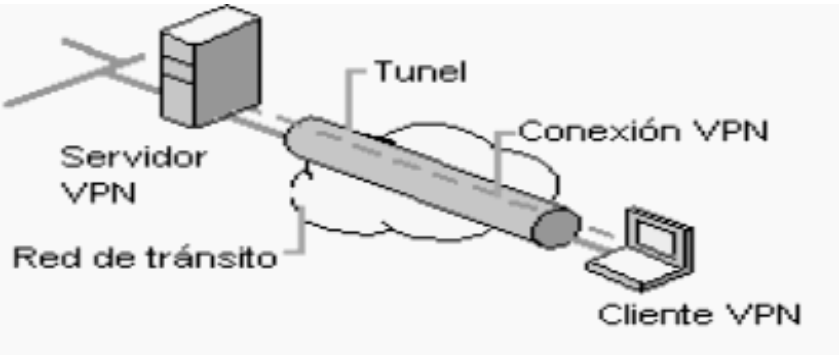


Fig. 3.3.2
Tecnología de túnel

El servidor busca mediante un router la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

Protocolos de Túnel.

Cuatro diferentes protocolos de túnel son los más usados para la construcción de VPN sobre la Internet:

- Protocolo de túnel punto - punto (PPTP).
- Envío de capa 2 (L2F)
- Protocolo de túnel de capa 2 (L2TP)

- Protocolo de seguridad IP (IPSec)

Protocolo PPTP:

Este protocolo fue utilizado como un mecanismo de encapsulamiento, permite una variedad de mecanismos de autentificación y algoritmos de encriptación.

La compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, dentro de sus productos los cuales han sido muy solicitados (Windows 98/ME, NT4, 2000) los cuales llevan incluidos estos protocolos.

Fue desarrollado por el Forum PPTP que esta constituido por la siguientes organizaciones:

- Ascend Communications.
- Microsoft Corporation
- 3 Com/Primary Access
- ECI Telematics
- U.S. Robotics.

La seguridad del protocolo PPTP

La seguridad es una de las características de este protocolo, el cual se divide en tres áreas las cuales son:

- Autentificación.
- Encriptación de datos.
- Filtrado de paquetes PPTP.

Las cuentas de usuarios son configuradas para que solo los usuarios específicos tengan acceso a la red. El uso de passwords seguras es uno de las mejores formas de utilización exitosa del PPTP.

Encriptación de Datos

Los datos que circulan por el túnel PPTP son encriptados desde origen ya sea este origen desde el cliente o servidor, viajan a través del túnel, y son desencriptados en el destino. los datos son invisibles al resto del mundo, dando así seguridad a la información.

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si esta activada en el servidor PPTP. Cuando esta activa acepta y enjuta solo los paquetes PPTP de los usuarios autorizados. Esto prevé el resto de paquetes entren el red privada y en el servidor de PPTP.

Ha sido utilizado para la implementación de VPN's de acceso remoto. El protocolo más común que se usa para acceso remoto es el protocolo de punto - punto (PPP); PPTP se basa en la funcionalidad de PPP para proveer acceso remoto que puede estar dentro de un túnel a través de la Internet hacia su destino. PPTP encapsula los paquetes PPP usando una versión modificada del encapsulado genérico de ruteo (Generic Routing Encapsulation GRE), lo que da al protocolo PPTP la flexibilidad de manejo de otros protocolos como: intercambio de paquetes de Internet (IPX) y la interfaz gráfica de sistema básico de entrada / salida de red NetBEUI. PPTP está diseñado para correr en la capa 2 del sistema OSI (Open System Interconnection) o en la capa de enlace de datos. Al soportar comunicaciones en la capa 2, se permite transmitir protocolos distintos a los IP sobre los túneles. Una desventaja de este protocolo es que no provee una fuerte encripción para proteger la información y tampoco soporta métodos de autentificación basados en tokens.

