UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERÍA EN COMPUTACIÓN
CON ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CLAVE: 8793-16

SEGURIDAD EN REDES EMPRESARIALES TIPO LAN Y WAN

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA

MAYRA GISELA PATIÑO RESÉNDIZ

ASESOR: ING. CLAUDIA PATRICIA ROJANO HERNÁNDEZ

CELAYA, GTO. NOVIEMBRE 2002

AGRADECIMIENTOS:

A DIOS: Por darme la vida y por haberme permitido terminar mi carrera profesional. *Mil gracias señor.*

A MIS PADRES: Por haberme heredado el tesoro más valioso: El amor. Y porque gracias a ellos, a sus desvelos, me han formado, educado y me han visto convertirme en persona de bien. *Los quiero mucho.*

A MI HERMANO: Por apoyarme siempre en los momentos difíciles y por alentarme a seguir adelante.

A MI ABUELITA: Estela y Engracia, porque gracias a su cariño y apoyo logré salir adelante en la vida.

A MIS AMIGOS: Miguel, Alberto, Rodrigo, Fernando y Laura por brindarme su amistad y porque son los mejores amigos que he tenido.

INTRODUCCIÓN

A finales de la época de los años setenta comenzó a tener un gran auge el tema de las redes informáticas, las cuales han ido evolucionando día con día. En ocasiones, es difícil entender el funcionamiento de una red ya sea LAN o WAN, por lo que es importante conocer lo que este tipo de red hace, ya que en este tipo de redes existe el peligro de no mantener la información asegurada y respaldada en cualquier momento. Precisamente de esto último surge la inquietud de realizar un estudio que brinde los conocimientos sobre la seguridad y las amenazas que ésta puede traer, es decir, un estudio que trate sobre la seguridad en redes empresariales tipo LAN y WAN.

Por lo anterior, se puede establecer que *el objetivo de este estudio es determinar la importancia que han tenido las redes en el campo de la informática y la forma en que se puede proteger la información de la empresa.*

Este trabajo de investigación consta de cuatro capítulos. En el capítulo 1 se dan a conocer los antecedentes de la seguridad informática con el fin de comprender su definición y las amenazas que existen en cuanto a seguridad se trata, así como su campo de aplicación. Con el propósito de tener un marco teórico que sirva de base para determinar las medidas para asegurar la información de una red LAN, en el capítulo 2 se brinda el concepto de lo que es una red y sus tipos. En el capítulo 3 se dan a conocer las diferentes técnicas de seguridad que se pueden aplicar en una red LAN, con el objetivo determinar cuál técnica es mejor para proteger la información de la empresa o de cualquier ordenador. Por último, en el capítulo 4 se menciona la

relación que existe entre el firewall y la seguridad en redes LAN y WAN y se brindan los conocimientos para comprender el significado de virus informático, sus tipos y consecuencias, y esto, para saber que técnica de seguridad se puede aplicar para evitarlos.

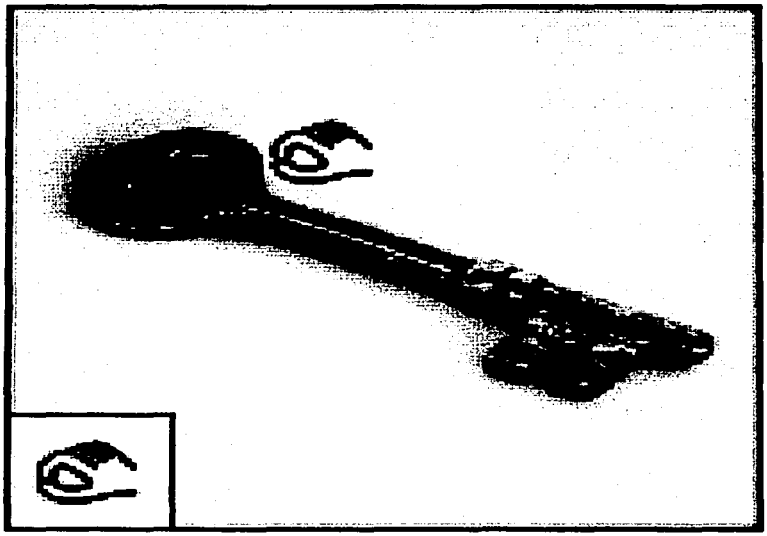
No hay duda alguna de que este estudio será de gran utilidad para todas las personas dedicadas al área de la computación.

INDICE

Capítulo 4

FIREWALLS Y SU RELACION CON LA SEGURIDAD EN REDES LAN Y WAN

CAPITULO 1



Seguridad en General

1.1 Antecedentes

Es importante tener en cuenta de lo importante que es para nosotros hoy en día el tener nuestra información asegurada, y claro, por qué no decir respaldada. Es por eso que desde que aparecieron las redes de computadora a mediados de los ochenta, la seguridad ha sido un tema que frecuentemente se discute con mucha frecuencia. Mientras más se habla de la seguridad en las redes, todo esto ha llevado a que muchas empresas y hasta en los hogares se limite el acceso al procesamiento de los datos y a cierto tipo de información que es de mucha importancia para nosotros.

Después de lo dicho anteriormente, es importante que se haga mención acerca del manejo de una red como una mayor responsabilidad y de saber qué relación tiene con la seguridad informática. Es necesario entender que uno de los principales objetivos de una red de área local es la conectividad, pues cabe decir que sin ésta no podría funcionar dicha red.

La conectividad es una forma de entender como están conectadas las computadoras en una pequeña o grande oficina, es decir, incluye lo que es el cableado, qué tipo de computadoras se debe tener y otras herramientas para poder echar a andar una red.

Además, la conectividad de una red incluye implantar un sistema altamente bien conectado para que éste no falle y no permita que nadie intente entrar al sistema; esto nos lleva a que la información esté mucho más segura y protegida de cualquier intento de robo por cualquier otra persona.

Podemos pensar que un sistema de seguridad es una serie de círculos concéntricos formando capas de protección alrededor de los datos almacenados en la computadora y de los recursos que se utilizan tales como impresoras, scanners,

etc. Es importante tener en cuenta que un sistema de seguridad en cualquier empresa es necesario, pues así tendríamos asegurada nuestra información y cualquier otro tipo de datos del que se quiera tener un respaldo.

Anteriormente se mencionó que la seguridad es un problema que a todos nos afecta, pero debemos entender que una red[1] también puede acarrear algunos problemas, como por ejemplo: el tamaño de una red es importante porque puede excluir problemas de seguridad o pueden aumentar.

Una pequeña red LAN (Red de Área Local) puede estar en una oficina y probablemente puede tener algunos problemas de seguridad como una red LAN un poco más grande. Estos problemas pueden ser que los datos no estén bien almacenados, ya sea en el disco duro o en disquetes, porque se puede correr el riesgo de que puedan ser borrados accidentalmente y esto es molesto.

En una red LAN un poco más grande, las técnicas de encriptación o de encapsulado de datos que más adelante se explicará, pueden ser necesarias para mantener la información protegida y bajo seguridad. Con una red LAN pequeña estas técnicas pueden ser posibles y fáciles de llevar a la práctica, ya que ayudan a mantener un mejor control de la información y a que no cualquier persona intente entrar al sistema que contiene dicha red. Este control de la información es un poco más difícil en una red LAN un poco más grande porque el tamaño de la red es más complejo, y se necesitará estudiar el funcionamiento de la red para poder implantar dichas técnicas.

Se puede decir también que un excesivo interés por la seguridad informática asegura una pequeña cantidad de paranoia por parte de los administradores de la red, es decir, de tanto pensar en asegurar la información de la red puede que con el tiempo se molesten de todo esto pero esperemos que esto no suceda, porque sin un

[1] HAYDEN, Matt, ***Aprendiendo redes en 24 horas,*** México, Editorial Pearson, 1999, p. 425.

administrador de la red simplemente la red no funciona. También podemos mencionar que otro problema de la seguridad en la red es el ataque repentino de los "hackers y crackers" (este tema se verá en el capítulo 4), que por lo regular siempre están esperando su oportunidad para atacar cualquier red y robar su información.

Hay que tener en cuenta que éstos pueden estar a un lado de nosotros y en cualquier parte y no nos damos cuenta de ello; es por eso que hay que tener cuidado con esto.

Por último, es importante saber que la seguridad en la información es un problema muy grande porque en una red no se puede tener una seguridad al 100%; sin embargo, se puede evitar haciendo un respaldo de toda la información que es de suma importancia para nosotros y que más adelante nos puede servir. La información se puede asegurar o respaldar para una mayor seguridad en disquetes, en el disco duro, en cintas magnéticas, o utilizando algunas técnicas que se enfatizarán en el capítulo 3.

1.2 ¿Qué es la seguridad informática?

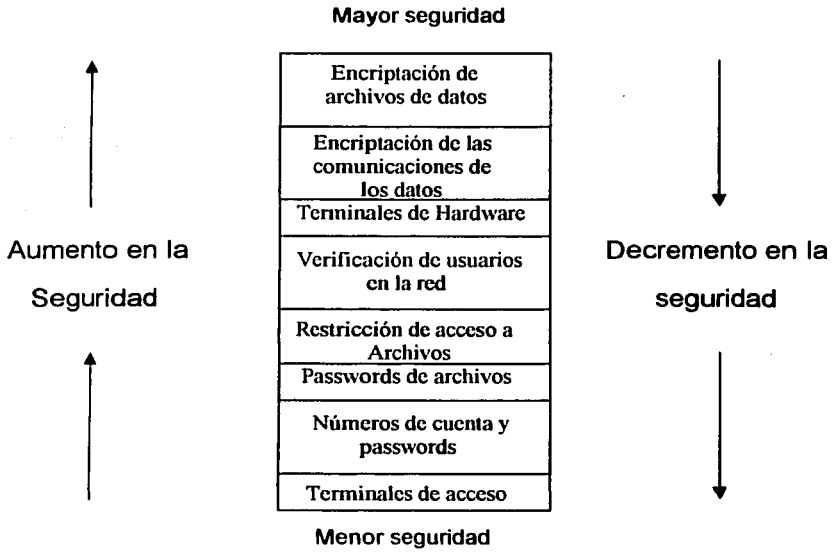
La seguridad informática, como se ha venido mencionando, es un problema muy grande que enfrentamos día con día y que en ocasiones es difícil enfrentarlo; es por eso que algunas veces no se tengan bajo protección los datos que se tienen en el ordenador o en alguna parte de éste, por lo cual se hace hincapié en lo que a seguridad informática se refiere y es por eso que se tratará de dar una definición o dar a conocer un concepto de lo que es la seguridad informática:

La seguridad informática es un proceso o una situación que se tiene de un problema del cual se requiere buscarle una solución respecto a lo que a información se refiere y que además se necesitan tomar medidas para proteger dicha información mediante técnicas que pueden ser: almacenamiento de los

datos en disquetes, utilizar la técnica de encriptamiento, utilizar claves de acceso al momento de comenzar a usar cualquier ordenador que puede estar en la oficina donde estés trabajando o simplemente el ordenador que usamos en casa, y otras técnicas que más adelante se describirán, todo esto con la finalidad de proteger nuestra información para que ninguna otra persona intente accesar por así decirlo a los datos que se tienen almacenados en nuestro ordenador o a cualquier ordenador de una red de área local o de cualquier otro tipo.

Se puede mencionar que también existen diferentes capas para clasificar a la seguridad informática de acuerdo al nivel de cómo se pueden asegurar los datos que se manejen, y por medio de un diagrama se representarán dichas capas:

Figura 1. Capas de la seguridad



Fuente: ***Data Network Design,*** U.S.A, Editorial Mc Graw Hill, 1993, p. 778

1.3 Tipos de seguridad

La seguridad de las computadoras en las comunicaciones se extiende más allá del uso de códigos de identificación de usuarios y passwords (contraseñas). Todo esto comprende un conjunto de reglas y de prácticas que aseguran que la información en cualquier parte de cualquier empresa y de nuestra sociedad está segura y no corre ningún riesgo de ser robada. Los tipos de seguridad que existen en las redes informáticas son cuatro: *la criptoseguridad, la transmisión de seguridad, la emisión de seguridad y la seguridad física.*

Primeramente, se hablará de lo que es la seguridad de la información y qué más incluye, y después se dará una breve descripción de lo que tratan los tipos de seguridad.

La *seguridad en la información* consiste en una combinación de la seguridad de los datos y de la seguridad en las comunicaciones, es decir, cada vez que tengamos que hacer un trabajo en cualquier computadora es necesario respaldar el documento que se está trabajando con la finalidad de que no se pierda la información que se tiene, y una mejor forma de almacenar y mantener segura la información es guardarla en un disquete, en una cinta magnética o en un CD-ROM para que no se pierda la información.

La *seguridad de los datos* es el conjunto de procedimientos y acciones diseñadas para prever un acceso no autorizado a la transferencia de datos, la modificación de los mismos o la destrucción de los mismos accidental o intencionalmente.

La *seguridad de las comunicaciones* (COMSEC, Communications Security) es el resultado de la protección de las aplicaciones o tipos de seguridad, como son: criptoseguridad, transmisión de seguridad y la emisión de seguridad, todas éstas

también son medidas para las telecomunicaciones y además son también medidas para la aplicación de la seguridad física y para la seguridad de la información.

Ahora se explicará en qué consisten los cuatro tipos de seguridad que se mencionaron anteriormente. Las definiciones respectivas fueron tomadas de un estudio que se realizó entre varias personas que estudian sobre la seguridad informática y que a su vez tiene relación con las telecomunicaciones.

1. **Criptoseguridad:** Es el componente de la seguridad en las comunicaciones que resulta de proveer criptosistemas técnicamente, que contienen sonido para mejorar la seguridad en la información.

2. **Transmisión de seguridad:** Es el componente de seguridad en las comunicaciones que resulta de todas las medidas, como son: seguridad de la información, seguridad de los datos y seguridad de las comunicaciones diseñadas para proteger las transmisiones de interceptación y de análisis que son realizadas principalmente por usuarios que intentan atacar los datos que se encuentran dentro del ordenador.

3. **Emisión de seguridad:** Es el componente de seguridad en las comunicaciones que resulta de todas las medidas tomadas para negar la información de valor a personas no autorizadas a la red y a la información que maneja dicha red.

4. **Seguridad física:** Es el componente principal de seguridad en las comunicaciones que resulta de todas las medidas físicas necesarias para salvaguardar el equipo de acuerdo a su clasificación, es decir, las características de la computadora como pueden ser: modelo, marca, color, etc., el material que se refiere al mobiliario con que cuenta la empresa y documentos de acceso u observación a personas no autorizadas a la red.

1.4 Amenazas a la seguridad

Diremos que se entiende por *amenaza* una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Un *ataque* no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

- *Interrupción.* Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

- *Intercepción.* Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras

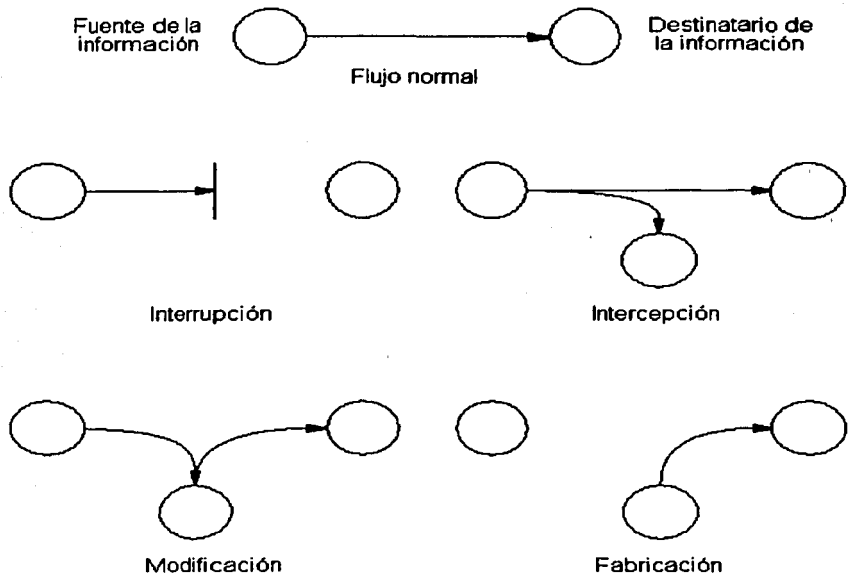
de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- *Modificación.* Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- *Fabricación.* Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Para entender un poco mas acerca de las amenazas a la seguridad informática, se muestra un diagrama que representa los diferentes tipos de amenazas.

Figura 2. Diagrama representativo de los diferentes tipos de amenazas a la seguridad



Fuente: http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

1.5 Campo de aplicación

Prácticamente, el campo de aplicación de la seguridad informática en cualquier red es muy importante porque cualquier empresa que utilice una red de información o hasta en el hogar, se tiene que asegurar toda la información; sin embargo, en ocasiones no es esto posible o no se quiere hacer, por lo que es necesario respaldar toda la información que es de suma importancia para la empresa y para uno mismo, pues no podemos pasar por alto que en cualquier negocio en el que se maneje mucha información se debe tener un respaldo de la misma, porque en ocasiones no falta qué persona intente tener un duplicado de la información que se maneja en el negocio o la empresa y éste la quiera vender a otra gente.

Es por eso que, en resumen, el campo de aplicación de la seguridad en la red básicamente se aplica en cualquier negocio que tenga o que maneje información en grandes cantidades y en cualquier empresa o negocio que cuente con una red de información.

CAPITULO 2

Seguridad en Redes de Área Local (LAN)

2.1 ¿Qué es una red?

Primeramente, se debe tener en cuenta que las redes de información están en todas partes. Es necesario saber que debido a que las redes controlan casi todo lo que existe y a que están constituidas por computadoras, es fácil hacer una suposición acerca de lo que la conectividad en redes puede hacer y que a lo mejor muchas de las personas no conocen aún lo complejo que es hablar de esto.

Antes de explicar lo que es una red, es preciso definir lo que es la conectividad en redes.

La ***conectividad en redes*** es una técnica especializada que permite saber cómo están conectadas las computadoras entre sí por medio de una red y saber de qué máquina se trata; es decir, cuando se instala una red es importante saber que cada una de las computadoras conectadas en red se identifica por medio de un nombre o por medio de una clave que nos permite identificar de qué computadora se trata.

Una ***red de computadoras o red física*** es un conjunto de computadoras que están conectadas por medio de cableado estructurado, tarjetas de red, de hubs o concentradores que permiten la comunicación entre las mismas, así como enviar y recibir información para que la red funcione.

Un punto importante que señala el Ing. Matt Hayden es que se debe tener en cuenta que una red puede ser lógica, es decir, una "*red lógica son colecciones de recursos tales como discos duros, impresoras y aplicaciones a las que su computadora no tendría acceso si no estuviera conectada a la red.*"[2] Las redes lógicas no son físicas porque éstas son el resultado de la organización de la red.

[2] En su libro ***Aprendiendo redes en 24 horas,*** México, Editorial Pearson, 1999, p. 425.

Debemos tener en cuenta que una red de computadoras es indispensable para una empresa o negocio que uno desee emprender, porque nos permite tener de una manera más organizada la información que se maneje dentro del negocio o cualquier otra empresa y además podemos consultar nuestra información cuantas veces sea necesario.

2.1.1 ¿Por qué es importante construir una red?

No está de más comentar que una red es indispensable para poder tener nuestra información al día y poder consultarla en cualquier momento que uno desee; pero también debemos saber que existen varias razones por las cuales es importante construir una red, y esas razones las vamos a reducir en los puntos que son más importantes, y son:

- Las redes tanto de datos como redes lógicas permiten incrementar la eficiencia en el manejo de la información.

- Las redes permiten disminuir la redundancia de la información haciendo que ésta sea más fácil de buscar y accesar en un momento dado en cualquier computadora.

