UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍAS

TESIS

PROPUESTA DE PROCEDIMIENTO PARA MANTENIMIENTO DE REDES TIPO LAN

Para obtener el título de:
Ingeniero en Electrónica y Telecomunicaciones

Presenta: Baruc Corona Zúñiga

Asesor: L.S.C. Alfonso Ávila Pérez Tagle

Pachuca de Soto, Hidalgo. 01 de Agosto de 2009.

ÍNDICE

OBJETIVO GENERAL

Alcanzar la seguridad en redes para que con un monitoreo constante y revisión de todas las personas que la utilizan, así como sus programas y documentos se puede vigilar. Ofreciendo aquí el conocimiento para aprender o conocer un poco más y de manera segura y confiable acerca de las computadoras y sus configuraciones para poder conectarse en cualquier equipo o red, ya que existen programas o agentes maliciosos que pueden dañar la computadora.

OBJETIVOS PARTICULARES

-Identificar los factores clave dentro de la seguridad en una red LAN, escanear, evaluar dicha red y así mismo canalizar, destruir y rectificar esos agentes que pueden dañar el sistema y por consiguiente toda la red.

-Concientizar a cada uno de los miembros de la organización para que mantengan confidencial la información de la empresa, ya que esto es lo más importante de la seguridad en redes, pues no solo los virus pueden destrozar una computadora o red entera, sino también las personas mismas al deformar o destruir algún documento o información contribuye a la vulnerabilidad del sistema en general, provocando un caos en todas la computadoras o red.

INTRODUCCION

En todas las redes de computadoras siempre es necesario tener disponibilidad y accesibilidad a diferentes documentos o información importante, pero sobre todo tener un adecuado control, además de tener una buena observación sobre cualquier computadora que esté conectada en nuestra red, por ello es indispensable conocer el funcionamiento de las maquinas.

Se debe de conocer como fue evolucionando la tecnología desde la imprenta, hasta lo que hay en nuestra actualidad como lo son las computadoras, por ejemplo el teléfono es el mayor y mejor invento que ha realizado el hombre ya que se convirtió en un servicio universal y sobre todo accesible.

Todo esto derivo en que todo ser humano quería muchísima más comunicación en todo el planeta, de ahí que surgiera la computadora pues en la actualidad nos ofrece el internet, que es el servicio más indispensable y usado del mundo, por nos podemos comunicar y a la vez estar viendo en vivo y directo a la otra persona.

Claro para ello debemos conocer cómo funciona internet, que pasos o protocolos debemos seguir para así poder conectarnos en una red, claro también es necesario ver de qué manera podemos conectarnos tanto física como lógica, lo que en este caso sería el software y hardware, tanto el cableado o si es de manera inalámbrica y ya de ese modo ver si esa es red es disponible pero por encima de todo segura y confiable.

Para todo esto como se menciona la seguridad es importante, ya que existen diferentes programas y sobre todo agentes maliciosos que solo se dedican a dañar nuestro sistema o red de computadoras, pero todo esto ya lo veremos a continuación.


Seguridad en Redes

1. CONCEPTO DE SEGURIDAD EN LAS REDES

La definición y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado, En la Fig. 1.1 muestra de manera global las amenazas que existen en la seguridad en redes.

Fig. 1.1 Amenazas en la seguridad.

1.2. TIPOS DE SEGURIDAD

Podemos clasificar a la seguridad en redes en dos tipos, y de ellos se subdividen en la siguiente tabla.

1. SEGURIDAD FÍSICA	2.SEGURIDAD LÓGICA
Desastres	Controles de acceso
Incendios	Identificación
Equipamiento	Roles
Inundaciones	Transacciones
Picos y ruidos electromagnéticos	Limitación a los servicios
Cableado	Control de acceso interno

1.2.1 SEGURIDAD FÍSICA.

La seguridad física es la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial".

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de computo así como los medios de acceso remoto del mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Es muy importante, que por más que nuestra organización sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

1.2.2 SEGURIDAD LÓGICA

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. Después de ver como nuestra red puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un sitio de cómputo, no será sobre los medios físicos, sino, contra información por él almacenada y procesada.