- **L2F** fue diseñado como protocolo de túnel de tráfico desde usuarios remotos hacia los corporativos. Una diferencia entre PPTP y L2F es que el túnel creado por L2F no es dependiente en IP, y le permite trabajar directamente con otro tipo de redes como frame relay o ATM. Al igual que PPTP, L2F emplea PPP para la autentificación del usuario remoto. L2F permite túneles para soportar más de una conexión.
- **L2TP** es un protocolo de capa 2, y permite a los usuarios la misma flexibilidad que PPTP para manejar protocolos diferentes a los IP, como IPX y NetBEUI. L2TP es una combinación de PPTP y L2F, y puede ser implementado en diferentes topologías como Frame Relay y ATM. Para proveer mayor seguridad con la encripción, se pueden emplear los métodos de encripción de IPSec. La recomendación es que para procesos de encripción y manejo de llaves criptográficas en ambientes IP, el protocolo IPSec sea implementado de manera conjunta.
- **IPSec** nació con la finalidad de proveer seguridad a los paquetes IP que son enviados a través de una red pública, trabaja principalmente en la capa 3. IPSec permite al usuario autentificar y/o cifrar cada un de los paquetes IP. Al separar las aplicaciones de autentificación y encriptación de paquetes, se tienen a dos formas deferentes de usar IPSec llamadas modos. En el modo de transporte sólo el segmento de la capa de transporte de un paquete IP es autentificado y encriptado. En el otro modo llamado de túnel, la autentificación y encriptación se aplica a todo el paquete. Mientras que el modo de transporte es útil en muchas situaciones, el modo de túnel provee mayor seguridad en contra de ataque y monitoreo de tráfico que pueda ocurrir sobre la Internet. A su vez este protocolo se subdivide en dos tipos de transformaciones de datos: el encabezado de autentificación (AH) y la carga de seguridad encapsulada (ESP).

3.4 Protocolo de seguridad WEP

Red Inalámbrica

En la cual los medios de unión y de comunicación entre las estaciones (computadoras) son frecuencias de radio o infrarrojos.

Entre las ventajas que brindan las redes inalámbricas son que permiten una amplia libertad en cuanto a movilidad, facilidad en la reubicación de las estaciones de trabajo evitando la necesidad de realizar la conexión por medio de cableado.

Algunas de las técnicas utilizadas para el uso de las redes inalámbricas son:

- Infrarrojos.
- Microondas.
- Láser y radio.

La seguridad es un aspecto esencial cuando se toca el tema de las redes inalámbricas. Cuando en una red inalámbrica desplegada en una oficina una persona ajena a la oficina tercero podría acceder a la red sin ni siquiera estar ubicado en las instalaciones de la misma, bastaría con que se encontrara en un lugar próximo donde le llegará la señal. Es una forma de ataque pasivo, donde sólo se escucha la información, y la desventaja de esto es ni siquiera se dejan huellas que posibiliten una identificación posterior, pero el ataque activo el cual consiste inyectar nuevos paquetes o modificar los ya existentes.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i, que permitiera dotar de suficiente seguridad a las redes WLAN. El problema de 802.11i está siendo su tardanza en ver la luz. Su aprobación se

espera para finales de 2004. Algunas empresas en vistas de que WEP (de 1999) era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como son las VPNs para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN.

Definición de WEP

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec.

Estándar IEEE 802.11

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP (Wireless Equivalent Privacy); su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

El elemento de seguridad que más se usa en redes WIFI es la encriptación WEP que consiste en cifrar los datos enviados mediante una clave alfanumérica que sólo el usuario conoce, pero fácil de traspasar. Sin embargo desde hace algún tiempo se está empezando a usar otro método de cifrado, el WPA aunque también presenta diversas vulnerabilidades ante un intruso, las cuales son:

Cifrado:

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida.

El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un *valor de comprobación de integridad* (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro.

El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

Autentificación:

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN.

Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red

Características

Según el estándar ya establecido, WEP debe proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso.

El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red.

Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

DESVENTAJAS DE EL PROTOCOLO WEP:

- Todos los usuarios deben usar las mismas claves.
- Un atacante puede sin demasiada dificultad determinar por fuerza bruta el WEP y desencriptar.
- el tráfico o inyectar paquetes válidos en la red.
- NUNCA CONFIGURAR UNA WIFI SIN ENCRIPTACION WEP

3.5 Firewall

Es un sistema capaz de proteger una red interna, la cual tiene conexión a internet o hacia otras redes y así evitar ataques de Hackers que puedan dañar la red (Fig. 3.5.1), dicho sistema puede ser hardware o software o una combinación de ambos, pero sin duda la mejor manera de conservar una red libre de amenazas es a través del uso del firewall.

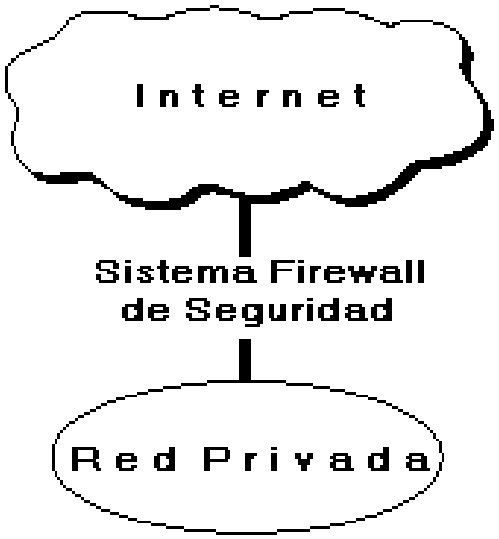


Fig. 3.5.1
Firewall (cortafuegos)

La función que tiene un firewall es la de comportarse como un filtro que controla todas las comunicaciones que pasan de una red a la otra, es decir la información que se permite o no entrar en la red. Para permitir o negar el acceso de la información, el firewall examina el tipo de servicio al que corresponde, como pueden ser:

- El web (WWW.)
- El correo electrónico (E-mail)
- Mensajera instantánea. (pop)
- ftp, etc.