- También ayudan de una manera muy rápida a organizar la información dentro de la misma, logrando así que dicha información se pueda modificar en cualquier momento y se pueda tener a salvo, ya sea en disquetes o en el disco duro o en cintas magnéticas, para no correr el riesgo de que se pierda la información.

- Es necesario que cuando se construya una red se tenga solamente el acceso restringido a personas que vayan a trabajar en la red, pues esto trae consigo que cualquier persona que intente entrar a la red pueda respaldar

alguna información y distribuirla en cualquier parte. Es por eso que es necesario asegurar toda nuestra información que se tenga en la red y en cualquier lugar de la computadora y si es posible hasta en los disquetes.

Es por eso que si se desea compartir información o alguna aplicación con cualquier usuario que se encuentre en la red y no se quiera ir de una computadora a otra llevando y trayendo discos flexibles o disquetes, lo mejor será que se tenga una pequeña red ya sea en la empresa donde se trabaja o en la propia casa, y se verán los beneficios que traerá el tener una red al alcance de la persona.

2.1.2 Dispositivos utilizados en una red de computadoras

Como ya se ha mencionado, una red es importante para tener nuestra información a nuestro alcance y el porqué es importante también tener una red. Es por esto, que si se va a construir una red, para que ésta funcione, es necesario saber qué dispositivos de red necesita. A continuación se señalan los dispositivos que más se utilizan para su funcionamiento.

Los primeros dispositivos que se requieren son: *computadoras e impresoras*, los cuales no requieren precisamente de una red para que trabajen. Enseguida se mencionan otros dispositivos de red básicos para que su red funcione:

- Una ***estación de trabajo*** que es la computadora que nos sirve para que cualquier usuario realice sus trabajos de todo tipo, ya sea trabajos escolares o trabajos de tesis y de cualquier otra categoría.

- Un ***servidor,*** que es aquella computadora que comparte sus recursos con otras computadoras. Los recursos que comparte son: disco duro y otros periféricos que estén a su alcance.

- Una ***impresora de red***, que es una impresora conectada a la red de tal forma que más de un usuario pueda imprimir en ella.

- Un ***hub o MAU*** o comúnmente llamado *concentrador*, que es un dispositivo que le proporciona a la red un punto de conexión para todos los dispositivos.

- Los ***ruteadores,*** que son dispositivos que administran el flujo de la información entre la red y permiten transferirla de computadora en computadora encontrando una ruta por la que puedan viajar los datos de una manera más rápida hasta llegar a donde debe ser.

- Los ***bridges o puentes,*** que son dispositivos que permiten unir o enlazar redes diferentes para formar una red lógica descrita anteriormente.

- Un ***repetidor*** es un dispositivo que permite que las redes se comuniquen entre sí amplificando y limpiando las señales digitales para poder enviarlas a su destino; esto se hace con la finalidad de que al momento de enviar información de una computadora a otra, la información no se pierda.

- Un ***módem*** es un periférico que permite que dos computadoras se comuniquen vía red telefónica conmutada. Uno de los dos ordenadores será de la red y el otro actuará como si lo fuera.

2.2 Tipos de redes

Como ya se ha venido comentando de lo importante que son las redes de computadoras en cualquier empresa o pequeño negocio, es propio mencionar que el hardware utilizado en las redes y las topologías que más adelante se verán, pero específicamente de una red de área local.

Se puede decir que las redes de computadoras existen de varios tipos, los cuales permitirán conocer algunas de sus características importantes y de saber cuáles tipos son, lo que permitirá comprender un poco más acerca de la conectividad de las redes.

Los tipos de redes que más se oyen hablar y de los que más se conoce son: LAN, MAN y WAN. Pero también existen otros dos tipos de redes adicionales, las CAN y TAN; éstas ultimas no son tan importantes, sin embargo hay que mencionarlas porque también son un tipo de red, y por último se mencionará también que existen tipos de redes más extendidas como son las ARCnet, Ethernet, Token Ring y las FDDI, de las cuales se dará una breve explicación de lo que son y otras características que las hacen distintas de las demás. El Ing. Matt Hayden[3] describe los tipos de redes como a continuación se menciona:

LANs. Una red de área local o *LAN* es la distinción organizacional menos compleja de las redes de computadoras. Una LAN no es más que un grupo de computadoras enlazadas o unidas a través de una red que se encuentran en un solo lugar o edificio.

MANs. Una red de área metropolitana o MAN es una red que utiliza líneas telefónicas de alta velocidad y que además utilizan un hardware especial como puede ser: unidades de transmisión por radio, microondas o láser, las cuales permiten una transferencia de datos a toda la velocidad de la LAN es decir, la velocidad de transferencia de datos de una red LAN que es de 10 a 20 megabits por segundo.

Además permiten que los recursos compartidos como pueden ser impresoras u otros dispositivos de red sean utilizados por usuarios localizados en varios sitios

[3] En su obra ***Aprendiendo redes en 24 horas,*** México, Editorial Pearson, 1999, pp. 425.

geográficos como si dichos usuarios fueran parte de la misma área local donde se efectúan dichas transferencias de datos en la red.

Sin embargo las MANs son en su totalidad redes locales; no tienen que utilizar necesariamente ruteadores (dispositivos responsables de la determinación de qué datos deben permanecer dentro de la red local y qué datos deben transferirse hacia otras redes).

WANs. Cuando una serie de LANs o MANs se encuentran muy dispersas geográficamente y no sea práctico enlazarlas a velocidades de LAN (generalmente separadas por un par de kilómetros), entonces es hora de construir una WAN (*Red de Área Amplia*). Las WANs son redes LANs o MANs dispersas geográficamente y conectadas entre sí a través de líneas telefónicas de alta velocidad. El acceso a los recursos de una red WAN a menudo se encuentra limitado por la velocidad de la línea telefónica que operan a velocidades de 56 Kilobits por segundo.

Las redes WANs a menudo se construyen cuando es importante que todos los usuarios tengan la capacidad de accesar a información común, como son bases de datos de productos o archivos bancarios de los cajeros automáticos. A diferencia de las redes LAN y MAN, las redes WAN casi siempre utilizan ruteadores.

Ancho de banda: Término que se utiliza para describir la velocidad máxima a la que un determinado dispositivo (como una tarjeta de red o un módem) puede transferir datos. El ancho de banda se mide en kilobits por segundo o megabits por segundo.

CANs. Una CAN es una *red de área de campus*. Típicamente, una CAN es similar a una MAN, ya que posee un ancho de banda de toda la velocidad de la red operando entre todas las LANs de la red. Algunas CANs están conformadas por toda una red distribuida a lo largo de un área local limitada, por ejemplo, un campus

universitario. Cuando esto sucede, se utilizan *puentes o repetidores* para enlazar las diferentes partes de la red, de tal forma que el usuario no sepa si el servidor que se está accesando se encuentra en alguna oficina o en el otro lado del campus.

Las CANs tienden a ser muy costosas, sin embargo son muy útiles en las organizaciones que utilizan mucho las computadoras, como las compañías de software y las universidades, ya que hacen que la red sea para los usuarios más sencilla y fácil de funcionar.

TANs. Son redes de área muy pequeña. Éstas son las dos o tres computadoras en red que la gente instala en sus casas o en cualquier otro lugar que no sea de negocios. A menudo se instalan TANs como una facilidad para los ejecutivos que desean tener en casa una réplica del ambiente de computación de su oficina o para que los niños puedan utilizar los recursos de computación en red.

Las TANs son excelentes si va a instalar su "primera red". Si dispone de los recursos, una TAN en el sótano o en un estudio ofrece invaluable experiencia de aprendizaje pues usted no tiene que compartir los recursos con ninguna otra persona.

Otro tipo de redes que se les conoce también como redes extendidas de acuerdo al tipo de cableado que utilizan, tipo de configuración e incluso al tipo de transmisión que se ajuste a las necesidades de cada usuario, se describen a continuación:

ETHERNET: Esta red fue desarrollada originalmente por Xerox y Dec como forma de solucionar el problema de cableado en redes. Los que inventaron esta red fueron Robert Metcalfe y David Boggs, que anteriormente trabajaban en la compañía Xerox en el Centro de Investigación de Palo Alto (PALRC, *Palo Alto Research Center*).

El nombre de Ethernet proviene de la palabra *Ether (éter),* la cual, como se sabe, denomina a un material inexistente que, según algunas teorías, llenaba el espacio y actuaba como soporte de la propagación de la energía a través del universo.

Se pensó utilizar cable coaxial pero hoy en día se utilizan otros tipos de cables como pueden ser la fibra óptica. El cable coaxial tiene una velocidad de transmisión de la información de 10 Mbps[4].

Token Ring: En 1985, IBM anunció su red local más sofisticada: la *Token Ring.* La Token Ring es una red en anillo con paso de testigo. Eso significa que los ordenadores conectados a la red se van pasando un testigo o una señal de unas a otras de forma secuencial y cíclica, de modo que sólo puede transmitir información aquel ordenador que tenga el testigo cada momento.

Como la velocidad de transmisión de información de estas redes puede ser hasta de 16 Mbps, el usuario no se da cuenta del tiempo que tiene que esperar su ordenador antes de recibir de nuevo el testigo para poder transmitir.

Los distintos ordenadores de la red se conectan a las unidades de acceso de multiestación, MAU (Unidad de Acceso a Multiestaciones), dentro de las cuales está formado el anillo. A cada MAU se puede conectar hasta 8 estaciones de trabajo, pudiendo tener como máximo 12 MAU, por lo tanto 96 estaciones.

La distancia máxima entre el ordenador y la MAU es de 50 metros (aunque se podría llegar hasta los 350 metros con cables de mayor calidad), y entre MAU es de 135 metros (pudiéndose llegar a los 215 metros).

---

[4] CARBALLAR, A. José ***El libro de las comunicaciones del PC. Técnicas, programación y aplicaciones,*** México, 1997, Editorial Computer Ra-Ma, p. 789.

El cable normalmente empleado en este tipo de red es el par trenzado telefónico, con o sin blindaje, aunque también se puede utilizar el cable coaxial o de fibra óptica.

ARCNET: Es una red en banda base que transmite a una velocidad de 2.5 Mbps, con una topología de estrella/bus. Este sistema fue desarrollado en 1978 por la empresa Datapoint, aunque fue potenciado en el mundo de los microordenadores por la empresa Standard Microsystems.

El acrónimo ARC proviene de la arquitectura de red de Datapoint, denominada *Attached Resource Computing*. Todos los ordenadores de la red se conectan en forma de estrella a un distribuidor central llamado HUB activo.

La distancia máxima entre el ordenador y el HUB activo debe ser de 660 metros. A los HUB activos también se pueden conectar HUB pasivos, conectándose un máximo de 3 ordenadores a cada HUB pasivo. La distancia máxima entre la estación de trabajo y el HUB pasivo es de 17 metros. Se puede conectar más de un HUB activo, distanciándose entre ellos un máximo de 660 metros. En total, el número máximo de estaciones no debe ser superior a 255.

FDDI: ANSI (Instituto Nacional de Estándares Americanos), ha desarrollado una especificación de redes de área local con fibra óptica.

En primer lugar, las computadoras funcionan a velocidades muy altas. Cuando las computadoras se conectan, la lentitud de los enlaces puede llegar a ser un cuello de botella. En consecuencia, las fibras ópticas de alta velocidad pueden ser el complemento adecuado a las computadoras de alta velocidad.

En segundo lugar, la tecnología de unidades de disco, en continua mejora, llegará a velocidades de lectura/escritura de 40 a 50 Mbps. Esta gran velocidad no

serviría de nada si el enlace de la unidad de disco con el computador fuera lento. Las fibras ópticas pueden ayudar a resolver ese problema.

En tercer lugar, las conversaciones de voz digitalizada requieren un ancho de banda mayor que el del canal telefónico convencional, especialmente si las conversaciones son interactivas y en tiempo real. Las fibras ópticas proporcionan un ancho de banda capaz de manejar conversaciones en tiempo real.

El canal de fibra óptica funciona a 100 Mbit/segundo. Un anillo de fibra óptica puede admitir hasta 1000 nodos. Los nodos pueden estar separados un máximo de 2 km y la máxima circunferencia del anillo puede ser de 200 km. La tasa total de transmisión es de 200 Mbps con cada canal transmitiendo a 100 Mbps.

2.3 ¿Qué es un protocolo?

Un protocolo es el conjunto de reglas previamente establecidas que definen los procedimientos para que dos o más procesos intercambien información. Además estas reglas definen la sintaxis, la semántica y la sincronización del protocolo.

2.3.1 Tipos de protocolos que existen en una red LAN

Existen varios tipos de protocolos en una red LAN, pero es importante mencionar que cada uno de ellos realiza una función diferente.

Los protocolos en una red de área local, como lo menciona el Ing. Andrew S. Tanenbaum[5], permiten detectar lo que las estaciones de trabajo están realizando y permiten adaptarse a todo tipo de cambio. Los tipos de protocolos que existen en una red de área local y que el autor muestra, se describirán por separado y son:

[5] En su obra ***Redes de computadoras***, 3ª. Ed, México, Editorial Prentice Hall, 1997, p. 813.

- CSMA 1-persistente y no persistente
- CSMA p-persistente
- CSMA con detección de colisión
- BRAP (Reconocimiento de difusión con prioridades alternas)
- MLMA (Protocolo multi-acceso de multinivel)
- Cuenta atrás binario
- Protocolo de contienda limitada
- Protocolo de recorrido adaptativo de un árbol
- Protocolo de la urna

A todos aquellos protocolos en los que las estaciones de trabajo escuchan a una portadora (transmisión o canal) se les llama ***protocolos de detección de portadora.***

- El primer protocolo de detección de portadora es el ***CSMA 1-persistente (Acceso múltiple por detección de portadora)***. Se le llama así, porque cuando una estación de trabajo necesita enviar alguna información a otra estación de trabajo, primeramente, la estación que envía la información debe de cerciorarse si alguna otra estación de trabajo no ocupa esa misma ruta por la que va a mandar la información, pero si la ruta se encuentra ocupada, la estación que envía la información debe de esperar hasta que se desocupe la ruta de envío.

Cuando la estación de trabajo detecta un canal o una ruta libre para mandar información o datos, comienza a mandar la información por ese canal. Pero si llegara a suceder una colisión o un retraso al momento de enviar la información a la estación de trabajo correspondiente, la estación en espera, tiene que esperar durante un intervalo de tiempo muy corto a que le llegue la información que solicitó, para después trabajar sobre ella.

A este protocolo se le llama *protocolo CSMA 1-persistente,* porque la estación de trabajo que transmite información, lo hace con una probabilidad de 1, es decir, transmite o envía información cada vez que encuentra un canal desocupado.

- El siguiente protocolo con detección de portadora es el ***CSMA no persistente***.

En este protocolo antes de transmitir o de enviar alguna información a otra estación de trabajo, la estación que va a enviar información, detecta el canal por el cual será enviada la información. Si la estación detecta que ninguna otra estación está enviando datos, ésta empieza a transmitir por su cuenta.

Pero si la estación encuentra el canal ocupado, lo ignora y espera un intervalo de tiempo para volver a mandar la información.

Este protocolo funciona similarmente que el protocolo CSMA 1-persistente, pero con la diferencia de que éste protocolo hace una mejor utilización del canal para transmitir datos, es decir, al momento de enviar los datos por el canal no se encuentra mucho trafico de información por el canal de envío.

- El tercer protocolo de transmisión de datos es el protocolo llamado ***CSMA p-persistente***.

Este protocolo, se aplica en estaciones de trabajo que se encuentren listas para transmitir datos o información inmediatamente, es decir, cuando la estación encuentra el canal desocupado por el cual enviará la información, si ésta encuentra el canal desocupado, transmitirá datos con una probabilidad *p (o sea n)* intentos para comenzar a transmitir.

Al terminar este proceso de transmitir o enviar información a otra estación de trabajo, es importante mencionar que este proceso de envío de datos o información, termina cuando otra estación de trabajo empieza a transmitir otros datos diferentes.

Pero cuando sucede de que otra estación comienza a transmitir, la estación de trabajo que primeramente comenzó a enviar los datos solicitados por otra estación, actúa como si hubiera existido una colisión (es decir, también esperará un determinado tiempo para comenzar de nuevo la transmisión de la información solicitada).

En general, los protocolos anteriormente descritos, aseguran que cualquier estación de trabajo comience a transmitir información cuando detecten que el canal de transmisión este ocupado.

También una de las mejoras de estos protocolos es que se pueden abortar o abandonar las transmisiones de información cuando se detectan colisiones. Dicho de otra manera, cuando dos estaciones de trabajo detectan un canal desocupado, y comienzan a transmitir datos de forma simultánea, ambas estaciones detectan una colisión.

Los protocolos, por lo tanto se encargan de detener el proceso de transmisión de datos en cuanto descubren que hay una colisión.

- El protocolo con detección de colisión, o también llamado ***CSMA/CD (Acceso múltiple por detección de portadora con detección de colisión)***, es utilizado en redes LAN y en subcapas MAC[6].

[6] Control de Acceso al Medio.

La capa MAC es muy importante en este tipo de redes porque casi todas las redes de este tipo utilizan un canal de acceso múltiple para transmitir datos y además utilizan esta subcapa como base para tener comunicación con el resto de las computadoras conectadas en red.

Sin embargo, cuando dos o más estaciones envíen datos a la misma vez, habrá una colisión.

Cuando esto sucede, cada estación de trabajo será capaz de abortar o abandonar el envío de datos o transmisión, y tendrá que esperar también un intervalo de tiempo en lo que termina la colisión, y tratará de repetir el proceso de envío de datos.

Este protocolo CSMA/CD, consiste en una serie de periodos alternados de contenida[7] y transmisión de datos, incluyendo periodos de inactividad por parte de cada estación de trabajo que ocurren cuando ninguna de las estaciones conectadas a la red permanecen en silencio, es decir, que no tengan trabajo que hacer.

Por otro lado, este protocolo trabaja con la detección de colisión que es un proceso en el cual la estación de trabajo por medio del hardware, deberá estar muy pendiente de los datos que se trasmitan en ese momento por el cable (medio físico), porque si la información que el cable esta leyendo al momento en que cualquier estación de trabajo los envía, si estos son diferentes a los que se están enviando, entonces el cable determina que ha ocurrido una colisión.

Cuando ocurre una colisión, el rendimiento del sistema se hace mas lento y puede no funcionar al encender la computadora.

[7] En estos periodos se guardan los datos temporalmente en lo que realiza la transmisión de datos de una estación a otra.

- Otro de los protocolos de una red LAN, es el ***protocolo sin colisión***. Este protocolo es llamado también *método básico del mapa de bits*. Es llamado así, porque cada periodo de contienda tiene *N* ranuras.

Si la estación de trabajo cero (0) tiene una trama para enviar, entonces ésta transmite un bit o sea un 1 en la primera ranura, por lo que a ninguna otra estación le está permitido transmitir o enviar una trama mientras se realiza el proceso de transmitir un bit a una ranura(espacio).

Pero, independientemente de lo que haga la estación cero, llegará un momento en el que la estación de trabajo 1 podrá realizar una transmisión de datos, es decir, un 1, y lo hará en la ranura 1 porque la ranura 0 está ocupada por la estación cero, pero solamente se realizará cuando se tenga una trama en espera.

Cuando terminen todas las estaciones de trabajo de realizar sus tareas de transmisión de datos o envío de información a través del cable (medio físico), se empezará otro nuevo proceso de transmisión de datos.

- El siguiente protocolo es el ***BRAP o RDPA (Reconocimiento de difusión con prioridades alternas).*** Este protocolo, permite a una estación de trabajo cualesquiera insertar un bit 1 o transmitir datos en una ranura (abertura o espacio) correspondiente. Esta transmisión la hace en la estación 1, la cual es la que comienza a transmitir datos en vez de la estación cero, que es la que va a recibir la información. Cualquier estación de trabajo que no trabaje en ese momento y que no reciba información, dejará libre la ranura a la que van a llegar los datos y permanecerá en estado inactivo.