Así, la seguridad física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la seguridad lógica.

Los objetivos que se plantean para la seguridad lógica son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.3 VULNERABILIDAD EN REDES.

Una vulnerabilidad es toda condición que permite un atentado a la seguridad dentro de las redes.
Existen diferentes formas en las que se puede encontrar vulnerabilidades tanto en Hardware como software.

1.3.1 VULNERABILIDADES EN LOS NAVEGADORES.

Generalmente las fallas de los navegadores, no se dan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”.

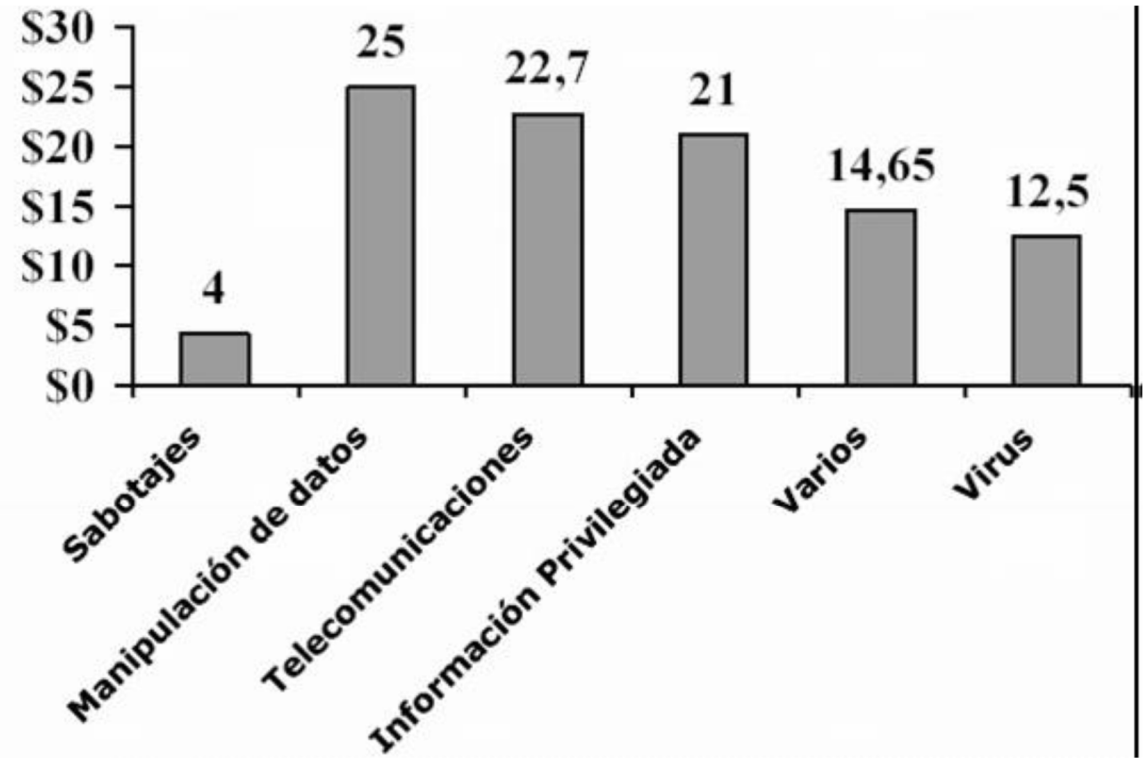
Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por ejemplo, cuando el usuario escribe una dirección en formato URL, ésta se guarda en un buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones. El protocolo usado puede ser http, pero también otro menos conocidos, internos de cada explorador, como el “res:” o el “mk:”. Precisamente existen fallos de seguridad del tipo “Buffer Overflow” en la implementación de estos dos protocolos.

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries relativo a los archivos “.lnk” y “url” de windows 95 y NT respectivamente. Algunas versiones de Microsoft Internet Explorer podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima.

1.4 RIESGOS EN LA INFORMACIÓN.

Estos riesgos provocan acciones hostiles como el robo, fraude y sabotaje de información.