Dependiendo del servicio el firewall decide si lo permite o no la entrada de estos servicios, ya que su objetivo es el de evitar la entrada de programas malintencionados que puedan dañar el equipo y la red, estas características de filtrado se pueden definir por el propio usuario. Pero un firewall tiene ciertas vulnerabilidades como por ejemplo:

- La copia de información, datos en cualquier medio de almacenamiento, ya sea diskette, CD, memoria UBS, etc. por personal de la misma empresa y que sea extraido de la misma empresa.
- Ataques de ingeniería social por Hackers hacia victimas que resultan ser elementos débiles, y así obtener claves para acceder al sistema.
- Ataques de virus al momento de descargar o descomprimir información de internet.

Hardware utilizado para la implementación de un firewall

Una de las opciones para proteger la red interna es el uso de dispositivos electrónicos, estos son los ruteadores (routers) (Fig. 3.5.2) que permiten el paso de los datagramas (paquetes) de acuerdo a sus reglas, las cuales analizan la información que se encuentra en el encabezado del paquete, la información consiste en los siguientes puntos:

- La dirección IP de origen o fuente
- La dirección IP destino
- Protocolo de encapsulamiento (TCP, UDP,ICMP, o IP tunnel).
- Puerto de origen TCP/UDP
- Puerto destino TCP/UDP

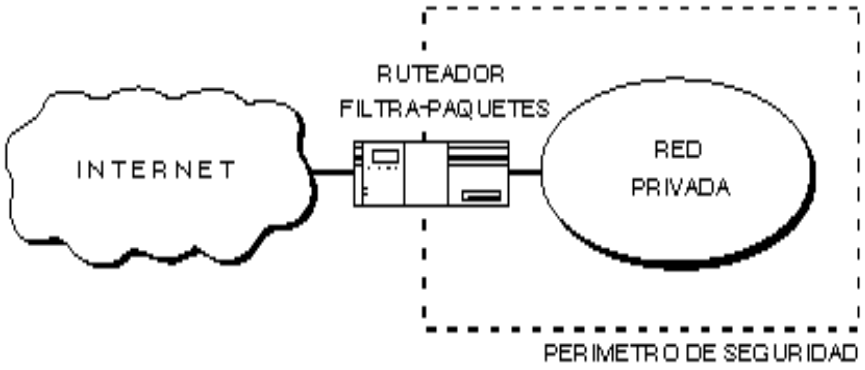


Fig. 3.5.2
Uso de ruteador como firewall

Ventajas del uso de un ruteador:

- la implementación puede ser barata.
- No necesita de software adicional para su manejo
- Es de fácil utilización, por lo que no se necesita de compleja capacitación.

CONCLUSIONES:

En la actualidad el uso de la computadora, es ya una necesidad, que permite agilizar las actividades a las que esta destinada, desde redactar una simple carta hasta controlar los procesos mas importantes de una empresa, y la mayor parte del tiempo esta computadoras se encuentran conectadas al WWW (internet), es entonces cuando se necesita contar con medidas de seguridad, para proteger toda nuestra información y estas medidas van desde diseñar una buena contraseña, contar con hardware y software que también suministren en su conjunto o por separado con herramientas de seguridad, es cuando podemos decir que nuestra información se encuentra segura, pero no hay que confiarse, ya que existen riegos diariamente de infección de nuevos virus los cuales son creados por hackers experimentados o por simplemente insertar disquetes prestados o permitirle a otras personas usar el equipo sin que estas tengan cuidado previamente de vacunar su disco, el robo de información no solo se da copiando los datos de la computadora, sino extrayendo físicamente el disco duro y hasta robo completo de equipos.

Así que en definitiva se diseñaran medidas de seguridad, pero también a la par se pueden crear de forma anónima, aquellas otras formas, trucos, software y hasta equipo que contrarrestan estas medidas, es por eso que se debe de tener cuidado en cuanto a la información a proteger, el de no visitar sitios web que se disfrazan de lugares conocidos por ejemplo como bancos, evitar leer correos electrónicos de personas desconocidas, o de aquellos contactos que llegan con información adjunta en otro idioma, ya que es la forma de contaminación de virus a equipos. Y por ultimo saber, si por alguna situación es necesario confiar la contraseña a alguien mas, se debe de proceder a cambiarla inmediatamente después de saber que ya ha sido usada, para evitar que la información que protegemos sea hurtada o borrada.