En general, este protocolo es similar en la forma de comportarse que el protocolo CSMA 1-persistente, pero en este caso el BRAP, consiste en que a cada estación de trabajo, le otorga un permiso para hacer uso del canal que envía información a otra

estación de trabajo, permitiendo que la estación emisora, es decir, la que envía la información, atrase un poco de su tiempo al hacer uso del canal, para después la estación de trabajo receptora, ahora utilice el canal.

El problema de este protocolo, es el retraso o retardo de los datos que se envían de una estación de trabajo a otra, pues esto ocasiona que el trafico de información sea pesado y lento, lo que a su vez permite que el sistema con el que se esta trabajando se vuelva lento al momento de mandar alguna información por el cable.

- El protocolo ***MLMA (Protocolo multi-acceso de multinivel)***, se presenta solamente cuando cualquier estación de trabajo tiene un bit en cada nivel, es decir, contiene varios niveles en los cuales se realizan diferentes operaciones, como lectura o escritura. El número de niveles necesario en este protocolo para *N* estaciones de trabajo, está dado por la expresión $\log_2 N$, donde *N* es el número de estaciones de trabajo con las que cuenta la red.

- Otro protocolo que también menciona el autor es el protocolo **cuenta atrás binario.** Su función es la de dar una señal indicativa cuando una estación de trabajo esté lista para transmitir sus datos, pero para esto necesita que la estación de trabajo que solicitó el proceso de trasmisión de datos, escriba su dirección en código binario.

No obstante, para evitar cualquier problema, se deberá utilizar la regla de arbitraje la cual nos dice que *tan pronto como una estación de trabajo encuentre u observe que otra estación de trabajo ha puesto un cero al momento de transmitir alguna información, pero que inmediatamente haya puesto un 1, la estación que esta esperando colocar un 1, para que ésta también transmita información, se dará por vencida.*

Pero después de que la estación que estaba esperando colocar un 1 en el canal, lo logra, no hay información disponible que indique cuantas estaciones de trabajo estaban esperando transmitir información.

- El siguiente protocolo, es el llamado ***protocolo de contienda limitada.*** Este protocolo combina propiedades de los protocolos de contienda y de libre colisión. Permite además, tener retardos de tiempo al momento de transmitir información lo que proporciona un mejor rendimiento en el canal por donde van a pasar los datos o información.

Los *protocolos de contienda limitada*, permiten a cada estación intentar adquirir un canal de transmisión pero con una probabilidad de *p,* porque no se sabe si ese canal vaya estar ocupado por otra estación de trabajo.

- El siguiente protocolo, es el ***protocolo de recorrido adaptativo de un árbol.*** Contiene varios niveles de información. Su funcionamiento, consiste en que una ranura (espacio) de contienda, permita hacer una transmisión o envío de información con éxito, en el que también todas las estaciones de trabajo están autorizadas para enviar datos por el canal. Pero, si hay una colisión, la ranura 1, competirá por aquellas estaciones de trabajo que se encuentren en el nodo 2. Si cualquiera de las estaciones logra tomar posesión del canal, la ranura que viene a ser ocupada por datos o información, se reservará para aquellas estaciones que se encuentren en el nodo 3 y así sucesivamente.

Si por otro lado, dos o más estaciones de trabajo, que se encuentren en el nodo 2 desean transmitir al mismo tiempo, ocurrirá una colisión.

- El último protocolo que se describirá es el ***protocolo de la urna.*** Este protocolo es parecido al protocolo anterior, pero con la diferencia de que utiliza una urna (caja) en lugar de un árbol.

Su funcionamiento, al igual que el protocolo de recorrido adaptativo de un árbol, limita el número de estaciones de trabajo que son autorizadas para transmitir información durante cada cierto tiempo en el que una ranura se encuentra desocupada para poder ser llenada por así llamarlo, de información, de tal manera que permita maximizar una probabilidad de tener una estación de trabajo preparada para recibir información por medio de una ranura de contienda.

2.4 ¿Qué es una LAN?

Básicamente, existen muchas definiciones acerca de lo que es una red de tipo LAN, pero se dará un concepto claro para todos aquellos usuarios que se interesan por saber sobre redes.

De acuerdo a lo que dice Merilee Ford y otros autores, una red LAN es: "*Una red de datos de alta velocidad es decir, que los datos que son enviados de una computadora a otra son rápidos al momento de recibirlos en cualquier ordenador, es tolerante a fallas, que cubren un área geográfica relativamente pequeña. Esta red por lo general conecta estaciones de trabajo, computadoras personales, impresoras y otros dispositivos. También este tipo de red tiene muchas ventajas para los usuarios que utilizan las PC's de las cuales son el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos o información entre los usuarios conectados a la red y también permite la comunicación entre los usuarios vía correo electrónico.*"[8]

Otra de las facilidades que brinda una red de área local o LAN, es que permite compartir bases de datos, programas de aplicación, impresoras, y además el uso de correo electrónico, así como también permitirá interconectar ordenadores que estén dentro de un mismo edificio o en edificios contiguos, pero siempre teniendo en

[8] En su obra ***Tecnologías de interconectividad de redes***, México, Editorial Pearson, 1998, p. 716.

cuenta que el cable con el que van a estar unidas no puede rebasar unos cuantos miles de metros.

Algunas características de las redes LAN son las siguientes:

- Ocupan sólo un lugar físico, es por eso que se les dice que son de área local.

- Pueden ser redes punto a punto, lo que significa que no existe una computadora central a la cual podamos estar conectados, o pueden ser redes cliente/servidor, lo cual significa que una computadora central, llamada servidor, tenga la mayor parte de los recursos de la red y es accesada por los usuarios.

- Tiene altas velocidades de transferencia de datos.

- Los datos que se manejan en esta red son parte de ella misma.

- Su velocidad de transferencia de datos es de 10 a 20 Mbps (Megabits por segundo), lo que las hace más rápidas que las redes de cobertura amplia.

- Tienen un campo de acción o cobertura cuyo tamaño no es mayor de unos cuantos kilómetros.

- Pertenecen a una sola organización, es decir, a un solo edificio.

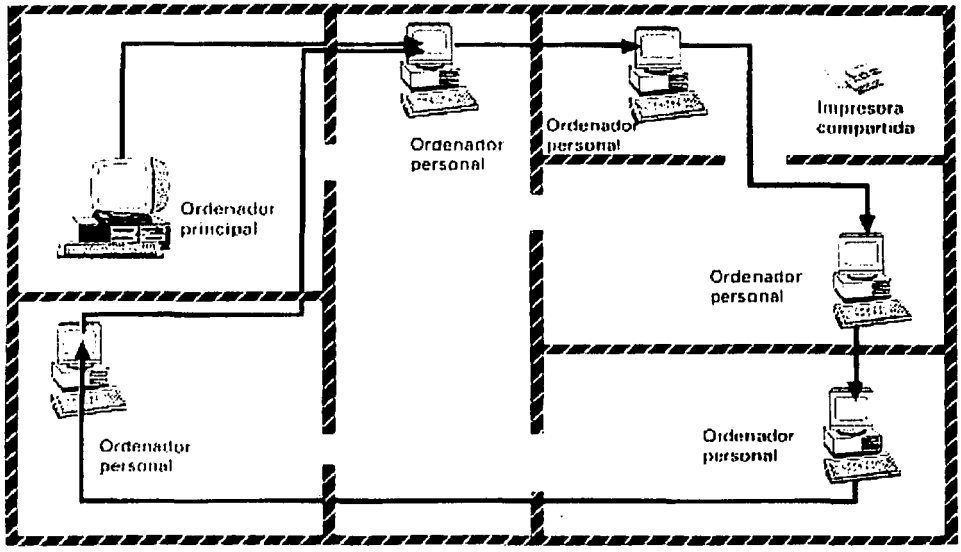
- Las LAN transmiten datos entre estaciones de usuario y computadoras, aunque también algunas redes LAN pueden transportar imágenes de video.

- La distancia entre las conexiones de las estaciones de trabajo se mantiene en el rango de los cientos de metros.

- Los canales para la transmisión de datos en una red de área local son propiedad de la organización que las utiliza.

A continuación se muestra una figura de cómo está constituida una red de área local (LAN):

Figura 3. Conexión de una red de área local



Fuente: MILERA MARTINEZ, María Esther, ***"Computación"*** Enciclopedia Autodidacta Siglo XXI, México, Editorial Euromexico, 1997, 240 p.

2.4.1 Topología de una red LAN

Las topologías definen una mejor forma de organización de los dispositivos de la red. Es por eso que se mencionarán las diferentes topologías que constituyen una red LAN y que son muy comunes hoy en día. Las redes de tipo LAN contienen cuatro topologías, las cuales son: bus, anillo, estrella y árbol; puede ser que se deriven otras topologías, pero solamente se tratarán las más importantes de este tipo de red.

Primeramente, se definirá lo que es la topología de la red, para después pasar a describir los diferentes tipos de topología que existen en una red de área local. Una definición que ayuda a entender acerca de lo que es una topología de red es la siguiente:

> *Una topología de red son las distintas formas o conexiones que nos permiten saber como están conectadas las computadoras entre sí formando por así llamarlo figuras.*

Sin embargo, las topologías son arquitecturas lógicas que nos permiten saber y distinguir cómo están conectadas las redes. A continuación se describe por separado cada topología con sus respectivas características.

Topología en Bus: Esta topología es de una arquitectura lineal en la que los envíos de información a cualquiera de las computadoras conectadas a este tipo de red se esparcen a lo largo del medio de transmisión que es el cable y esa información llega y es recibida por todas las computadoras o estaciones conectadas a la red.

En este tipo de red los ordenadores están conectados a un solo canal de comunicación, donde toda la información circula por ese canal y donde además de

enviarla cada ordenador se queda solamente con la información que va dirigida hacía él.

Además, el número de ordenadores conectados a este tipo de red no debe ser muy grande ni tampoco la distancia que separa a dos ordenadores contiguos, porque los ordenadores cercanos al ordenador principal donde éste envía mensajes, los ordenadores al momento de recibir dicho mensaje, lo reciben con una señal muy fuerte que los ordenadores que están más alejados del ordenador principal, y es por eso que puede fallar en algún momento la red.

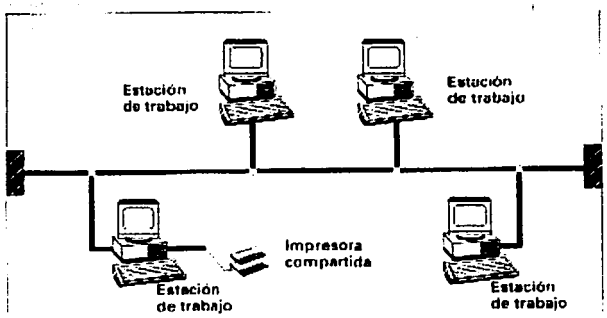
En la red de bus se pueden utilizar repetidores que son instalados a lo largo del canal de comunicación, los cuales permiten que cuando se envíen datos o mensajes a otro ordenador y como el envío de datos se hace a base de señales eléctricas, es mucho más fácil que los datos lleguen a su destino sin ninguna interrupción y al momento de recibir el mensaje por medio del canal de comunicación, éste amplifique la señal y permita que los datos no se pierdan.

Desventajas:

- Este tipo de red tiene muchos puntos de falla, es decir, que si uno de los enlaces donde están conectados los ordenadores entre sí de este tipo de red falla o se rompe, la red deja de funcionar.

A continuación se muestra una figura de cómo está constituida una red con topología de bus:

Figura 4. Red con topología de bus



Fuente: Idem

Topología en árbol: Esta topología es una arquitectura de LAN similar a la topología en bus, excepto que en esta topología las ramas o brazos que contiene ésta pueden tener múltiples nodos.

La topología en árbol suele utilizarse cuando los ordenadores que forman una red se encuentran situados en pisos diferentes de un mismo edificio. Para esto, en cada piso se emplea una red de bus para conectar los ordenadores de ese piso, y a su vez, las redes en bus de los demás pisos se unen a un cable de conexión común para todo el edificio.

La instalación de este tipo de topología es fácil, así como la ampliación del número de ordenadores conectados a esta red.

En esta topología, a cualquier estación de trabajo no le afectan las averías ni al resto de los ordenadores conectados.

Algunas desventajas de este tipo de red son:

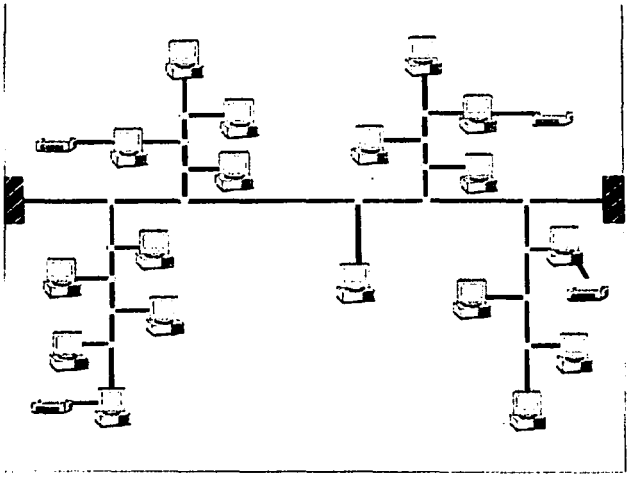
- Se afectan las averías en el cable de conexión principal y en los cables principales de las ramas del árbol o de la red.

- La topología en árbol no es adecuada para conectar ordenadores de diferente fabricante.

Para esta topología generalmente se utiliza el cable coaxial de banda ancha para permitir una mejor transferencia de datos.

A continuación se muestra una figura que indica como está conectada una red con topología de árbol:

Figura 5. Red con topología de árbol



Fuente: Idem

Topología en anillo: En este tipo de topología se dice que es de anillo porque los ordenadores conectados a esta red están conectados en forma de círculo. En una red con topología de anillo, cada ordenador tiene conectados una unidad de acceso y un repetidor porque la información pasa de un ordenador a otro. Si éste es el destinatario, la información la recibe por medio de su unidad de acceso, y si no es así, la información la pasa al siguiente ordenador utilizando su repetidor. Esto es lo que la hace diferente a la topología de bus.

Para mejorar la velocidad de transmisión, las redes con topología de anillo disponen de dos canales que permiten enviar la información más rápida eligiendo cual de los dos caminos es más seguro. Además, comparada con otros tipos de topologías de red, la topología de anillo requiere un hardware más costoso y más complejo.

Desventajas:

- Una avería o fallo en cualquier estación de trabajo paraliza el funcionamiento de toda la red, ya que el flujo de información queda interrumpido al llegar a la estación de trabajo que falló.

- La instalación de esta red es bastante complicada.

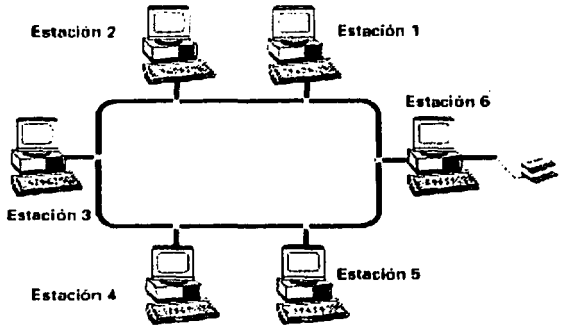
Pero también es importante mencionar que una topología en anillo ofrece algunas ventajas.

- En primer lugar, cuando el tráfico de datos o información es muy alto, el tiempo de espera de una estación de trabajo u ordenador para poder accesar a la información es menor que en otros tipos de redes.

- En segundo lugar, la capacidad de transmisión de datos y de recibirlos se reparte de una forma equitativa o igual entre todos los usuarios que ocupan cualquier estación de trabajo sin que se perjudique a ninguno.

A continuación se muestra una figura de cómo está constituida una red con topología de anillo:

Figura 6. Red con topología de anillo



Fuente: Ibidem

Topología en estrella: En una red con topología de estrella, es una red en la cual los ordenadores o estaciones de trabajo están conectadas a un ordenador central por medio de un Hub o concentrador; pero las estaciones no están conectadas entre sí.

Para enviar información desde una estación de trabajo a otra, la estación emisora pasa la información al ordenador central y éste, posteriormente, la retransmite a la estación receptora.

El ordenador principal o central es la estación de trabajo donde se tiene toda la información de la red; si ésta falla, toda la red queda inutilizada. Por el contrario, si una estación de trabajo falla, el resto de las estaciones puede seguir funcionando como si nada hubiera pasado.

Desventajas:

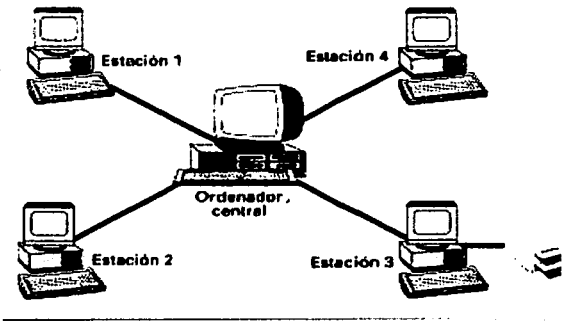
- La instalación de una red con topología de estrella es bastante complicada y su precio resulta elevado en comparación con las redes con topología de bus y anillo, debido a la complejidad de la tecnología que se utiliza en este tipo de red con esta topología.

- El precio de cableado es bastante caro.

- La velocidad de transmisión depende en gran manera de la capacidad y potencia del ordenador central.

A continuación se muestra en la siguiente figura como está constituida una red con topología de estrella:

Figura 7. Red con topología de estrella



Fuente: Ibidem

2.4.2 Funcionamiento de una red LAN

El funcionamiento de una red de área local (LAN), se basa en lo que a cableado se refiere, es decir, primeramente se debe tener en cuenta que una red de área local no es tan sencilla como parece porque se necesita estudiar a fondo qué es lo que se necesita para poder construir una red de este tipo.

Por principio de cuentas, es necesario saber que una red local va a permitir compartir bases de datos, programas, impresoras o módems, poniendo a disposición otros medios, como el correo electrónico.

Además, permite interconectar ordenadores que estén dentro de un mismo edificio o en edificios colindantes, pero teniendo en cuenta que un cable de varios miles de metros los va a unir.

Entonces, ¿cómo se puede explicar el funcionamiento de una red LAN? Primeramente, se debe tener en cuenta que para que una red LAN funcione, ésta necesita que tenga equipo para poder construirla; con equipo se entiende el tipo de

computadoras que se van a usar, el cableado que se va a utilizar para que los datos que se van a tener estén seguros y con esto poder utilizarlos en el momento que se requiera; se necesitan también los recursos que se van a ocupar, como son: impresoras, scanners u otro dispositivo, para que la red sea más completa.

Además, se necesitan concentradores o hubs para poder establecer qué computadoras estarán conectadas a la red, y otras cosas más; pero, en sí, se puede decir que para que una red LAN funcione es necesario unir todos estos componentes, para poder tener una red fiable, eficiente y sin tantos problemas.

2.4.3 Medios de transmisión de una red LAN

Otro punto importante que se menciona son los diferentes medios de transmisión de datos de las redes de área local; esto es, el tipo de cable que utiliza para una mejor transferencia de datos, el cual es el cable coaxial, que puede ser de dos tipos: *cable coaxial de banda base y de banda ancha.*

- El *cable coaxial de banda base* se empleó en antenas de televisión y en ciertos tipos de comunicaciones telefónicas. En el cable coaxial de banda base, alrededor del hilo que conduce la información, se coloca un aislante. Rodeando ambos, es decir, el aislante y el hilo, se dispone de una malla formada por finos hilos de cobre, y por último contiene un blindaje exterior que aísla el cable de las posibles interferencias que pueden distorsionar el tráfico de la información.

El cable coaxial de banda base tiene un diámetro aproximado de 1 milímetro y su capacidad de transmisión es de unos 10 Megabits por segundo; además, este cable puede ponerse en la pared, en el techo o bajo el suelo de cualquier oficina.