En la sig. Figura aparece un desglose de las pérdidas que obtienen las organizaciones anualmente.



Pérdidas monetarias de las organizaciones.

1.4.1 ROBO.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o

para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan mejor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

1.4.2 FRAUDE.

Cada año, millones de dólares son sustraídos de empresas y en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines. Sin embargo, ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da publicidad a este tipo de situaciones.

1.4.3 SABOTAJE.

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada, la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado.

Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

HISTORIA DE LA COMUNICACIÓN

2. BREVE HISTORIA

Recordemos que anteriormente el problema que se presentaba en las llamadas de larga distancia consistía en la perdida de la calidad del sonido; este viejo problema fue solucionado en los años 60 al digitalizar la voz. Gracias a esto la calidad de la voz no sufre deterioro y una llamada de larga distancia tenía la misma calidad que una llamada local. Después en los 70 se presentó el reto por parte de las grandes empresas de interconectarse a través de sus computadoras, esta necesidad dio lugar a las primeras redes de transmisión de datos.

En la asamblea general de a CCITT hoy ITU del año 1984 se tomó la decisión de reconvertir la antigua línea analógica en una línea digital y así poder convertir la red telefónica mundial en una red global de transmisión de datos y ofrecer otros servicios además de voz.
No era posible construir una red totalmente nueva, así que se debía crear a partir de la red analógica existente. En su primera fase se debían reemplazar las antiguas centrales por centrales computarizadas. Durante esta fase se mezclan enlaces analógicos con digitales, al concluir esta fase en que el único enlace analógico era entre el abonado y la central, la red digital integrada (RDI) estaba lista.

La siguiente fase era ampliar el enlace digital de extremo a extremo es decir, una comunicación enteramente digital de abonado ha abonado y así nace la RDSI. Esta fue una breve historia de la RDSI, pero es prudente y necesario ir más allá de una simple historia de RDSI y debemos remontarnos a la historia de la comunicación, la telefonía y las redes; y así podamos conocer y ampliar el panorama de la necesidad y la importancia del nacimiento de la RDSI.

2.1. HISTORIA DE LA COMUNICACION.

El ser humano siempre ha tenido la necesidad de comunicarse y esto lo ha orillado a buscar diferentes formas de comunicación como son el lenguaje y la escritura. El primer medio masivo de comunicación fue la imprenta, inventada por el alemán Johann Gutenberg (1387-1468) seguido de este gran invento surgieron: el telégrafo, el teléfono, la radio, la televisión, hasta los conocidos actualmente, los cuales facilitan la comunicación entre la gente. Las raíces etimológicas de la palabra comunicación, son las siguientes: *comunis* que significa, lo que pertenece a varios; *ica,* que es un sufijo de relación u origen; y *ción*, que es una terminación que denota una acción. Comunicación = acción y efecto de comunicar o comunicarse.

Notablemente sobre lo que es nuestro estudio, nos podemos dar cuenta que los inventos más sobresalientes para la RDSI, fue el teléfono, las computadoras, entre otros, que hacen posible las redes de datos. Algunos inventores famosos que hicieron posible la comunicación son:

Algunos inventos importantes para la RDSI.	
Johann Gutenberg (1387-1468)	Imprenta
Samuel Finley B. Morse (1791-1872)	Telégrafo eléctrico
Tomas Alba Edison (1847-1931)	Lámpara incandescente, Fonógrafo Perfeccionamiento del telégrafo
Alexander Graham Bell (1847-1922)	Precursor del teléfono, radiófono, etc.
Heinrich Hertz (1857-1894)	Propiedades de ondas electromagnéticas.
Guglielmo Marconi (1874-1937)	Radio
Intelsat (1965)	Nace la comunicación por satélite

Existen más personajes que realizaron experimentos en comunicación o mejoraron los dispositivos. Torres Quevedo realizó experimentos de transmisiones de imágenes

a distancia, dichos experimentos son los predecesores de la telefotografía y de la televisión. Jonh L. Baird realizó una transmisión primaria de la cara humana a través de luces y sombras; E.F.W. Alexanderson en 1928 logró transmitir rostros humanos a distancia. El mexicano Guillermo González Camarena sofisticó la televisión blanco y negro a televisión a color. Estos personajes han contribuido en el progreso de las comunicaciones, a tal punto en que cualquier suceso de interés puede ser escuchado y visto en cualquier parte del mundo en el justo momento en que acontece.

En 1878. Dos años después de la invención del teléfono, Alexander Graham Bell estableció dicha idea claramente: "*Creo que en el futuro los cables unirán las centrales principales de las compañías telefónicas de diferentes ciudades. De este modo un hombre en cualquier lugar del país podrá comunicarse mediante la palabra hablada con cualquier otra parte*".

Desde el mismo año de su invención, el uso del teléfono aumentó rápidamente, solo dos años después de la primera comunicación, realizada en 1878 en New Haven, Connecticut, la mayor parte de las ciudades europeas importantes ofrecían el servicio telefónico. El espíritu científico, tecnológico e innovador, permitió la creación en 1925 de los Bell Telephone Laboratories. Innovaciones tales como auriculares, conmutación automática, servicio transoceánico y llamadas directas de larga distancia han estado, en efecto, separadas por bastantes años entre sí.

2.2. HISTORIA DE LAS REDES.

A mediados del siglo XIX los telégrafos conformaban las primeras redes de comunicaciones de la era moderna, la codificación en Morse constituía un método simple y eficaz para la transmisión de información a largas distancias. Aunque el telégrafo se siguió utilizando durante mucho más tiempo el teléfono acabó por imponerse junto con las redes analógicas que fueron mayoritarias durante casi un siglo. El télex, inventado en 1935, fue la primera red digital y que aún hoy sigue

utilizándose prácticamente en su formato original. La historia de las computadoras comienza con el desarrollo de las primeras calculadoras automáticas en los años 40, y pronto se observó la necesidad de acceder a ellas desde puntos remotos, necesidad que se resolvió utilizando módems conectados a las líneas telefónicas existentes.

En los años 70 las comunicaciones informáticas se empezaron a estructurar en protocolos e interfaces estandarizadas. Las primeras redes públicas diseñadas específicamente para el intercambio de información entre ingenieros informáticos fueron las redes de paquetes que datan también de la década de los 70. Gracias a sus mecanismos de routing, control de errores y control de flujo, resultaban más indicadas para la transmisión de datos que las redes de circuitos utilizadas hasta entonces que, en realidad, habían sido concebidas con el único objetivo de transmitir voz.

Este fue el panorama que domino la escena de las redes públicas durante casi veinte años, hasta que apareció la RDSI (ISDN por sus siglas en Inglés) que unificaba las redes de circuitos y de paquetes bajo la misma red, proporcionando simultáneamente los servicios de voz y de datos. La RDSI, ha sido el primer estándar de aceptación universal y en su seno han aparecido nuevas tecnologías de comunicaciones avanzadas como ATM, Frame Relay, etc. Mientras la RDSI se ponía en marcha, tuvo lugar el nacimiento de la informática distribuida (LAN) y un aumento espectacular de la capacidad de proceso de las estaciones de trabajo (PC). Este espectacular crecimiento vivido en la informática no tuvo una comparación equivalente en las redes de comunicaciones que, hoy por hoy, se hallan en clara posición de desventaja.

2.3. HISTORIA DE LA TELEFONIA.

En 1878. Dos años después de la invención del teléfono, Alexander Graham Bell estableció dicha idea claramente: "*Creo que en el futuro los cables unirán las centrales principales de las compañías telefónicas de diferentes ciudades. De este modo un hombre en cualquier lugar del país podrá comunicarse mediante la palabra hablada con cualquier otra parte*".

Desde el mismo año de su invención, el uso del teléfono aumentó rápidamente, solo dos años después de la primera comunicación, realizada en 1878 en New Haven, Connecticut, la mayor parte de las ciudades europeas importantes ofrecían el servicio telefónico.