Este cable es mucho más sólido, ligero y resiste mejor las interferencias producidas por máquinas, aparatos de radio y demás dispositivos electromagnéticos que el cable de tipo par trenzado.

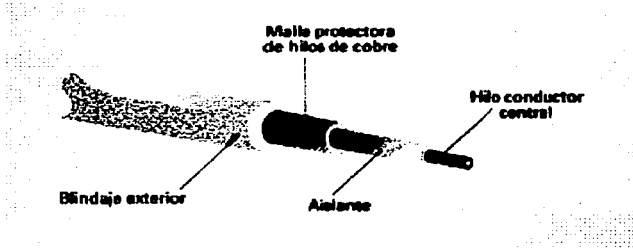
Es importante mencionar que este tipo de cable es el que predomina. Sin embargo, algunas redes que utilizan este tipo de cable han sido reemplazadas por PBX[9].

Desventajas:

- Uno de los principales inconvenientes de este tipo de cable es que puede actuar como una especie de antena que emite señales constantemente y que a su vez pueden ser interceptadas por una computadora no conectada a la red.

Enseguida se muestra una figura que nos ayuda a identificar cómo es este tipo de cable:

Figura 8. Cable coaxial de banda base



Fuente: Ibidem

[9] PBX: Centralitas de conmutación privadas.

- El *cable coaxial de banda ancha* es conveniente utilizarlo en redes no muy extensas pero con un número considerable de estaciones de trabajo. Este cable se construye de una forma similar al de banda base. Primero se coloca un cable conductor y una malla de hilos de cobre o aluminio separados por un material aislante, y el conjunto, a su vez, se rodea de una capa protectora.

Por este cable se pueden transportar las señales de hasta 100 canales de TV y por ello es el cable utilizado en los sistemas CATV o de televisión por cable.

Para transmitir datos por el cable coaxial de banda ancha es necesario utilizar dispositivos, como pueden ser: módems, repetidores, alimentadores de corriente, acopladores de dirección y terminadores.

Además este tipo de cable se suele utilizar en topologías de árbol y estrella. Su costo es mayor al del cable de par trenzado por lo que no se aconseja utilizarlo en redes pequeñas.

En este tipo de cable, cuando se tienen más de 100 estaciones de trabajo conectadas a una red LAN, es mas conveniente utilizar este tipo de cable.

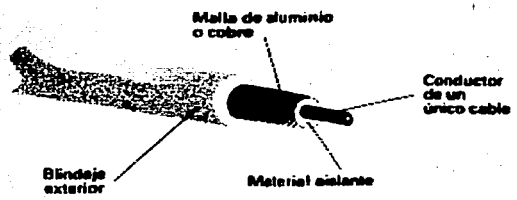
Desventajas:

- Al utilizar este tipo de cable, los dispositivos como pueden ser impresoras u otro dispositivo, pueden fallar.

- Es muy sensible a los cambios de temperatura.

Enseguida se muestra una figura que nos permite conocer como está constituido este tipo de cable:

Figura 9. Cable coaxial de banda ancha



Fuente: Ibidem

Es importante mencionar que cualquier tipo de red también utiliza otros dos tipos de cableado que son: el de par trenzado y fibra óptica.

- El cable de par trenzado es el que comúnmente se utiliza en las instalaciones telefónicas. Está compuesto por un par de hilos de cobre trenzados entre sí. El cable de par trenzado ha sido hasta el momento el más utilizado en redes de área local y se puede usar en topologías de bus, anillo o estrella. Su principal ventaja es su precio porque al ser muy utilizado en las redes telefónicas, se fabrica en grandes cantidades por lo cual tiene un costo muy bajo. Pero así como los demás tipos de cables, éste presenta también algunos inconvenientes.

Desventajas:

- En primer lugar, sólo se puede emplear en redes que tienen pocas estaciones de trabajo colocadas en el mismo edificio.

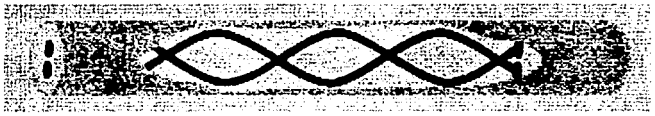
- En segundo lugar, es un cable delicado que puede resultar dañado si se dobla demasiado o si se instala en superficies ásperas.

- En tercer lugar, este tipo de cable no suele estar blindado, y si lo está el blindaje acostumbra a ser reducido por lo que la falta de protección lo hace vulnerable a las interferencias eléctricas, es por esta razón que este cable no se debe instalar junto a aparatos de radio, transformadores, motores eléctricos, maquinaria industrial y todo tipo de dispositivos que produzcan fuertes campos eléctricos.

- Y por último, en este tipo de cable se debe cerciorar que los datos transmitidos a través de él pueden ser interceptados por otros ordenadores que no estén específicamente conectados a la red.

A continuación se muestra una figura en la cual podemos identificar que partes constituyen a este tipo de cable:

Figura 10. Cable de par trenzado



Fuente: Ibidem

➢ El cable de fibra óptica es un tipo de cable que se está empezando a utilizar en las redes locales de ordenadores. Este tipo de cable transmite señales luminosas, y por tanto es radicalmente distinto a los otros tres tipos que anteriormente se explicaron.

Para utilizar el cable de fibra óptica, lo primero que se necesita es un dispositivo transmisor formado por una fuente de alimentación y un foco de luz. Este foco o emisor de luz puede ser un láser o un LED (Diodo Emisor de Luz).

El cable de fibra óptica no es más que un conjunto de fibras de vidrio rodeadas de un material de revestimiento que aísla las fibras entre sí impidiendo que se produzcan interferencias. El conjunto de las fibras y el revestimiento rodea un cable central de acero, y es rodeado a su vez por otro revestimiento de acero que da firmeza al cable, y por último se coloca una capa de protección de polietileno de baja densidad.

El cable de fibra óptica es capaz de transmitir datos a velocidades mucho más altas –mil millones de bits por segundo- y a distancias mucho mayores que las que permiten los otros tipos de cable.

Además, este tipo de cable es muy ligero, flexible y resistente a las interferencias electromagnéticas porque tiene un periodo de vida muy largo y ha demostrado que tiene un mejor y mayor rendimiento y no se pincha tan fácilmente.

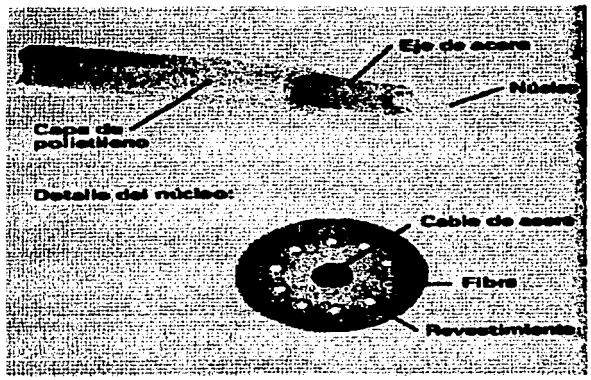
Este tipo de cable presenta también algunas desventajas, que son:

- Su precio es muy elevado para redes pequeñas, aunque en los últimos años se dice que ha habido una disminución en lo que a costo se refiere.

- La dificultad de las conexiones es complicada porque se necesita de un equipo de gran precisión ya que si los cables no están bien alineados, las señales luminosas que transportan se pierden. Si por el contrario, las fibras no están perfectamente alineadas o bien conectadas, la velocidad de transmisión será menor y las posibilidades de que se dispersen las señales luminosas serán mayores.

A continuación se muestra una figura que nos permite conocer cómo es el cable de fibra óptica:

Figura 11. Cable de fibra óptica



Fuente: Ibidem

Enseguida se muestra una tabla que muestra las diferencias de los diferentes medios de transmisión que existen en las redes de área local:

Figura 12. Tabla de diferencias de los medios de trasmisión

	De par trenzado	Coaxial de banda base	Coaxial de banda ancha
Fiabilidad	Escasa	Buena	Buena
Posibilidad de interferencias	Alta	Moderada	Escasa
Distancia	Pequeña	Moderada	Larga
Seguridad	Poca	Poca	Poca
Precio	Bajo	Bajo	Moderado
Instalación	Fácil	Difícil	Muy difícil

Fuente: Ibidem

2.4.4 Tipos de LAN

Los tipos de LAN más comunes que existen son de dos tipos: *LAN por cable y LAN inalámbrica.* Podemos decir que solamente daremos una breve descripción acerca de estos dos tipos de LAN es decir, de que se trata y cuales características contienen.

Las LAN de tipo cable, como su nombre lo indica, utilizan el cableado fijo como puede ser: cable de par trenzado, cable coaxial de banda base, cable coaxial de banda ancha y fibra óptica. Estos se pueden usar como medios de transmisión anteriormente mencionados.

Las LAN de tipo inalámbrico utilizan ondas de radio o de luz. Pero antes que nada daremos una breve definición de lo que es una red de tipo inalámbrico, se le llama así porque los medios de unión entre sus terminales no son cables, sino un medio inalámbrico, es decir, sin cableado, como puede ser la radio, los infrarrojos, las microondas o el láser.

El *Infrarrojo* son ondas electromagnéticas que se propagan o se expanden en línea recta, siendo susceptibles a ser interrumpidas por cuerpos opacos u obscuros. Su uso no necesita licencias administrativas y no se ve afectado por interferencias radioeléctricas externas, pudiendo alcanzar distancias de hasta 200 metros.

El *radio UHF* necesita para su instalación una licencia administrativa y tiene la ventaja de no verse interrumpido por cuerpos opacos u obscuros. Se utiliza ampliamente en muchas aplicaciones; entre ellas, la difusión de radio y televisión y las redes de telefonía celular.

Las *microondas* son ondas electromagnéticas cuyas frecuencias se encuentran dentro del espectro de las super altas frecuencias, SHF, utilizándose para las redes

inalámbricas la banda de los 18-19 Ghz. Estas redes tienen una propagación muy localizada y un ancho de banda que permite alcanzar los 15 Megabits por segundo.

El *láser* en estos tiempos debe y tiene todavía que resolver problemas en el terreno de las redes inalámbricas antes de que se consolide su gran potencial de aplicación.

2.5 Campo de cobertura de una red LAN

El campo de cobertura de una red LAN básicamente se describe en varios puntos que son importantes para dar a conocer que tan grande se extiende. Los puntos a considerar son:

- Un campo de cobertura que puede ser variante, es que la distancia entre las conexiones de las estaciones de trabajo se mantiene en el rango de los cientos de metros.

- Otro punto es que la red de computadoras debe estar situada a una distancia máxima de por lo menos unos 1000 metros.

- El campo de acción de una red LAN no es mayor a unos cuantos kilómetros.

- Tienen una velocidad total de datos, de cuando menos varios Mbps.

- El cableado utilizado en las redes LAN es mas fiable, es decir, en la transmisión de datos, la tasa de error es 1000 veces inferior que la de una red WAN.
- Todos los datos que contienen las redes de área local son parte de la misma.

CAPITULO 3

Técnicas de seguridad en redes LAN

3.1 ¿Qué es una técnica?

Una *técnica* consiste en una serie de pasos a seguir con la finalidad de resolver un problema y poder determinar su resultado.

3.2 Tipos de técnicas utilizadas en redes LAN

Las técnicas utilizadas en redes de área local son muy importantes porque de éstas se deduce el cómo se pueden asegurar los datos o la información que se necesita proteger en la empresa. Es importante tener en cuenta que así como se puede asegurar la información mediante software, no debemos olvidar que también se puede tener seguridad por medio de hardware, y esto es, en consecuencia, importante tanto para el usuario como para el personal que trabaja en la empresa.

Las técnicas a utilizar son:

3.2.1 Cifrado

Existen técnicas de software y hardware que están diseñadas para proteger la información y evitar que usuarios no deseados puedan accesar o entrar a una computadora personal; pero a pesar de esto, no se puede tener al 100% seguridad de que la información más importante no pueda caer en manos de intrusos. La desventaja de estas técnicas de aseguramiento de la información o también llamadas protección de acceso a la computadora, es que si cualquier persona o usuario logra descifrar alguna clave de acceso, la cual protege la información, la computadora queda libre para que esta persona la utilice a su disposición o a su manera.

Es importante mencionar que la información que se maneja en la empresa que no es demasiado importante, con sólo protegerla con una clave de acceso, es suficiente. Sin embargo, algunas veces esa información necesita de un mayor nivel de seguridad y esto se consigue con la técnica de criptografía o cifrado de los archivos o de la información. Con el método de la criptografía o cifrado, lo que se protege es la información.

Las técnicas de criptografía y cifrado no sólo se utilizan para proteger la información de cualquier computadora de los intrusos que intentan atacarla, sino que pueden utilizarse cuando se va a enviar algún documento por un medio de comunicación, como puede ser un fax o por correo electrónico.

En el caso de las comunicaciones en línea, la técnica de cifrado o el proceso de cifrado debe producirse antes de transmitir información, aunque existe software de comunicaciones que permite realizar este proceso en forma más rápida.

En el caso de las redes de área local, existen varias posibilidades:

- Modificar las aplicaciones que hagan uso de la red, de manera que toda la información transmitida haya sido previamente cifrada.

- Instalar dispositivos software que protejan la información automáticamente (a nivel de red) antes de su transmisión y realicen el proceso inverso de la recepción.

- Emplear elementos hardware que se encarguen de realizar el proceso de la protección de las comunicaciones de forma totalmente transparente.

Las técnicas de cifrado convierten a los ficheros en una secuencia de caracteres de forma que no se puedan leer correctamente a menos que se disponga de la clave correcta para su descifrado. La técnica de cifrado es una forma en la cual podemos proteger la información de la empresa mediante algoritmos.

Se pueden dividir en dos categorías: *cifradores de bloque*, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y *cifradores en flujo*, que trabajan sobre flujos continuos de bits.

En resumen, la técnica o mecanismo de *cifrado* consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.

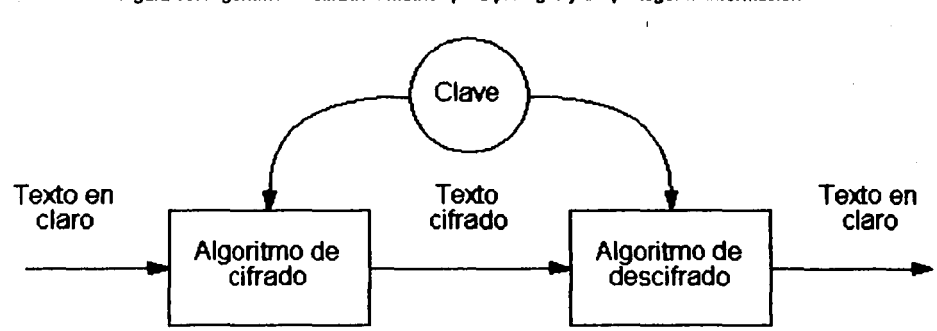
Esta técnica sigue dos métodos para cifrar o descifrar la información, los cuales son:

3.2.1.1 Cifrado simétrico

Es un mecanismo en el cual, cuando el texto es cifrado o protegido contra cualquier ataque, se emplea la misma clave con la que se protegió el texto en las operaciones de cifrado o descifrado, es decir, para proteger o desproteger el texto; además, cuando esto sucede, se dice que el texto cifrado o encriptado es *simétrico*.

A continuación se muestra una figura, en la cual se muestra el algoritmo para proteger la información mediante el cifrado simétrico:

Figura 13. Algoritmo de cifrado simétrico para proteger y desproteger la información



Fuente: http://www.iec.csic.es/criptonomicon/images/simetrico.gif

Estos sistemas son mucho más rápidos que los de clave pública o también llamado *cifrado asimétrico*, y resultan apropiados para el cifrado de grandes volúmenes de datos.

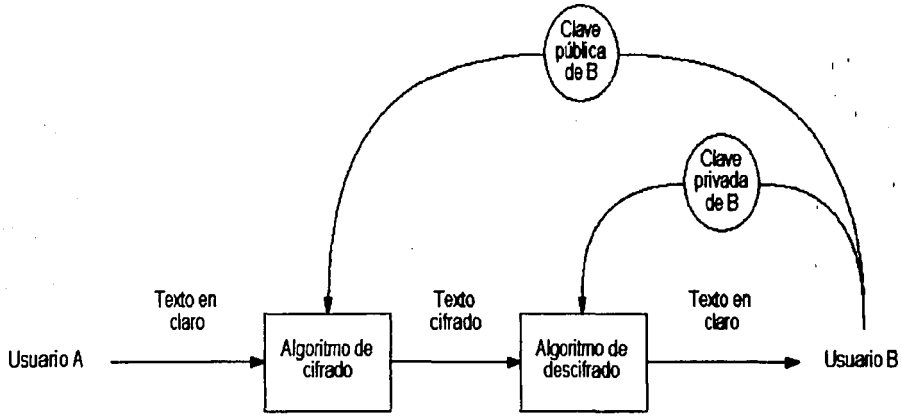
3.2.1.2 Cifrado Asimétrico

Otra técnica o mecanismo es el *cifrado asimétrico,* el cual consiste en utilizar dos claves para separar los procesos de cifrado y descifrado o proteger y desproteger la información; cuando esto se hace, a la información o al texto cifrado o encriptado se le llama cifrado asimétrico o clave pública.

Este mecanismo funciona con dos claves: una clave privada y una clave pública; en la clave privada se mantienen en secreto u oculta la información que se necesita proteger, mientras que clave pública, es conocida por todos. En forma general, las claves públicas se utilizan para cifrar, proteger u ocultar la información, mientras que las claves privadas se utilizan para desproteger o descifrar dicha información.

A continuación se muestra un algoritmo de cifrado asimétrico:

Figura 14. Algoritmo de cifrado asimétrico para proteger y desproteger la información



Fuente: http://www.iec.csic.es/criptonomicon/images/asimetrico.gif

El sistema posee la propiedad de que a partir del conocimiento de la clave pública o cifrado asimétrico, no es posible determinar la clave privada ni descifrar el texto cifrado con la clave. Los criptosistemas o texto cifrado de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión de trabajo y firmas digitales.

En general, el cifrado asimétrico se emplea para cifrar o proteger las claves de sesión utilizadas para cifrar el documento, de modo que puedan ser transmitidas sin peligro a través de la red junto con el documento cifrado, para que en éste pueda ser descifrado.

Además, el cifrado asimétrico se emplea para firmar documentos por medio de la técnica de firma digital.

3.2.2 Clave pública

La técnica de clave pública consiste en una combinación de las técnicas DES (*Data Encryption Standard*, Estandar de cifrado de datos) e IDEA (*International Data Encryption Algorithm*, Algoritmo Internacional de Cifrado de Datos). En este método se dispone de una clave secreta o privada que es utilizada para cifrar o descifrar la información.

Este hecho hace que para poder comunicar una información o mandarla, el destinatario o receptor no sólo tiene que conocer el mensaje cifrado, sino que tiene que conocer la clave para poder descifrar el mensaje que es enviado. Pero, para poder saber la clave, el emisor o el que envía la información debe darle a conocer la clave o comunicársela de alguna manera, y eso no puede ser de alguna otra forma más que por algún medio seguro.

Sin embargo, por eso es que en este punto es donde entran en juego las llamadas *claves públicas*. A diferencia de los sistemas de claves privadas, en los cuales se utiliza una misma clave para el cifrado y descifrado de la información, en la técnica de clave pública hay dos claves: una privada y otra pública. La clave privada se debe mantener siempre oculta, pues ésta clave no se da a conocer a nadie.

Cuando se quiera tener alguna comunicación de cifrado con alguien, es necesario que le entreguemos la clave pública con la que nosotros trabajamos, pero con la ventaja de que podremos hacerlo sin mayor preocupación, ya que para lo único que esta clave sirve es para cifrar información o datos que nosotros como criptoanalistas podemos descifrar.

Es importante tener en cuenta, que a partir de la clave pública es imposible deducir la clave privada. Puesto que las claves públicas y privadas son totalmente dependientes, éstas han sido diseñadas para que cualquier persona pueda conocer

y cifrar mensajes, información o datos con la clave pública. Pero solamente quien conozca la clave privada, podrá descifrar los mensajes o la información.

3.2.3 Criptografía

La criptografía (también conocida como encriptación) es una de las tantas técnicas que nos permiten guardar y tener segura la información de la empresa, así como también asegurar los datos que se tienen en cualquier PC.

Las técnicas criptográficas hacen que los ficheros no tengan utilidad para aquellas personas que no tienen acceso autorizado. La ciencia que se ocupa de las técnicas de cifrado y descifrado (llamadas también codificar y decodificar) de la información se llama *criptografía.*

La *criptología o criptografía* estudia la historia y los diferentes tipos de códigos y de cifrados que existen, mientras que el *criptoanálisis* se encarga de la codificación de mensajes cifrados. El procedimiento utilizado para cifrar información se denomina *algoritmo.*

Las técnicas criptográficas han cambiado a lo largo del tiempo. A lo largo de la historia existen documentos sobre el uso de la criptografía desde el siglo XIV, aunque existen evidencias del uso de codificación en la época egipcia, griega y romana. Una de las formas más simples acerca de la criptografía consiste en representar cada carácter por un carácter distinto.

Históricamente, existen 4 tipos o clases de individuos que han utilizado y han contribuido al uso de la técnica de la criptografía: los militares, los cuerpos diplomáticos, las personas que llevan un diario y los enamorados. De las cuatro clases, una de ellas es la que más ha destacado al usar esta técnica, y es el grupo de los militares.

Dentro de este grupo, los mensajes o la información que era de suma importancia para los jefes de mayor mando y que se necesitaban poner en clave o protegerlos de cualquier ataque externo, le asignaban ese trabajo a empleados que trabajaban para los jefes, y que realmente éstos eran los indicados para poder efectuar dicho trabajo y para transmitir los mensajes encriptados a los jefes.

Pero la escasez de mensajes o información que se tenía que encriptar, impedía que este trabajo se llevara a cabo, porque a los empleados encargados de hacerlo no podían, y es por eso que se le asignó dicho trabajo a un grupo de especialistas en el arte de encriptar mensajes o información secreta para el campo militar.

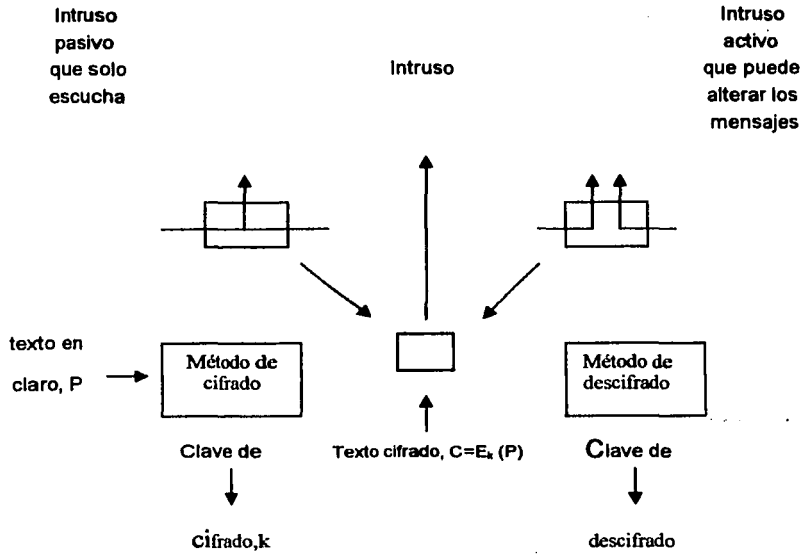
Cuando aparecieron las computadoras, las principales restricciones de la criptografía, era la falta de habilidad que tenían los codificadores para poder entender la información que se encontraba oculta y transformarla en mensajes más entendibles para el usuario; pero esto era un proceso demasiado lento, porque no se contaba con el equipo adecuado para hacerlo.

Una de las tantas restricciones ha sido la dificultad para conmutar o unir la información o mensajes requeridos de un método criptográfico a otro, puesto que esto obliga a reciclar personal para que realice este trabajo de conmutar de un método criptográfico a otro la información.

Sin embargo, aunque existe el peligro de que un codificador sea intervenido por algún intruso que quisiera esa información, éste puede ser mucho más hábil y tener la capacidad para cambiar el método criptográfico cuando sea necesario y cuantas veces lo requiera.

Es por eso que dichos requisitos de conflicto referentes al ataque de querer tomar información solamente para modificarla, ha generado un modelo para los requisitos de conflicto que se presenta en la siguiente figura:

Figura 15. El modelo puesta en clave



Fuente: ***Arquitectura de computadoras. Un enfoque cuantitativo,*** España, 1993, Editorial Mc Graw Hill, p.827

Una regla fundamental de la criptografía es que, por lo regular, el criptoanalista[10] debe estar capacitado para conocer el método de cifrado que nos permita cifrar la información de la empresa. En resumen, el criptoanalista debe conocer la forma en como trabaja el método de cifrado mostrado en la figura anterior, y además esto se hace con el criptoanálisis.[11]

Sin embargo, veamos que, desde el punto de vista de los criptoanalistas, no es tan sencillo ver que el problema del criptoanálisis cuenta con tres desventajas, que son:

[10] **Criptoanalista:** Es la persona que se encarga de cifrar la información o mantenerla segura, es decir, de proteger la información bajo alguna clave de acceso utilizando otra técnica o mecanismo de seguridad.
[11] **Criptoanálisis:** Es el arte o manera de quebrar, tumbar o desproteger la información que es importante para la empresa y que se tiene oculta.

- Cuando alguna cantidad de información que se encuentre cifrada y otra no, surge el problema de que el criptoanalista solamente tiene *texto cifrado*.

- Cuando se tiene información cifrada y alguna solamente se encuentre sin cifrar, a este problema se le conoce como *problema de texto en claro o sin cifrar conocido*.

- Y, por último, es cuando el criptoanalista tiene la habilidad de poner en clave la información que esté sin cifrar que se desee; a este problema se le conoce como *problema de texto en claro seleccionado*.

Históricamente, podríamos decir que la criptografía abarca lo que es la técnica de cifrado, pero este método se ha dividido en dos categorías que serán mencionadas dentro de ésta técnica, y son: *cifradores de substitución* (incluyendo los códigos) y *cifradores de transposición*. Se mencionará a cada uno de ellos por separado.

3.2.3.1 Criptografía de cifrado por sustitución

En este método, cada letra o grupo de letras que se tiene para proteger la información, se substituye por otras letras diferentes para poder disfrazarlas, es decir, para que otro usuario no adivine cuál es la clave secreta que permite ver la información. Esta técnica utiliza el cifrado de César, en el cual las letras del alfabeto son representadas por otras letras del mismo alfabeto pero en letras mayúsculas, por ejemplo la letra *a* se representa por *D, b* se representa por *E, c* se representa por *F,....,* y *z* se representa por *C*. Cuando se tengan letras o texto sin cifrar, éste se representará con letras minúsculas, mientras que la información o textos cifrados utilizarán letras mayúsculas. Esta técnica de cifrado de César permite que la información o texto cifrado se pueda desplazar *k* espacios, en lugar de que sean 3 lugares, el cual es el desplazamiento requerido.

El origen de esta técnica es muy antiguo, pues se dice que Julio Cesar utilizó la técnica de cifrado para desplazar letras del alfabeto tres posiciones. Este tipo de técnica se conoce como *cifrado por sustitución.*

Esta técnica se utiliza en aplicaciones donde el grado de protección no es tan importante, para esto se utiliza un plan de codificación llamado *ROT-13*[12] que es utilizado en Internet para poder ocultar información, por ejemplo, chistes ofensivos u ocultar el final de una película, es por eso que esta técnica de sustitución se basa en desplazar cada letra 13 lugares o posiciones.

A continuación se muestra la tabla que muestra el plan de codificación, así como su código en lenguaje C:

Figura 16. Plan de codificación ROT-13

Rot-13	Normal	Rot-13	Normal	Rot-13	Normal	Rot-13	Normal
A	N	H	U	O	B	V	I
B	O	I	V	P	C	W	J
C	P	J	W	Q	D	X	K
D	Q	K	X	R	E	Y	L
E	R	L	Y	S	F	Z	M
F	S	M	Z	T	G		
G	T	N	A	U	H		

Fuente: ***El libro de las comunicaciones del PC,*** México, Editorial AlfaOmega, 1997, p. 743

[12] **ROT-13:** Plan de codificación para ocultar información o texto para que sea protegido, y poder desplazar cada letra del texto, 13 posiciones dentro de la memoria.

Figura 17. Código en C de la codificación ROT-13

```
/ * Cifrado de sustitución Rot-13 * /

# include < stdio.h >
int main ( ) {
        int c;
        while ((c=getchar( )) ! = EOF) {
          if (c>='a'&&c<='m') c=c+13;
          else if (c>='n'&&c<='z') c=c+13;
          else if (c>='A'&&c<='M') c=c+13;
          else if (c>='N'&&c<='Z') c=c+13;
          putchar(c);
        }
        return 0;
}
```

Fuente: Idem

Otra de las técnicas de sustitución que se utilizan son aquellas que se basan en escribir una palabra clave que es seguida por letras del alfabeto, al cual le han quitado las letras de la palabra clave; por ejemplo, si la palabra clave fuese la palabra PUERTA, al querer ocultar esta clave con la técnica de cifrado sería de la siguiente manera:

Abierto: PUERTABCDFGHIJKLMNÑOQSVWXYZ

Cifrado: ZYXWVUTSRQPOÑNMLKJIHGFEDCBA

El resultado deseado es que para conseguir un texto cifrado o protegido, se sustituirían en el texto abierto la letra P de la palabra PUERTA por la letra Z en el texto cifrado, la letra U por la letra Y, la letra E por la X, y así sucesivamente.

El decodificar cualquier texto cifrado con la técnica de sustitución llamada ROT-13 no tiene mucha complejidad, porque para un criptoanalista que tiene experiencia en el encriptado de datos, es mas sencillo, ya que solamente basta con contar las veces que aparece cada letra del texto cifrado y aplicarle la tabla de frecuencias de las letras del idioma en el que está escrito el texto.

Enseguida se muestra la tabla de frecuencias de las letras de acuerdo al idioma en el que está cifrada la información:

Figura 18. Tabla de frecuencias para desplazar letras del texto cifrado

TABLA DE FRECUENCIA DE LAS LETRAS							
INGLES				HOLANDES			
A	7.25	N	7.75	A	8.25	N	10.25
B	1.25	O	7.50	B	1.75	O	6.00
C	3.50	P	2.75	C	1.00	P	1.75
D	4.25	Q	0.50	D	5.25	Q	0.25
E	12.75	R	8.50	E	19.00	R	6.25
F	3.00	S	6.00	F	1.00	S	4.00
G	2.00	T	9.25	G	3.00	T	7.25
H	3.50	U	3.00	H	2.50	U	2.50
I	7.75	V	1.50	I	6.50	V	2.25
J	0.25	W	1.50	J	1.50	W	2.00
K	0.50	X	0.50	K	2.75	X	0.25
L	3.75	Y	2.25	L	4.00	Y	0.25
M	2.75	Z	0.25	M	2.75	Z	1.25

Fuente: ***El libro de las comunicaciones del PC***, México, Editorial AlfaOmega, 1997, p. 743

3.2.3.2 Criptografía de cifrado por transposición

A diferencia del cifrado por sustitución, los cifradores de transposición, reordenan el texto que fue cifrado pero no lo disfrazan.

En la figura mostrada, se describe un cifrador de transposición de tipo columnar.

Figura 19. Cifrador de transposición

M	E	G	A	R	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Texto en claro (sin cifrar):
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Texto cifrado:
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Fuente: ***Arquitectura de computadoras. Un enfoque cuantitativo,*** España, Editorial Mc Graw Hill, 1993, p. 827

En este tipo de cifrado, la clave es una palabra o una frase que no contiene ninguna letra repetida. En el ejemplo anterior, la palabra clave es **MEGABUCK**, y su propósito es el de numerar las columnas, en donde la columna 1 (que es el texto en claro) queda enumerada debajo de la palabra clave de acuerdo a la letra que se encuentra más próxima al comienzo del alfabeto (en este caso es la letra **A**), y así sucesivamente.

El texto cifrado se lee por columnas, es decir, comenzando por la columna donde se encuentra el numero 1, en este caso es en la letra **A**, después con la letra **B**, y así sucesivamente.

Para que un criptoanalista pueda descifrar o desbaratar un cifrado por transposición, debe reconocer que se trata de un cifrado de este tipo, después identifica la frecuencia de las letras **E, T, A, O, I, N**, las cuales son las letras que mas se adaptan al texto que se encuentra sin cifrar o en claro. Si esto llega a suceder, entonces se trata de un cifrador de transposición, porque todas las letras que aparecen en el texto que se cifrará, se representan a sí mismas.

Por otro lado, el siguiente paso consiste en determinar cuál es el número de columnas de acuerdo al tamaño de la palabra clave que protege la información, ya que en la mayoría de los casos puede una palabra o frase, ser adivinada.

Algunos cifradores de transposición, aceptan un bloque de entrada de datos de longitud fija, y producen una salida de la misma longitud.

Además estos cifradores pueden describirse, es decir, con dar solamente una lista de palabras se indicará el orden en que se deben de salir las letras. Veamos un ejemplo de este cifrado:

En la figura 18, se muestra un cifrador con un bloque de 64 caracteres, en la cual su salida, es decir, el texto cifrado es 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, ..., 62. En otras palabras los números indican el caracter de entrada, en este caso es la letra *a* que se encuentra en el número 1, y es la primera en salir, después seguirá la letra *f* que corresponde al número 12 dentro de esa misma columna, y así sucesivamente.

3.2.4 DES

Otra de las técnicas para proteger la información de la empresa, es la técnica llamada *DES*. Esta técnica, como su nombre lo indica (*Data Encryption Standard, Estándar de cifrado de datos*), es un método que es parecido al cifrado y es una de las técnicas más utilizadas para proteger la información.

Esta técnica fue desarrollada por IBM en los años sesenta, al cual se le dio más tarde el nombre de Lucifer.[13] Esta técnica o método es un código combinado de la criptografía de cifrado por sustitución y transposición que funciona con bloques de datos de una longitud de 64 bits.

[13] Se le dio ese nombre porque hace referencia a una combinación de las técnicas de cifrado por sustitución y transposición y además porque funciona similarmente.

Sin embargo, este código utiliza una palabra clave de 7 caracteres, los cuales contienen un numero de combinaciones posibles de 256^7 = 72.057.594.037.927.940.

De otra forma si la computadora mas poderosa del mundo, construida especialmente para descifrar claves, quisiera descifrar dicha clave, tardaría más de 10 horas descifrando esa clave.

Es importante tener en cuenta que la criptografía moderna utiliza ideas que se basan en la criptografía tradicional, es decir, cifrado de sustitución y transposición, pero que su énfasis es diferente.

Es por eso, que los criptógrafos utilizan algoritmos más sencillos para proteger la información de la empresa de una manera segura utilizando claves muy largas para una mayor protección.

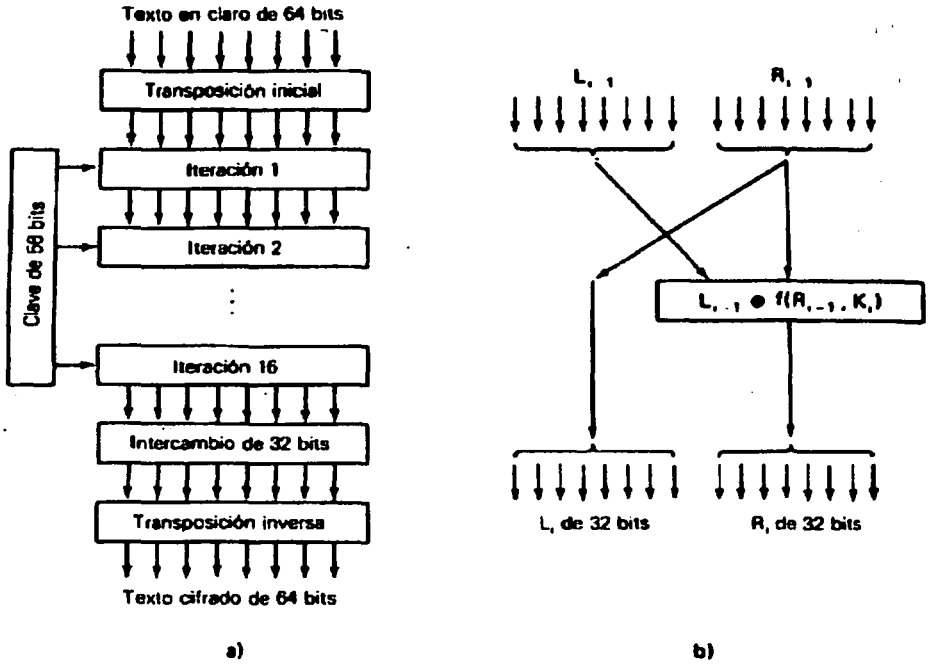
Sin embargo, en enero de 1977, la compañía IBM desarrolló un cifrador, el cual el gobierno de los Estados Unidos adoptó como una norma para proteger su información de posibles ataques.

Pero al adoptar este cifrador llamado DES, los fabricantes que se dedicaban a cifrar información en su computadora, al estar enterados de esto, ellos comenzaron a cifrar la información que tenían dentro de sus computadoras por medio de esta técnica y la llamaron *Cifrado de datos*. Esta técnica hacía que el proceso de cifrado fuese más rápido.

Otro punto importante es la disponibilidad de tener un equipo de cómputo para poder realizar esta tarea, es decir, que sea rápido y económico. Pues ya que esto ha estimulado a muchos usuarios dentro de la empresa y externos a optar por usar esta técnica.

A continuación se muestra uno de los algoritmos que utiliza esta técnica para cifrar la información de cualquier computadora:

Figura 20. Técnica DES. a) Esquema general b) Detalle de una iteración



Fuente: ***Redes de Ordenadores,*** 3a. ed., México, Editorial Prentice Hall, 1997, p. 813

3.2.5 IDEA

Otra técnica que también es muy importante para la protección de la información, es la llamada IDEA (*International Data Encryption Algorithm*, Algoritmo Internacional de Cifrado de Datos).

IDEA las que sus siglas son (*International Data Encryption Algorithm, Algoritmo Internacional de Cifrado de Datos*), fue creado en 1992 por dos ingenieros llamados Xuejia Lai y James L. Massey en Zurcí, Suiza.

IDEA lo que hace es que corrige los principales errores que tiene la técnica DES, pero a diferencia de la técnica anterior, ésta es un cifrador de bloque simétrico, porque funciona similar al cifrado simétrico, solo que esta técnica opera con bloques de 64 bits y emplea una llave de 128 bits para mayor seguridad de la información. Entre más grande sea la llave, mayor seguridad en nuestra información, y no corre peligro de que la clave sea descifrada.

Es importante tener en cuenta que esta técnica, es considerada como un cifrador por bloques robusto de gran seguridad, porque al momento de escoger la clave para asegurar la información, la palabra que será cifrada para ocultar la información se debe de hacer similar a la criptografía de cifrado por transposición, es por eso que se dice que se hace por bloques.

Una de las desventajas de esta técnica es que como es una técnica muy reciente, corre el riesgo de que sea vulnerable, y que día con día exista una nueva técnica que sea mejor que el IDEA, pero que aún no se ha descubierto.

3.2.6 PGP

La técnica del PGP (*Pretty Good Privacy, Privacidad realmente buena*) es una técnica de cifrado de datos que ha alcanzado un gran avance en los sistemas de cifrado de datos en general. Este programa fue desarrollado por Phil Zimmermann en 1990.