Toda Europa tenía 97000 abonados en 1887, frente a los 150 000 de los EE.UU. A partir de 1890, varios gobiernos recuperaron el control de las redes telefónicas privadas. El inicio del servicio comercial de larga distancia fomentó la expansión de la telefonía del siglo XIX.

Las primeras tarifas telefónicas no eran baratas. La Bell Telephone Company ensayó varias estrategias en un intento de hacer que el servicio telefónico fuera más asequible, incluyendo en su intento el servicio de contadores y el teléfono público, el cual fue implantado por primera vez en Springfield (Massachusetts) en 1893. Al final, fue el continuo proceso de la ciencia y la tecnología lo que permitió que el teléfono llegara a convertirse en un servicio universal accesible.

Un servicio de alta calidad no se suministro hasta la instalación del primer cable telefónico transatlántico en 1956. Desde la iniciación de la telefonía comercial por satélite en 1965, el número de naciones que quedaban enlazadas por teléfono se incremento aceleradamente.

El espíritu científico, tecnológico e innovador, permitió la creación en 1925 de los Bell Telephone Laboratories. Innovaciones tales como auriculares, conmutación automática, servicio transoceánico y llamadas directas de larga distancia han estado, en efecto, separadas por bastantes años entre sí.

El abonado no ve excesivos cambios en la central telefónica. La provisión de un servicio cada vez más extenso y complicado, frente a un incremento de costos de trabajo y materiales, se ha conseguido gracias a una continua investigación de nuevos materiales, nuevos dispositivos, nuevas técnicas y nuevos métodos. Los plásticos han reemplazado a la madera, al metal y a la ebonita de los viejos aparatos telefónicos y revestimientos de las cubiertas de los cables. Los últimos cables transmiten señales tanto a través de fibras ópticas como de los coaxiales y los bifiliares de cobre. Semiconductores de alta pureza han hecho posible la aparición de los circuitos integrados.

En resumen los primeros teléfonos transmitían una señal a la vez con un solo conductor y retorno por tierra (la tierra hacía de segundo conductor). Hoy en día, miles de conversaciones se transmiten simultáneamente a través de fibras ópticas. Y aunque los radio enlaces por microondas han estado enviando mensajes a través de continentes durante mucho tiempo, ahora pueden enviar las señales alrededor del mundo vía satélite.

REDES DE COMUNICACION

3.1. DEFINICION DE RED

Una red consta de dos o más computadoras conectadas entre sí y permiten compartir recursos e información. La información por compartir suele consistir en archivos y datos. Los recursos son los dispositivos o las áreas de almacenamiento de datos de una computadora, compartida por otra computadora mediante la red. La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresos.

La tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los computadoras (computadores), así como a la puesta en órbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez.

A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

Estos sistemas, se conocen con el nombre de redes de computadoras. Estas nos dan a entender una colección interconectada de computadoras autónomas. Se dice que las computadoras están interconectadas, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que las computadoras son autónomas, excluimos los sistemas en los que una computadora pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

Una red debe ser:

Confiable, estar disponible cuando se le requiera, poseer velocidad de respuesta adecuada, confidencial. Proteger los datos sobre los usuarios de ladrones de información, integra. En su manejo de información.

3.1.1. VENTAJAS

Integración de varios puntos en un mismo enlace. Posibilidad de Crecimiento hacia otros puntos para integración en la misma red. Una LAN da la posibilidad de que las PC's compartan entre ellos programas, información, recursos entre otros. La máquina conectada (PC) cambia continuamente, así que permite que sea innovador este proceso y que se incremente sus recursos y capacidades. Las WAN pueden utilizar un software especializado para incluir mini y macro - computadoras como elementos de red. Las WAN no está limitada a espacio geográfico para establecer comunicación entre PC's o mini o macro - computadoras. Puede llegar a utilizar enlaces de satélites, fibra óptica, aparatos de rayos infrarrojos y de enlaces.

3.1.2. DESVENTAJAS

Se pueden encontrar problemas en el uso de los tipos de topologías, como por ejemplo en el caso de la Bus, en la cual las distancias son limitadas. Y en el caso de la Topología Anillo puede haber dificultad para dar de alta nuevos nodos (pre-cableado), o la operación normal de la red se puede ver afectada si falla algún enlace o nodo.