Aunque actualmente existen otras versiones de sistemas operativos, esta técnica permite trabajar en diferentes sistemas operativos como: MSDOS, Unix, Mac,

Linux y VAX/VMS, aunque también es importante decir que ésta técnica utiliza algoritmos, los cuales son gratuitos (se puede encontrar una copia en Internet).

Es importante mencionar que esta técnica, se enfoca principalmente en asegurar nuestro correo electrónico, porque es el medio que más rápido puede atacarse, es por eso que ésta técnica se usa para proteger la información que se envía por este medio y al momento de recibir algún correo externo, también corre el riesgo de que se pueda perder dicha información.

Es importante mencionar que la técnica PGP no utiliza ningún algoritmo propio, sino que integra algoritmos conocidos como DES, IDEA y otros.

Sin embargo, esta técnica cuenta con ciertas características que la hace diferente a las demás, y son:

- Primer programa de fácil uso que emplea métodos de cifrado de calidad en operaciones militares.

- Permite la protección de ficheros personales o archivos de datos, mediante la técnica de clave secreta o privada utilizando una de las técnicas mas fiables y robustas, IDEA.

- Facilita el intercambio de mensajes y ficheros de datos protegidos sin necesidad de disponer de un canal seguro por el cual se puedan enviar los datos y la clave secreta. Pero esto es posible gracias a la técnica de RSA.

- Dispone de un mecanismo de *firma electrónica o digital,* que garantiza la autenticidad de un mensaje enviado o un fichero de datos. Esto se hace con la técnica MD5.

Para un mejor entendimiento, la técnica del PGP se trata de "*un programa para cifrar y descifrar datos de todo tipo, y resulta especialmente práctico para el uso de correo electrónico*"[14].

En resumen, las ventajas que ofrece esta técnica son muy importantes, para asegurar la información que se envía por correo, y son:

- Es un programa gratuito para usos no comerciales.
- Está disponible para múltiples tipos de computadoras y sistemas operativos.
- Es un programa de manejo sencillo, especialmente si se usa a través de MSDOS, o en otros sistemas operativos como Windows, Linux, Mac.
- Resulta virtualmente indescifrable para cuando la clave es larga.

El funcionamiento de esta técnica, es básicamente como un algoritmo que utiliza clave pública o asimétrica.

Esto es, que en un algoritmo de clave pública, cada usuario que quiera proteger la información importante, deberá crear un par de claves que consisten en una clave pública y otra privada. La clave pública es la que se distribuye, por ejemplo como si fuera la cuenta de correo electrónico, y sirve para enviar un mensaje codificado en el cual solo el usuario puede descifrar mediante su clave privada, como por ejemplo, la contraseña del correo.

[14] **http://www.iec.csic.es/criptonomicon/correo/recursoscorreo.html**

Es preciso saber que, no se puede cifrar ni descifrar con la misma clave porque esto ocasionaría conflicto, y además, la clave privada debe mantenerse en secreto por el usuario.

Por último, al emplear la técnica de PGP y al entender su funcionamiento, resulta demasiado complejo, pero no lo es, ya que esta técnica en resumen, es enormemente segura y fácil de usar.

3.2.7 Claves de acceso

Otra técnica mas es la llamada *claves de acceso;* como su nombre lo indica, es utilizado para guardar bajo una clave cualquier documento que queremos que esté asegurado.

No obstante, es importante tener en cuenta que algunas veces, los ataques que se realizan a la red, pueden ser de las personas que accesan a cualquier computadora de la red que se encuentra en cualquier área de la empresa, o personas que de alguna forma han tenido acceso al servidor de la red que es el que controla todas las tareas que se realizan en cada estación de trabajo.

Es por eso que, para disminuir el riesgo de acceso a cualquier computadora dentro de la empresa, se disponga de niveles de control que nos permitan proteger y prevenir la información de un posible ataque. Los puntos a considerar son:

- Restringir el acceso físico a las personas mediante llaves o tarjetas de identificación a las áreas donde se encuentran las estaciones de trabajo.

- Utilizar procedimientos como huella digital, dibujo ocular o frecuencia de voz, al personal que quiera accesar al área de trabajo donde se encuentren las computadoras a usar.

- Restringir la posibilidad de poner en funcionamiento las estaciones de trabajo. Para ello, se utilizarán claves de acceso a la computadora a utilizar, tarjetas de identificación o llaves.

- Restringir el acceso a la información de la red, mediante claves de acceso a la computadora.

- Restringir el acceso de los usuarios a determinadas áreas de datos, mediante claves de acceso.

- Registrar toda la actividad que se realiza en las estaciones de trabajo, identificando al usuario que las lleva a cabo.

- Controlar o impedir todas las operaciones de copia de archivos a discos flexibles de información de la red.

Este último punto es muy importante porque hay computadoras que cuentan con una unidad de disco flexible y otras no, entonces para aquellas que si tienen unidad de disco flexible corren el riesgo de infectar el servidor, principalmente la red, de virus que las que no tienen unidad de disco flexible.

Por último, hay que tener en cuenta que el servidor de la red, es aquel donde está contenida toda la información de la red, y hasta de la empresa, es por eso que es necesario tener siempre copias de seguridad o asegurar la información que se encuentre dentro de éste, además solamente esto lo debe hacer el administrador de

la red, pues él solamente debe tener acceso al servidor y a la información almacenada dentro de él.

3.2.8 Firma digital

Otra técnica más es la llamada *Firma digital o electrónica,* la cual consiste en "*cifrar un documento con clave privada para obtener una firma digital segura, puesto que el usuario que posea la clave privada puede descifrar el documento y puede hacerlo*"[15].

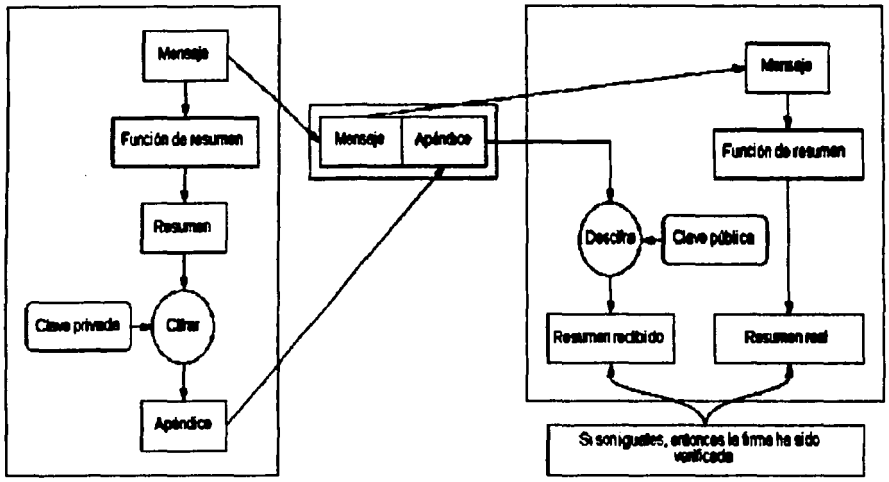
En principio, cualquier persona puede descifrar la información protegida por clave pública, demostrando así la identidad del firmante. Por eso es importante que en la practica, debido a que las técnicas de clave pública no son tan confiables al momento de cifrar la información o un documento que es demasiado grande, los protocolos de firma digital se implementen junto con funciones unidireccionales para que en vez de firmar todo el documento o la información que va a ser protegida o cifrada, y esta a su vez vaya a ser enviada, se firme el resumen del documento o, en otras palabras como si fuera una copia.

Esta técnica de firma digital, implica el cifrado mediante la clave del emisor, que es el que realiza el cifrado del mensaje antes de ser enviado y ser recibido por el receptor; cuando el mensaje es recibido por el receptor, éste se procesa para verificar su integridad y su validez.

Por tanto, los pasos del protocolo de firma digital se muestran en el diagrama siguiente:

[15] **http://www.iec.csic.es/criptonomicon/correo/firma.html**

Figura 21. Esquema para llevar a cabo una firma digital de un documento



Fuente: http://www.iec.csic.es/criptonomicon/images/firma.gif

Los pasos para llevar a cabo la firma de un documento, como lo muestra la figura son:

1. A genera un resumen del documento.
2. A cifra el resumen con su clave privada, firmando por tanto el documento.
3. A envía el documento junto con el resumen firmado a B.
4. B genera un resumen del documento recibido de A, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De alguna forma, estos pasos ofrecen los servicios de *no repudio*[16], ya que nadie, excepto A (cuadro 1), podría haber firmado el documento, y de autenticación,

[16] El "*no repudio*" ofrece protección a un usuario de otro (es decir tienen cierta comunicación), pero cuando el segundo usuario recibe cierto mensaje enviado por el usuario uno , éste lo niega y se dice que no se realizó ninguna comunicación.

porque si el documento viene firmado por A, entonces podremos estar seguros de su identidad.

Por último lugar, la técnica de firma digital garantiza la integridad del documento.

3.2.9 Intercambio de autenticación

Otra técnica basada en el cifrado de información es la llamada *Intercambio de autenticación o autentificación.* Esta técnica asegura que una entidad, ya sea origen o destino donde va a llegar la información, sea la correcta y deseada.

Un ejemplo de ello, es cuando A envía un numero aleatorio cifrado con la clave pública de B, pero B lo descifra con su clave privada y se lo reenvía a A.

Es importante que en esta técnica se tenga que ser cuidadoso al momento de diseñar los protocolos que nos van a permitir enviar la información cifrada, porque pueden existir ataques para poder desbaratar la información cifrada.

Otra fuente de información, nos dice que "*la autenticación o autentificación puede realizarse en el momento en que se establece una sesión, es decir, al momento de comenzar a trabajar en una computadora*".[17]

Esto se hace, cuando el usuario comprueba su identidad, mediante una contraseña, la cual le va a permitir hacer uso de la computadora.

[17] En su obra ***Redes de Computadoras,*** 3ra. ed., México, Editorial Prentice Hall, 1997, p. 813.

3.2.10 Integridad de datos (ICV)

Esta técnica, no es muy conocida pero funciona similar al cifrado, esta técnica implica el cifrado de cadena comprimida de datos o información a transmitir, llamada generalmente valor de comprobación de integridad (*Integrity Check Value o ICV*).

Esta técnica, envía los datos o información al receptor, el cual repite la comprensión de los datos y el cifrado de los mismos, y enseguida compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

3.2.11 Tráfico de relleno

Esta técnica, consiste en enviar tráfico de información junto con los datos cifrados, para que el usuario que ataque dicha información no sepa si se está enviando información a otro usuario, así como también no sepa la cantidad de datos que se están transmitiendo.

Como vemos, esta técnica es fácil de usar, pero al igual que las demás, se necesita un algoritmo para poder cifrar la información que se quiere mandar, y además dicho algoritmo debe contar con seguridad de la información al momento de enviarla a otra persona.

3.2.12 Control de encaminamiento

Otra técnica que nos permite asegura la información es la llamada *control de encaminamiento,* esta técnica nos permite enviar determinada información por determinadas zonas, ya sea por correo electrónico o simplemente enviar información de una computadora a otra.

Asimismo, nos permite poder utilizar otras rutas, en caso de que se detecten violaciones de integridad al momento de enviar la información a otro usuario y por la ruta equivocada.

3.2.13 Unicidad

Al igual que las técnicas anteriores, existe otra mas llamada *unicidad,* la cual consiste en añadir a los datos o información un numero de secuencia, es decir, fecha y hora en la que será enviada la información a otra persona.

Esto se hace con la finalidad de que en la información que se enviará, incluya firma digital e integridad de los datos, para poder así evitar amenazas, como el que se pierdan los datos o el volver a firmar la información.

Por ultimo, es importante mencionar que existen otras técnicas[18] que nos permiten guardar o proteger la información de la empresa y de cualquier computadora de cualquier ataque pero que de cualquier manera, son igual de útiles como las anteriores.

3.3 Seguridad en las PC's

Cuando se habla de la seguridad en la PC, es importante tener en cuenta que mucha gente cree que se tiene que proteger dicha PC de alguna caída o de algún robo, pero esto no es así.

La seguridad en las PC's, va más allá de lo anteriormente propuesto. Debemos tener en cuenta que una PC (comúnmente llamada *computadora de escritorio*), también se debe proteger internamente. Esto es, proteger el software que está

[18] HASH, Triple DES, RC5, MD5, RSA, DSS, NIST, AES.

almacenado dentro de ella, el sistema operativo, el BIOS[19] y hasta el sector de arranque.

Pero, antes de entrar en materia de la seguridad en las PC's, debemos distinguir entre lo que es la seguridad o protecciones de acceso a la computadora que se desea utilizar y lo que corresponde a proteger o asegurar la información que se tenga dentro de la computadora. Los puntos a considerar para proteger el acceso a la computadora personal, son:

- *Protección por clave en el BIOS.* Si la BIOS está protegida, al momento de encender la computadora, se ejecuta una rutina del BIOS que se encuentra en el sistema operativo y pregunta al usuario cual es la clave de acceso. Si en este caso no se sabe la clave o si se tecleó y no fue correcta, la computadora, detiene el proceso de acceso al ordenador.

- *Protección por clave en el sector de arranque.* Tanto los discos duros como los discos flexibles cuentan con un sector especial o principal que es el sector llamado "sector de arranque o sector cero". Este sector contiene las rutinas de arranque de la computadora, ya sea cuando la computadora tenga cargado el sistema operativo MSDOS. Los programas protectores graban su código en el sector de arranque, de forma que al encender la computadora se ejecutarán pasando el contenido original del sector de arranque a un sector diferente que él mismo ejecuta.

- *Protección por cable en el AUTOEXEC.BAT o CONFIG.SYS.* En este tipo de protección, la comprobación de la clave que protege estos archivos, se hace a través de programas que los mismos archivos tienen instalados. Es por eso que

[19] BIOS (Basic Input Output System): es el sistema básico de entrada/salida donde se encuentra todas las características de la computadora.

este método no es muy conveniente porque el propio usuario lo puede abortar o ignorar, lo cual convierte al método en un método no seguro de usar.

- *Protección de arranque desde el disco flexible.* En los casos en los que se este utilizando algunos programas de seguridad que deban ser cargados desde el disco duro, es necesario impedir que el usuario de algún modo pueda cargar el sistema operativo que trae en el disco flexible de arranque. Por eso, casi todas las computadoras actuales no permiten que el arranque desde el disco flexible se haga, y para hacerlo se tiene que especificar en la configuración del SETUP de la BIOS, pero para los casos en los que esto no sea posible, los programas de protección que se graban en el sector cero del disco duro solucionan este problema.

Otro caso, es cuando más de una persona tiene que utilizar la misma computadora, para este caso puede que se necesite disponer de ciertas medidas de seguridad que permitan mantener hasta cierto grado un punto de confidencialidad. Para estos casos, es importante mencionar algunos puntos para evitar que esto suceda.

Los puntos son:

- *Protección de directorios/ficheros.* En este punto existen ciertos programas de seguridad que controlan el acceso a dichos directorios. Esto permite que muchos usuarios puedan compartir una misma computadora sin necesidad de perder dicha información almacenada en la PC.

- *Auditorias.* En las auditorias se realiza un registro del tiempo en el cual los usuarios realizaron tareas en una determinada computadora. Es importante mencionar que las auditorias se lleven a cabo cuando se tenga que hacer uso de alguna computadora, es decir, tener control de las personas que usan

dicha computadora y así poder depurar errores que no permitan que la computadora se apague.

3.3.1 Medios de seguridad para proteger la información

Para poder proteger cualquier computadora que este al alcance de cualquier usuario, es importante que se tengan las precauciones necesarias para que una computadora no sufra ningún daño alguno.

Es por eso que existe la posibilidad de que al momento de encender cualquier computadora se tenga que restaurar el sistema para una mayor seguridad y así poder proteger la computadora de cualquier daño.

No obstante, si por alguna razón cuando se tenga que encender la computadora y ésta no responda, es necesario tener toda nuestra información respaldada en disquetes o en un CD-ROM para una mayor seguridad.

Por eso, es importante respaldar la información que se tiene en la computadora, porque nunca se puede predecir que es lo que vaya a pasar y pues algo como lo anteriormente expuesto a nadie se le desea y, además en casos como este, siempre es bueno saber que hacer.

Dicho de otra manera, cuando suceda este tipo de situaciones, si no se puede arrancar la computadora, es decir, encenderla, se debe tener previsto un disco flexible con los programas necesarios para poder arrancar el sistema y restaurarlo.

Para cuando esto sucede no esta de mas decir que se tengan dos disquetes en caso de alguno de ellos se dañe. A estos discos se les llama *discos de emergencia.*

Pero en estos discos de emergencia, se pueden guardar dos tipos de datos diferentes, es por eso que estos discos se dividen en dos categorías que son: ***discos de emergencia de programas y discos de emergencia de datos.*** A continuación se describe cada uno de ellos.

- *Discos de emergencia de programas.* En estos discos se guardan todos aquellos ficheros y programas que nos permiten arrancar la computadora cuando ésta falle y también contiene las utilidades para poder recuperar información que ha sido perdida. Los ficheros pueden ser:

    1. *Ficheros del sistema operativo para poder arrancar la computadora.*
    2. *Utilidades para revisar el disco duro que este libre de fallos y de recuperación de la información.*
    3. *Utilidades de respaldo (Backup) para poder recuperar copias de seguridad de los archivos perdidos.*

- *Discos de emergencia de datos.* En este tipo de discos, se guarda información referente a datos de restauración completa para el área del disco duro. Los datos que contiene son los siguientes:

    1. *Copia de los ficheros CONFIG.SYS y AUTOEXEC.BAT del disco duro.*
    2. *Copia de los ficheros BAT específicos que tengamos en el directorio raíz o principal.*
    3. *Copia del sector que contiene la tabla de particiones.*
    4. *Copia del sector de arranque, sector 0.*
    5. *Copia de los sectores que contienen la FAT.*
    6. *Copia de los sectores que contienen el directorio raíz.*

Es importante mencionar que para tener copia de todos estos ficheros, se pueden utilizar los comandos del DOS[20], algunos de ellos son: COPY o XCOPY, o bien cualquier programa que sea alguna herramienta de utilería como lo es: PCtools, Norton, etc.

Para el caso del sector de arranque, se utiliza la tabla de particiones, FAT, etc., pero también se puede utilizar herramientas del DOS como Mirror o Unformat, aunque también existen software comercial que puede hacer o realizar esta tarea, tales como PCTools, utilerías Norton, Mace Utilities, entre otras.

Para poder tener una copia de seguridad de la información que tiene un determinado valor tanto para la empresa como para cualquier usuario, se debe de tener una copia de seguridad o *backup.* Sin embargo, para muchos esto no es muy importante, pero debería serlo.

Debe serlo, porque en ocasiones cuando se intenta abrir un archivo, por ejemplo una base de datos o un programa como pudiera ser una nomina, y que la computadora no funcione o que los datos no se muestren, entonces si nos preocupamos porque los datos no se ven y es cuando decimos ¡Porque no hice una copia de seguridad de los archivos!. Es por eso que el que no haga copias de seguridad de su información está perdido.

Para que esto no suceda tan frecuentemente, podemos pensar en hacer copias de todo el disco duro para no perder información importante en discos flexibles pero para esto se necesitarían muchos discos y además tiempo para hacerlo.

[20] DOS: Disk Operating System. Disco de Sistema Operativo.

Sin embargo, como lo menciona el autor José A. Carballar[21], existen varias formas o medios de hacer copias de seguridad de la información, y estas son:

- *Copias de seguridad globales.* En este tipo de copias se tienen que copiar todos los datos que se encuentran en el disco duro, incluyendo la estructura de árbol del directorio raíz. En este tipo de copia se saca una copia del disco duro en discos flexibles, por lo cual es muy fácil recuperar por completo el disco duro en caso de que éste tenga una falla total. Por otro lado, es muy tardado hacer este tipo de copia o backups (respaldos).

- *Copias de seguridad parciales.* Este tipo de copias consiste en sacar copias de todos los ficheros que se encuentren en un mismo directorio o subdirectorio pero que a su vez pueden o no contener la misma extensión. Este tipo de copia es más fácil de hacer y es mucho más rápida porque pueden ocupar de espacio un solo disco flexible y también se pueden utilizar los comandos del DOS. Además existen muchas utilerías de copias de seguridad para hacer este tipo de copias parciales.

- *Copias de seguridad parciales avanzadas.* En este tipo de copia, se realiza una copia de todos los ficheros o archivos a los que se le han hecho algún cambio desde que se realizó la última actualización. Los archivos contienen atributos que son, archivos de lectura, archivos ocultos o archivos de sistema, etc., pero uno de los atributos es el de archivo, y se pone en uno (*on*) cada que se va a hacer uso de ese archivo y éste sea modificado, y se pone en cero (*off*) cuando el DOS hace una copia de él por medio de una utilidad de backup (respaldo).

[21] En su obra ***El libro de las comunicaciones del PC. Técnicas, programación y aplicaciones,*** México, Editorial Alfaomega, 1997, p. 743.

Es importante hacer énfasis en lo que a copias de seguridad se trata, porque al mencionar las diferentes formas de tener una copia de seguridad de nuestros archivos y que además faltan por mencionar algunas mas, es necesario recordar que también por medio de la utilería PCTools se pueden ver los atributos de los ficheros o incluso modificarlos, pero esto se hace mediante el comando del DOS llamado ATTRIB.

Otros medios para asegurar la información almacenada en cualquier computadora de la empresa o incluso la que se tiene en el hogar, es mediante otros medios o formas que se menciona el autor José A. Carballar[22], las cuales son:

- *Copias de seguridad simultáneas.* Estas copias de seguridad son realizadas por un medio como lo son, las unidades especiales que permiten hacer trabajar a dos unidades de discos en paralelo, permitiendo así que se escriban los datos simultáneamente en los mismos sectores de ambos discos.

- *Copias de seguridad temporales.* Este tipo de copia de seguridad, consiste en realizar copias secundarias de los ficheros a los que se les quiera hacer una copia. Esta segunda copia se realiza en la misma unidad de disco, ya sea un disco duro o un disco flexible. La mayoría de los programas realizan esta operación automáticamente, asignándole el mismo nombre al fichero que se copió con la extensión BAK. Es por eso que cuando suceda por alguna razón un borrado de algún archivo o fichero, ya se tiene por precaución una copia de éste archivo.

- *Copias de seguridad en serie.* Este tipo, consiste en hacer varias copias de cada una de las versiones de todos aquellos ficheros que han sido modificados y de los que constantemente se hagan modificaciones. Este tipo

[22] Idem.

de copia se diferencia de las copias temporales en que mientras las copias temporales hacen dos copias de cada fichero, es decir, original y la copia, las copias en serie hacen varias copias de cualquier fichero con todo y las versiones anteriores y las actuales. Este tipo de copia es utilizada por los programadores porque les permite corregir una modificación mal realizada en algún programa.

- *Copias de seguridad en cintas magnéticas.* Existe una última copia de seguridad la llamada *copia en cinta magnética.* Este medio es ideal para hacer copias de seguridad (backups) de los datos que se tengan en el disco duro. Además, las unidades de cinta se conectan a la computadora como si fueran una unidad de discos flexibles. Las cintas tienen una densidad de datos que es de 3150 bits por centímetro y una velocidad de lectura/escritura de aproximadamente 2.3 metros por segundo. En este caso las unidades de disco son diez veces más rápidas, lo que nos llevaría unos 8 minutos en realizar una copia de seguridad de un disco duro con capacidad de 40 Mbytes.

Es importante mencionar que aunque estos medios no son los mejores para hacer una copia de seguridad de la información, no esta de más mencionar que son importantes, porque pudiese pasar que como el archivo copiado esté en el mismo disco o en el fichero original del cual se copió, se pudiera dañar el disco y entonces si se perdería la información tanto de la copia como del archivo original.

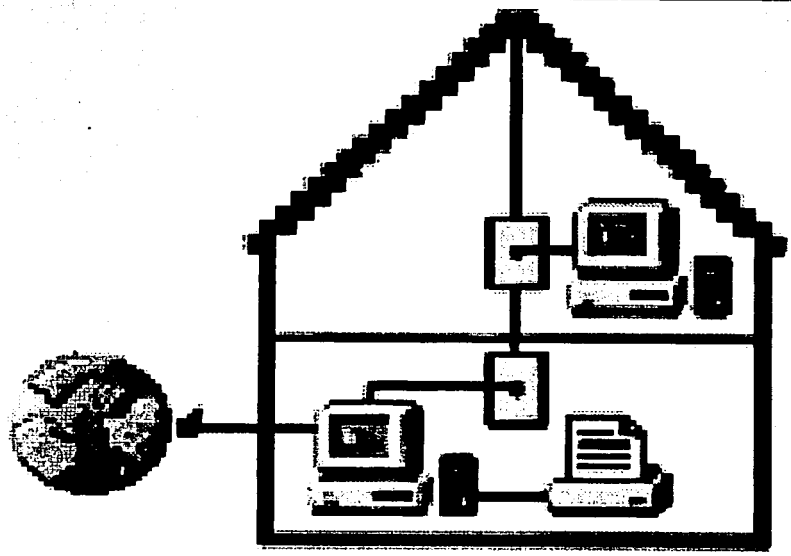
Por eso es importante recordar que estos medios de seguridad son importantes, y para una mayor seguridad, se recomienda que se tenga una *copia de seguridad de la información de suma importancia de cualquier computadora.*

Después de haber visto las diferentes formas o medios de seguridad para asegurar la información de cualquier computadora, se llega a la conclusión de que

como se mencionó anteriormente, lo ideal o correcto es hacer por lo menos una copia de seguridad de todos nuestros archivos o ficheros, pero esta seguridad debe de ser global y posteriormente, cada cierto tiempo. Con este tipo de seguridad global se asegura la integridad de los datos.

En ocasiones suele pasar que no todos los datos o la información contenida en cualquier ordenador es importante, para esto es recomendable realizar copias parciales para una mayor comodidad.

CAPITULO 4



Firewalls y su relación con la seguridad en redes LAN y WAN

4.1 Antecedentes de una firewall

Internet — Es la red global de computadoras que proporciona la base para el correo electrónico universal, WWW, y formas numerosas de comercios electrónicos — varios lo han descrito como lo fue en su aparición la computadora personal, más significativa que la prensa y tan revolucionario como el descubrimiento del fuego.

Aunque una *firewall* se diseña para controlar el flujo de la información entre dos redes, ésta apareció antes de que el mundo hubiera oído hablar del Internet. Un administrador de red debe considerar el usar de una firewall al momento de conectar dos redes. Este proceso se llama conexión de redes (internet working).

Típicamente, el término capitalizado Internet se refiere específicamente al descendiente de TCP/IP de la unión de ARPAnet's a SNET en 1982, ahora sirven diez de millones de usuarios vía servidores de Internet.

En prácticamente todos los casos, la conexión de redes debe considerar la conexión de una firewall para medir y para vigilar las conexiones de la red interna. Estas preocupaciones se hacen mayores, cuando la conexión incluye una conexión directa a Internet.

4.2 ¿Qué es una firewall?

Existen muchos conceptos acerca de lo que es una *firewall*, por lo que trataremos de mostrar diferentes definiciones que los autores de varios libros nos dan a saber.

"Una *firewall*[23] es un sistema o grupo de sistemas que establece una política de control de acceso entre dos redes".

[23] http://www.utp.ac.pa/seccion/topicos/seguridad/firewall.html

Es importante conocer algunas de las propiedades que contienen las firewalls, las cuales son:

- Todo el trafico de información de adentro hacia fuera, y viceversa debe pasar a través de ella.

- Solo el trafico autorizado, definido por la política de seguridad es autorizado para pasar por ella.

- El sistema es realmente resistente a la penetración.

Como ya se mencionó, algunas de las propiedades de las firewalls son sumamente importantes, ya que éstas protegen al servidor de ataques externos e incluso internos, permitiendo así que la información esté mucho mas segura y protegida. Sin embargo, aún así, existe el peligro de que los hackers o crackers puedan romper esa firewall o pared.

Otro autor nos da a conocer su definición acerca de lo que es una firewall o puerta cortafuego como él le llama.

Una puerta cortafuego o firewall es un software o hardware que filtra los intentos de establecimiento de conexión a partir de criterios definidos, de forma que pueda detectar e impedir el acceso al sistema a los posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre el intruso y el sistema"[24].

[24] CARBALLAR, A. José, ***El libro de las comunicaciones del PC***, México, Editorial Prentice Hall, 1997, p. 743.

Las puertas cortafuego o firewalls pueden impedir el acceso al sistema aunque se tenga una clave de acceso al sistema y un nombre de usuario válidos. Pero solamente este tipo de acceso al sistema, se emplea cuando se tengan puntos de acceso externo de una red LAN o WAN. Estos accesos externos se hacen por medio de gateways con otras redes.

Como menciona también el autor[25], las funciones de las firewalls pueden ser realizadas por:

- Máquinas exclusivamente dedicadas al filtrado de paquetes.
- Encaminadores de red (routers) configurados para esta tarea.
- Paquetes de software para distintos sistemas operativos.
- En general, cualquier dispositivo intercalado entre la red interior y exterior que soporte el filtrado de paquetes.

En general, una firewall nos permite proteger información de gran importancia, tanto para la empresa como para los que hacen uso de ella.

Por eso es importante mencionar que una firewall o cortafuego es un mecanismo de seguridad que nos permite poner una barrera de protección a la información de cualquier ataque externo. Las firewalls solamente se usan para proteger mas que nada, información en grandes cantidades que se encuentran almacenadas en servidores, permitiendo asegurar esos datos.

[25] Idem.

4.3 Tipos de firewall

Existen hoy en la actualidad, diferentes tipos de firewalls que nos permiten proteger información en grandes cantidades de posibles ataques. Es por eso, que se mencionarán los diferentes tipos de firewalls que permiten asegurar la información.

Los tipos de firewalls[26], que se describirán a continuación, son los más conocidos, aunque existe la posibilidad de que haya algunos más, solamente se tratarán los mas conocidos.

Los tipos son:

- ***Firewalls como filtros.*** El router es un tipo especial de switch, el cual realiza el trabajo de hacer las conexiones externas y convertir el protocolo IP a protocolos de WAN y LAN.

Los paquetes de datos transmitidos hacia Internet, desde un visualizador de una PC, pasarán a través de numerosos ruteadores a lo largo del camino, cada uno de los cuales toma la decisión de hacia donde dirigir el trabajo.

Los ruteadores toman sus decisiones basándose en tablas de datos y reglas, por medio de filtros, así que, por ejemplo, solo datos de una cierta dirección pueden pasar a través del ruteador, esto transforma un ruteador que puede filtrar paquetes en un dispositivo de control de acceso o firewall. Si el ruteador puede generar un registro de accesos esto lo convierte en valioso dispositivo de seguridad.

[26] http://www.utp.ac.pa/seccion/topicos/seguridad/seguridad.html

Si el servidor de Internet solicita información, o bien la suministra hacia sistemas de bases de datos distribuidas, entonces esta conexión entre el servidor y la estación de trabajo debería ser protegida.

- ***Firewall como gateway.*** Las firewalls son comúnmente referidas como gateways, que controlan el acceso a la información desde afuera hacia adentro y viceversa.

Una gateway es una computadora que proporciona servicio de intercambio de datos entre dos redes. Una firewall puede consistir en un poco mas que un ruteador filtrador, como una gateway controlada. El trafico va hacia la gateway, en vez de dirigirse directamente hacia la red. La gateway pasa los datos, a través de un filtro, hacia otra red o hacia otra gateway conectada a otra red.

Esta medición toma en una cuenta, direcciones de fuente y destino, tipos de paquetes de datos, política de seguridad. Típicamente una firewall registra los accesos y los intentos de acceso de una red a otra.

- ***Firewalls como puntos de atrapado.*** Algunas firewalls proveen servicios de seguridad adicionales, como encriptación y desencriptación. Ambas deben usar sistemas compatibles de encriptación. Existen varios fabricantes que ofrecen dichos sistemas. Encriptación de firewall a firewall es la forma que se usa en el Internet de hoy.

Verificar la autenticidad del usuario así como el sistema que este usando, también es importante, y las firewalls pueden hacerlo usando tarjetas inteligentes, fichas y otros métodos.

Las firewalls, pueden incluso proteger otras redes exteriores. Una compañía puede aplicar las mismas restricciones de trafico, mejorado con autenticación.

- ***Firewalls internas.*** Alguien fuera de la empresa podría solicitar cierta información, pero no necesariamente necesita accesar a toda la información interna. En estas circunstancias, las firewalls juegan un importante papel forzando políticas de control de acceso entre redes confiables protegidas y redes que no son confiables.

En una WAN que debe ofrecer conexión de cualquier persona a otra, otras formas en el nivel de aplicación pueden ser implementadas para proteger datos importantes.

Sin embargo, separar las redes por medio de firewalls reduce significativamente los riesgos del ataque de un hacker desde adentro, esto es, acceso no autorizado por usuarios autorizados.

Agregando encriptación a los servicios de la firewall la convierte en una conexión firewall a firewall muy segura. Esto siempre permite tener redes grandes interconectadas por medio de Internet.

Agregando autenticación se puede aumentar el nivel de seguridad. Por ejemplo, un vendedor que necesite ver la base de datos de inventario, tendrá que comprobar que es él.

- ***Firewalls con filtrado de paquetes.*** Todos las firewalls desempeñan algún tipo de filtrado de paquete IP, comúnmente por medio de un ruteador de filtrado de paquetes. El ruteador filtra paquetes, haciendo que ellos pasan por el ruteador, implementando un conjunto de reglas con base en la política de la firewall.

El filtrado puede bloquear conexiones desde o a las redes específicas, y pueden bloquear conexiones a puertos específicos. Un sitio podría desear bloquear las

conexiones desde ciertas direcciones, tales como desde anfitriones o los sitios consideraron hostiles o indignos de confianza.

Desafortunadamente, los ruteadores de filtrado de paquetes, son difíciles de usar en su configuración y su mantenimiento por lo complejos que son.

- ***Firewalls con inspección de paquetes.*** Algunas firewalls de Internet combinan el filtrado de paquetes y el enfoque de aplicaciones gateway, usando un filtrado de paquetes o un ruteador de hardware para controlar los niveles bajos de comunicación, y gateway para habilitar aplicaciones. Esto puede crear un alto grado de control de acceso.

Otro punto de vista que gana aceptación, es la inspección de paquetes que no solo filtra, esto es, considerar su contenido tanto como sus direcciones.

Las firewall de este tipo emplean una inspección de módulos, aplicable a todos los protocolos que comprenden los datos de los paquetes destinados desde el nivel de red (IP) hasta el nivel de aplicación.

Por ejemplo, las aplicaciones gateway solo acceden a los datos del nivel de aplicación, los ruteadores tienen acceso solo a niveles bajos, el enfoque de la inspección de paquetes integra toda la información reunida de todos los niveles en un simple punto.

- ***Firewalls híbridas.*** En la práctica, muchos de los firewalls comerciales de hoy usan una combinación de estas técnicas. Por ejemplo, un producto que se originó como una firewall filtradora de paquetes puede haber sido mejorado

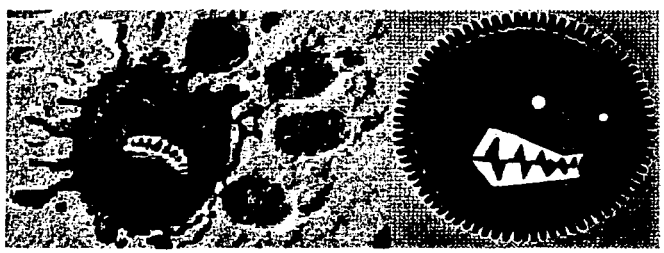
con filtrado inteligente a nivel de aplicación. Las aplicaciones proxy[27] en áreas establecida como FTP[28] puede agregar una inspección de filtrado base en su esquema.

Nota: Recuerde, agregando los métodos o técnicas de seguridad, no significa necesariamente un aumento en la seguridad. Los mecanismos adicionales pueden aumentar, disminuir, o dejar infectado la postura de seguridad del firewall.

4.4 ¿Qué es un virus informático?

Un *virus informático* es un programa que se introduce en cualquier computadora de diferentes formas, ya sea por medio de un disco flexible o por correo electrónico, que es capaz de infectar todos los archivos que se encuentran dentro del disco duro de la computadora.

Figura 22. Virus informático



Fuente: http:// www.sinvirus..com/losvirus.shtml

Este tipo de programas, en los cuales están hechos los virus, pueden resultar dañinos a cualquier parte del sistema operativo y producir efectos no deseados en cualquier PC.

[27] Es un servidor que se conoce como "puerta de comunicación", que nos permite ver el tráfico de información entre una red protegida e Internet.
[28] Protocolo de transferencia de archivos.

Una vez que el virus se ha introducido en cualquier PC, puede estar escondido o almacenado en lugares donde el usuario al encender la computadora, por accidente puede activar al virus sin darse cuenta.

Hasta que no se ejecuta el programa infectado o se cumple una determinada condición (una fecha concreta, una acción que realiza el usuario,...), el virus no actúa. Incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución.

Entre los efectos destructivos que puede realizar un virus podemos destacar los siguientes: dañar o borrar los datos almacenados en un ordenador, provocar el bloqueo del equipo afectado, mostrar mensajes en pantalla, etc.

Una característica típica de los virus es su capacidad de duplicarse y propagarse a otros ficheros o programas.

4.5 Tipos de virus

Existen varios tipos de virus informáticos[29] que se pueden clasificar de acuerdo al tipo de función que realicen. Los tipos son los siguientes:

- ***Virus residentes***. Estos virus, se colocan automáticamente en la memoria de la computadora y, desde ella esperan la ejecución de algún programa o la utilización de algún archivo.

Son aquellos que se colocan, o ubican, automáticamente en zonas determinadas de la memoria RAM de un ordenador, cuando son ejecutados, o cuando se enciende y arranca el ordenador.

[29] http://www.sinvirus.com/tipos.shtml

Desde ella esperan la ejecución o manipulación (apertura, cierre, copiado, etc.) de algún fichero, para infectarlo.

- ***Virus de acción directa.*** Los virus que se pueden englobar en este grupo, realizan copias de sí mismos en el ordenador que infectan. Se caracterizan por realizar automáticamente copias de si mismos dentro de un mismo ordenador infectado, en diferentes ubicaciones (directorios o carpetas de ese ordenador). El objetivo primordial de los mismos es reproducirse y multiplicarse.

- ***Virus de sobreescritura:*** Sobreescriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos. Cuando infectan un archivo, la información que éste contiene, no es respetada. Es decir, el contenido del archivo infectado se pierde total o parcialmente.

- ***Virus de boot.*** Atacan a los disquetes y discos duros, haciendo imposible su utilización. Todos los discos (disquetes y discos duros) tienen una sección muy importante, denominada *sector de arranque.*

El sector de arranque, es el sector principal o cero donde se almacena la información acerca de las características del disco, además de poder albergar un programa con el que es posible arrancar el ordenador, mediante la utilización de ese disco.

Aunque tanto para los disquetes como para los discos duros se habla de sector de arranque, éstos son diferentes y se denominan de forma diferente:

- *BOOT*. Hace referencia al sector de arranque de un disquete.
- MBR[30]. Hace referencia al sector de arranque de un disco duro.

En ambos casos, dicho sector de arranque, corresponde al primer sector del disco y ocupa un tamaño de 512 Bytes. Estas "zonas especiales" de los discos, son el objetivo de los virus denominados de Boot y también pueden ser el objetivo de otros tipos de virus.