3.2. REDES EN AMERICA LATINA.

Numerosas redes permiten a investigadores y profesionales tener una visión más amplia de la producción en los más variados sectores, cabe señalar que a pesar de un desarrollo tecnológico acelerado, la práctica de comunicación por redes en nuestros países es aún incipiente, sin embargo las que están interconectadas y que intercambian correo electrónico y/o "noticias" como CCC (Centro de Comunicación Científica de la Universidad de Buenos Aires) y CLACSO en Argentina están creciendo con la aparición de INTERNET. BITNET, FIDONET, UUCP, e INTERNET son las redes mundiales más grandes y de estas, INTERNET es la mayor en cuanto a su crecimiento, su alcance y el volumen de computadoras conectadas, sin embargo, desde cualquiera de estas redes es posible comunicarse con cualquiera de los aprox. 5 a 30 millones de usuarios activos en el mundo de las comunicaciones electrónicas a través de correo electrónico.

3.3. APLICACIÓN DE LAS REDES.

El trabajo a distancia entre instituciones y personas muy diversas, separadas geográficamente como es el caso de CLACSO, ha recibido un gran impulso gracias a la introducción del fax y del correo electrónico. Ello está acelerando el ritmo del intercambio a tal punto que podemos plantearnos acciones concretas e investigaciones de todo tipo coordinadas a distancia. Tal como lo señalo A. Toffler: "lo que está cambiando el equilibrio del poder en el mundo es la combinación de nuevas tecnologías de comunicación cada vez más accesibles (computadoras, teléfonos, módems, satélites), que se traducen en autenticas "autopistas electrónicas".

Las nuevas tecnologías permiten trabajar sin salir de nuestras casas. El tele trabajo ha dejado de ser un mito lejano. Ocho millones de tele-trabajadores europeos y veinticinco en Estados Unidos son los primeros tecnomadas del ciberespacio. No

importa el lugar de residencia, los tecnomadas asumen su condición de pioneros. Las telecomunicaciones les permiten adquirir el don de la ubicuidad.

3.4. USOS DE LAS REDES DE COMPUTADORAS.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente. Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Otro objetivo es el ahorro económico. Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se le denomina LAN (red de área local), en contraste con lo extenso de una WAN (red de área extendida), a la que también se conoce como red de gran alcance.

3.5. TIPOS DE REDES:

3.5.1. RED DE ÁREA LOCAL

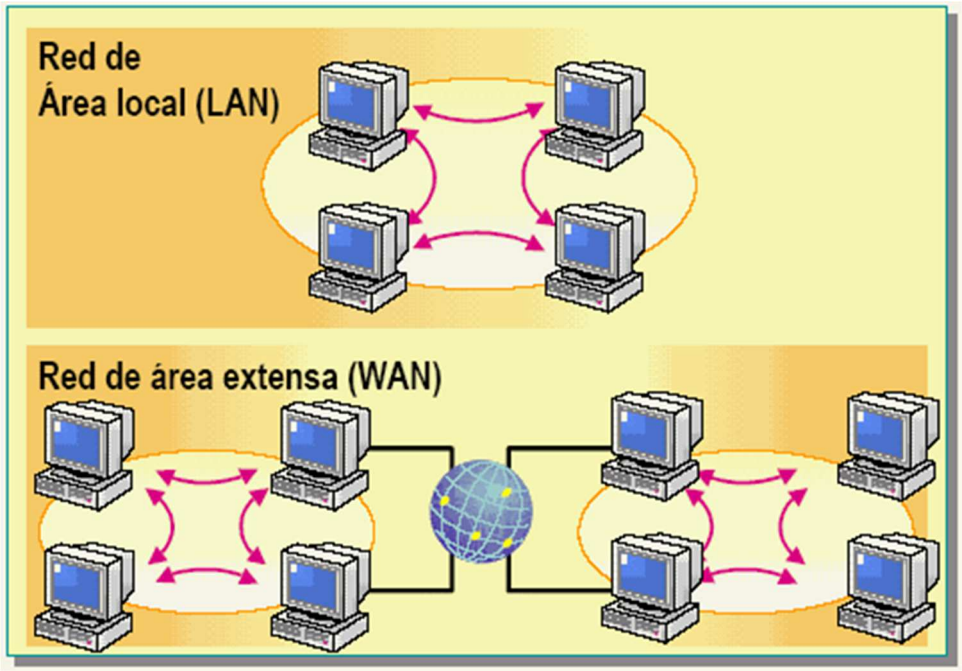
Una red de área local (LAN) conecta equipos ubicados cerca unos de otros. Por ejemplo, dos equipos conectados en una oficina o dos edificios conectados mediante un cable de alta velocidad pueden considerarse una LAN. Una red corporativa que incluya varios edificios adyacentes también puede considerarse una LAN.