- ***Virus de macro.*** Este tipo de virus no infectan cualquier tipo de archivo, sino los que se han creado con determinados programas como por ejemplo documentos de Microsoft Word, bases de datos de Microsoft Access, hojas de calculo de Microsoft Excel, presentaciones con Microsoft Powerpoint, etc. Cada uno de estos tipos de archivos puede tener adicionalmente unos pequeños programas, denominados macros. Una macro no es más que un micro-programa que el usuario asocia e incluye en el archivo que ha creado.

Estas macros[31] (al ser realmente programas) pueden ser infectadas. Al abrir un archivo que las contenga, éstas se cargarán de forma automática, en ese instante o posteriormente, el virus actuará realizando cualquier tipo de operación perjudicial.

Dentro de los virus de macro, existen varios tipos dependiendo las aplicaciones o los programas a los que afectan:

- Virus de Macro para Microsoft Word.
- Virus de Macro para Microsoft Excel.
- Virus de Macro para Microsoft Power Point.

[30] Master Boot Record (Registro del sector de arranque maestro).
[31] Una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) las realice de forma automática y secuencial.

- ***Virus de enlace o directorio.*** Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes. El resultado es que posteriormente será imposible localizarlos y trabajar con ellos.

4.6 Antivirus

Son todos aquellos programas que permiten analizar memoria, unidades de disco y otros elementos de un ordenador en busca de virus. Una vez que el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.

Es importante que en cualquier antivirus, se consideren ciertos puntos para poder tener una buena herramienta para combatir a los virus. Los puntos son:

- Detectar y eliminar gran cantidad de virus como sea posible.

- La velocidad del programa antivirus, debe ser demasiado rápida.

- Capacidad de reconstrucción. Debe poder reconstruir todas las modificaciones realizadas por determinados virus en la configuración del sistema.

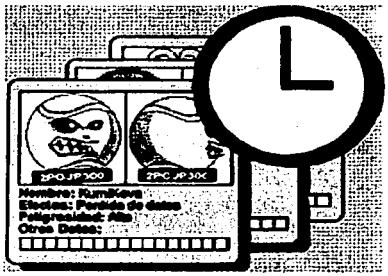
- Protección permanente (residente). Debe contar con una análisis continuo (en tiempo real) sobre todos los elementos con los que se trabaja y que llegan a través de Internet.

- Capacidad de actualización. Debe poder actualizar tanto el programa completo, como el archivo que permite la identificación de todos los virus que van apareciendo a diario (Archivo de identificadores de virus[32]).

Por lo tanto, un buen programa antivirus debe contar con dos tipos de actualizaciones, las cuales son:

- *Update (Archivo de identificadores de virus)*. Actualiza exclusivamente el Archivo de identificadores de virus (consigue que el antivirus detecte todos los virus surgidos hasta esa fecha).

Figura 24. Archivo identificador de virus.



Fuente:http://www.sinvirus.com/detecciones.shtml

- *Upgrade (Actualización completa)*. Actualiza el programa antivirus completo, tanto el Archivo de identificadores de virus, como las nuevas mejoras incluidas en el propio antivirus.

[32] Es un archivo que forma parte de un programa antivirus y contiene cada una de las características o firmas de todos los virus que éste detecta.

Pero, para que un programa antivirus realice una búsqueda o detecte cualquier virus en la computadora, se utilizan medidas de búsqueda y detección[33] más avanzadas, como son:

- ***Búsqueda de cadenas.*** Se buscan determinadas cadenas de texto las cuales identifican a cada uno de los virus.

Cada uno de los virus contiene en su interior determinadas cadenas de caracteres que le identifican. Los programas antivirus incorporan un fichero denominado "fichero de firmas de virus" en el que guardan todas estas cadenas, para hacer posible la detección de cualquiera de ellos.

Por lo tanto, para detectar un virus, se analizan los ficheros comprobando si alguno de ellos contiene alguna de las cadenas comentadas. Si el fichero analizado no contiene ninguna de ellas, se considera limpio. Si el programa antivirus detecta alguna de esas cadenas en el fichero, indica la posibilidad de que éste se encuentre infectado. En tal caso, se producirá la desinfección.

- ***Excepciones.*** El programa antivirus realiza la búsqueda de un virus en concreto.

Una alternativa en lo que se refiere a la detección de virus, es la búsqueda de excepciones. Cuando un virus utiliza una cadena para realizar una infección, pero en posteriores infecciones emplea otras distintas, es difícil detectarlo.

En ese caso lo que el programa antivirus consigue es realizar directamente la búsqueda de un virus en concreto.

[33] http://www.pandasoftware.es/enciclopedia.asp?page=Glosary

- ***Análisis Heuristico.*** Permite detectar nuevos virus de los que no se conocen sus cadenas.

Cuando no existe información para detectar un posible nuevo virus (que aun no se conoce), se utiliza esta técnica. Con ella se analizan los archivos, obteniendo determinada información (tamaño, fecha y hora de creación, posibilidad de colocarse en memoria, etc.).

Esta información es contrastada por el programa antivirus con las informaciones que se hayan podido recoger en ocasiones anteriores acerca de cada uno de los ficheros objeto del análisis. El antivirus será quien decida si puede tratarse de una infección vírica, o no.

- ***Protección permanente.*** Mientras el ordenador se encuentra encendido, el programa antivirus analiza cada uno de los archivos con los que se trabaja, en busca de posibles infecciones.

La protección permanente vigila constantemente todas aquellas operaciones realizadas en el ordenador que sean susceptibles de permitir una infección por un virus.

Si se tiene activada una buena protección, el riesgo de contagio es mínimo, y se facilita enormemente el trabajo con el ordenador, ya que no hay que estar pendiente de analizar todo lo que se recibe: la protección permanente se encarga de ello automáticamente.

- ***Vacunación.*** El antivirus puede detectar los cambios existentes en el archivo que analiza, desde la última vez que lo analizó.

El programa antivirus almacena información sobre cada uno de los archivos. Si se detecta algún cambio entre la información guardada y la información actual, el antivirus avisa de lo ocurrido.

Existen dos tipos de vacunaciones, las cuales son:

- *Interna.* La información se guarda dentro del propio archivo analizado. Al ejecutarse, él mismo comprueba si ha sufrido algún cambio.

- *Externa.* La información que guarda en un archivo especial y desde él se contrasta la información.

Por esta razón, es muy importante contar con un antivirus actualizado, que detecte y elimine todos los virus y cada uno de los que surgen a diario.

4.7 Hackers

Con el advenimiento de la **era de la computación,** han surgido diversas definiciones que se emplean para designar a personas o grupos de ellas que se dedican a actividades ilícitas.

Con el paso del tiempo, es importante mencionar que empresas trasnacionales que se dedican a hacer software, adoptaron el nombre de *hacker* para calificar a personas que se dedican a realizar actos ilícitos como robo de información u otro acto que esté penalizado contra la ley, seguridad en las redes, autores de virus, intrusos de servidores, interceptadores de mensaje de correo, vándalos del ciberespacio, etc.

Sin embargo, existen muchas definiciones acerca de lo que es un hacker, las cuales se definirán a continuación:

- Un ***hacker*** es toda aquella persona que se dedica a realizar tareas de investigación o desarrollo realizando esfuerzos más allá de los normales, anteponiéndose un apasionamiento por la computación[34].

- Un ***hacker*** es un término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, las redes, los problemas de seguridad, etc[35].

- Un ***hacker*** es una persona que disfruta aprendiendo los detalles de los sistemas de programación y cómo extender sus capacidades, tan intensamente como, al contrario, muchos usuarios prefieren aprender sólo el mínimo necesario[36].

- Un ***hacker*** es toda aquella persona que disfruta investigando los detalles de los sistemas operativos y programas, buscando nuevas formas de optimizar o aumentar sus capacidades[37].

Sin embargo, existen dos tipos de hackers, y son:

- Los buenos, que son aquellos que usan sus conocimientos para divertirse sin hacer daño a los demás.

[34] http://www.perantivirus.com/sosvirus/hackers/index.htm
[35] http://www.geocities.com/especial_de_jamon/mayo.htm
[36] Idem
[37] http://sites.netscape.net/lizbethloza/acercadeloshackers

- Y los malos, que son los que abusan de sus conocimientos para perjudicar y dañar archivos o la información que se tiene en las computadoras.

Terminar de aclarar que los Hackers no escriben dañinos virus de computadora, no quiere decir que tampoco son delincuentes comunes, cuya hambre de riquezas les obligan a aprender computación.

En definitiva, son genios informáticos que pueden usar su talento y preparación para el bien o para el mal.

4.8 Crackers

Los *crackers* también están muy de moda en la era de la computación, pero ¿realmente sabemos que son?. Existen varias definiciones que daremos a continuación acerca de lo que son.

- Un ***cracker*** es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obsesionado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo[38].

Este tipo de cracker moderno usa programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web, tales como rutinas desbloqueadoras de claves de acceso o generadores de números, para que en forma aleatoria y ejecutados automáticamente puedan lograr vulnerar claves de accesos de los sistemas.

[38] http://www.delitosinformaticos.com/seguridad

- Un ***cracker*** es aquella persona maliciosa que trata de obtener o descubrir información confidencial y usarla con motivos no honestos. Es la persona que rompe la seguridad de un sistema[39].

- Un ***cracker*** es una persona que ingresa ilegalmente en un sistema informático para robar, destruir o simplemente causar desorden con la información existente en el sistema[40].

Obviamente que antes que llegar a ser un cracker, se debe ser un buen hacker.

4.9 Campo de aplicación

Es importante saber el campo de aplicación que tiene o que abarca una firewall. El campo de aplicación nos permite saber que tan grande puede ser la protección que nos brinda una firewall.

Primeramente, una firewall como se mencionó anteriormente, nos permite proteger nuestra información que se encuentra dentro de la computadora de cualquier ataque externo o interno.

El campo de aplicación, prácticamente se puede dar redes WAN, pero también en redes LAN, de acuerdo al tipo de protocolos que utilicen los dos tipos de redes, y al servidor.

En el servidor, se debe tener un software que permita detectar cualquier ataque que se quiera tener al servidor y a la información contenida en él. Es por eso, que se debe estar muy alerta a cualquier tipo de ataque a éste.

[39] http://www.geocities.com/especial_de_jamon/mayo.htm
[40] http://sites.netscape.net/lizbethloza/acercadeloshackers

En general, el campo de aplicación, se utiliza solamente para servidores que estén conectados a Internet o que tengan ese servicio, porque son los que están expuestos a un peligro de ser atacados por un intruso.

4.10 Relación con la seguridad

Las firewalls relacionadas con la seguridad informática, es un punto importante porque nos permitirá saber que tan relacionadas están las firewalls con ella.

Por principio de cuentas, cuando nacen los primeros sistemas informáticos que emplean la interconexión de computadoras en red, era poco imaginable el potencial de peligro que esto implicaba.

Al comenzar a interconectarse redes entre sí, se inició la era de la seguridad pero inicialmente a través de contraseñas para el acceso a los recursos de los equipos que físicamente podían ser alcanzados.

El detonante de la seguridad es sin duda Internet, a través de la cual, millones de personas se encuentran analizando día a día mejores técnicas para descubrir y aprovechar las vulnerabilidades de los sistemas que pueden alcanzarse en esta red mundial[41].

Los sistemas informáticos actuales, al aparecer Internet, comienzan a ser blanco de ataques. La primer herramienta defensiva que sale al mercado es esta muralla llamada, **"Firewall"**.

Hoy en día ya existen metodologías mucho más eficientes para proteger la información que se encuentra en cualquier computadora, se tratan de, sistemas de

[41] http://www.fundaciondike.org/seguridad/sobrecortafuegos.html

detección de intrusos, sistemas de monitoreo de tráfico con sus correspondientes alarmas, Honey pots (también llamadas zonas o servidores de sacrificio), listas de control de acceso, el viejo Proxy que sigue en vigencia, etc.

Pero, ¿cómo se verá el futuro de nuestras computadoras que se encuentran conectadas en red, si la información no está protegida y asegurada?.

- Primeramente, sin una firewall, la información contenida en un servidor con servicio de Internet, puede ser accesada por cualquier intruso.

- Con un análisis de contenido (es decir, saber que información es muy importante, para que la demás, se elimine) en los mismos servidores, permitirá, en definitiva, se deban realizar las operaciones de fragmentación y reensamble y el posible análisis del mal empleo de Unicode (passwords).

- Con muy buenas listas de control de acceso en Proxy, access servers y routers, pero con mucho conocimiento de protocolos de comunicaciones, los administradores deberán checar que usuarios, en caso de que se esté trabajando en red, son los que accesan a la información almacenada en el servidor.

- Con muy buenos sistemas de alarmas ajustados a cada organización y zona en particular, nos deben permitir la detección temprana de todo intruso que se haga presente, pues se debe tener la certeza que estos accesos tarde o temprano sucederán.

- Planificando la seguridad de los sistemas, cualquier intruso que intente accesar a la información del servidor, se determinarán las causas que produjeron esa intrusión.

Empleando estrategias de seguridad en las redes informáticas y empleando firewalls para proteger la información que se encuentra en cualquier computadora, se asegura el futuro de la computación y de la empresa a la cual se le tenga que proteger su información.

CONCLUSIÓN

Mediante este estudio se corroboró que realmente las redes del tipo LAN y WAN se pueden proteger con técnicas que permiten asegurar y resguardar la información de la empresa y de cualquier ordenador. He aquí el logro del objetivo fijado, ya que a través de los temas tratados se ha determinado y comprendido la importancia que tienen las redes en el campo de la informática y su seguridad.

Este trabajo de investigación ha brindado los conocimientos necesarios con respecto a las diversas técnicas que existen para proteger la información de una empresa (o de cualquier usuario). Aquí cabe mencionar que dependiendo el tipo de información se utilizará una determinada técnica, y esto es muy importante que lo tome en cuenta el usuario.

Sin embargo, en el caso de una red grande, por ejemplo Internet, se concluye que la técnica de firewall es la más recomendable, ya que no permite accesar a los datos de un servidor y debe tenerse una clave de acceso para hacer uso de la información.

Otra de las técnicas que considero de mejor utilidad es la firma digital, ya que permite, a través de una clave privada, accesar a la información que se tiene en forma personal.

En resumen, se puede concluir que este estudio ha brindado las herramientas necesarias para que el usuario pueda decidir qué tipo de técnica utilizar para proteger su información.

BIBLIOGRAFIA

BLACK, Uyless., ***Redes de Computadoras, Protocolos, Normas e Interfaces,*** 2ª ed., México, Editorial Computec Ra-Ma, 1997, 586 p.

CARBALLAR, José A., ***El libro de las comunicaciones del PC. Técnica, Programación y aplicaciones,*** 2ª ed., México, Editorial Computer Ra-Ma, 1997, 530 p.

CHORAFAS N, Dimitris., ***Beyond LAN'S. Client / Server Computing,*** 2ª ed., E.U.A, Editorial Mc Graw Hill,1997, 420 p.

COMER E, Douglas., ***Redes de Computadoras, Internet e Interredes,*** 2ª ed., México, Editorial Prentice Hall Hispanoamericana, S.A., 1997, 506 p.

CORTES FERREIRA, Gonzálo., ***World Wide Web ¡Espectacular!,*** 2ª ed., México, Editorial Computec, 1997, 434 p.

HALSALL, Fred, ***Comunicación de datos, redes de computadoras y sistemas abiertos,*** 4ª ed., México, Editorial Addison Wesley Longman, 1998, 955 p.

HAYDEN, Matt., ***Aprendiendo Redes en 24 hrs,*** 2ª ed., México, Editorial Prentice Hall Hispanoamericana, S. A, 1999, 428 p.

RODAO DE MARCELO, Jesús., ***Guía de campo de los virus informáticos,*** 2ª ed., México, Editorial Computec Ra-Ma, 1997, 363 p.

SANDERS H, Donald., ***Informática, Presente y Futuro,*** 3ª ed., México, Editorial Mc Graw Hill, 1995, 887 p.

TANENBAUM S, Andrew., ***Redes de computadoras,*** 3ª ed., México, Editorial Prentice Hall, 1997, 813 p.

UREÑA A, Luis; Antonio M. Sánchez; María T. Martín, y Mantas M. José, ***Fundamentos de Informática,*** 2ª ed., México, Editorial Alfa Omega Ra-Ma, 1998, 308 p.

OTRAS FUENTES:

http://www.iec.csic.es/criptonomicon/seguridad/
http:// www.iec.csic.es/criptonomicon/seguridad/amenazas.html
http://www.iec.csic.es/criptonomicon/seguridad/servicio.html
http://www.nueva-propuesta.com/nueva/desarrollo/seguridad-informatica/html
http://www.nueva-propuesta.com/nueva/consultoria/redes/redes.htm
http://www.securityfiles.es/index01.htm
http://www.ctv.es/users/mpq/estrado/estrado004.html
http://www.sistema.itesm.mx/va/graduados/plan98/Sinteticos/sin-cs.html
http://www.pvc.cl/curso_dist/cbc/textos/tgeneral/diccion.html
http://www.ssh.fi/tech/crypto/introhtml
http://www.w3.org/Security/Overview.html
http://www.mat.upc.es/~soriano/crypto.htm
http://www.delitosinformaticos.com/seguridad/subastas.html
http://www.bit.es/cursos/seguridad.htm
http://www.iec.csic.es/criptonomicon/acceso/
http://www.iec.csic.es/criptonomicon/acceso/localizacion.html
http://www.iec.csic.es/criptonomicon/seguridad/mecanism.html
http://www.iec.csic.es/criptonomicon/correo/cifrado.html
http://www.iec.csic.es/criptonomicon/images/simetrico.gif
http://www.iec.csic.es/criptonomicon/images/asimetrico.gif
http://www.iec.csic.es/criptonomicon/acceso/nombres.html
http://www.iec.csic.es/criptonomicon/correo/firma.html
http://www.iec.csic.es/criptonomicon/images/firma.gif
http://www.e-gallaecia.com/2der.htm
http://www.pki.gov.ar/
http://www.pki.gov.ar/fd-def.html
http://www.virusprot.com/Amzsolup.html
http://www.iec.csic.es/criptonomicon/correo/recursoscorreo.html
http://www.ugr.es/~aquiran/cripto/pgp01.htm
http://www.ugr.es/~aquiran/cripto/pgp02.htm
http://www.ugr.es/~aquiran/cripto/pgp03.htm
http://www.geocities.com/SiliconValley/Pines/2332/index.html
http://www.geocities.com/SiliconValley/Pines/2332/descrip.htm
http://www.geocities.com/SiliconValley/Pines/2332/gestion.htm
http://www.fundaciondike.org/seguridad/sobrecortafuegos.html
http://www.fundaciondike.org/seguridad/muertefirewalls.htm
http://www.sinvirus.com/default.shtml
http://www.sinvirus.com/infovirus.shtml
http://www.sinvirus.com/losvirus.shtml
http://www.sinvirus.com/tipos.shtml
http://www.sinvirus.com/tecnicas.shtml
http://www.sinvirus.com/detecciones.shtml
http://www.sinvirus.com/acciones.shtml
http://www.sinvirus.com/entrada.shtml

http://www.sinvirus.com/proceso.shtml
http://www.sinvirus.com/elementos.shtml
http://www.sinvirus.com/virus_historicos.shtml
http://www.geocities.com/especial_de_jamon/mayo.html
http://perantivirus.com/susvirus/hackers/index.htm
http://www.delitosinformaticos.com/seguridad
http://www.pandasoftware.es/
http://www.pandasoftware.es/enciclopedia.asp?page=Glosary
http://sites.netscape.net/lizbethloza/acercadeloshackers
http://www.utp.ac.pa/seccion/topicos/seguridad/seguridad.html
http://www.utp.ac.pa/seccion/topicos/seguridad/firewall.html