3.5.2. RED DE ÁREA METROPOLITANA

Una red de área metropolitana (MAN) abarca una ciudad, el ejemplo más conocido de una MAN es la red de televisión por cable disponible en muchas ciudades. Este sistema creció a partir de los primeros sistemas de antena comunitarias donde la recepción de la televisión al aire era pobre. En dichos sistemas se colocaba una antena grande en la cima de una colina cercana y la señal se canalizaba a las casas de los suscriptores. A partir de que internet atrajo audiencia masiva, los operadores de la red de TV por cable se dieron cuenta de que con algunos cambios al sistema, podrían proporcionar servicio de internet de dos vías en la partes sin uso del espectro. En ese punto el sistema de TV por cable empezaba a transformarse de una forma de distribución de televisión en una red de área metropolitana.

3.5.3. RED DE ÁREA EXTENSA

Una red de área extensa (WAN) conecta varios equipos que se encuentran a gran distancia entre sí. Por ejemplo, dos o más equipos conectados en lugares opuestos del mundo pueden formar una WAN. Una WAN puede estar formada por varias LANs interconectadas. Por ejemplo, Internet es, de hecho, una WAN.



3.5.4. GAN (GLOBAL ÁREA NETWORK)

GAN es un servicio de comunicación móvil que ofrece datos, voz y fax de alta calidad a velocidades de hasta 64 Kbps Los usuarios pueden elegir el servicio ISDN móvil de GAN (Red Digital de Servicio Integrado) para la transferencia rápida de grandes archivos de datos o el servicio móvil de datos por paquete (Mobile Packet Data Service) para aplicaciones de datos de uso variable como es el acceso a Internet y el correo electrónico. GAN también ofrece comunicaciones por voz con calidad de difusión.

Características del servicio

GAN apoya una variedad de canales de comunicación, satisfaciendo así a diversos requisitos de utilización.

Ventajas de GAN

• El servicio GAN puede configurarse para funcionar con casi cualquier aplicación apoyada por las redes terrestres.
• Los terminales son leves, con un peso aproximado de 4 kgs/8,8 lbs., y es fácil ponerlos en funcionamiento.
• GAN es compatible con la tecnología de tarjetas SIM de Telenor, ofreciendo a los usuarios acceso a múltiples terminales, facilitando al mismo tiempo el seguimiento y la facturación de llamadas.

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí. Con el ejemplo de una red es relativamente fácil para dos o más personas que viven en lugares separados, escribir informes juntos.

3.6. ESTRUCTURA DE UNA RED.

En toda red existe una colección de máquinas para correr programas de usuario (aplicaciones). Seguiremos la terminología de una de las primeras redes, denominada ARPANET, y llamaremos hostales a las máquinas antes mencionadas. También, en algunas ocasiones se utiliza el término sistema terminal o sistema final. Los hostales están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre hostales, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales).
Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan

de mover bits entre máquinas. Los elementos de conmutación son computadoras especializados que se utilizan para conectar dos o más líneas de de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos

3.7. RAZONES PARA INSTALAR REDES DE COMPUTADORAS.

Desde sus inicios una de las razones para instalar redes era compartir recursos, como discos, impresoras y trazadores. Ahora existen además otras razones:

Disponibilidad del software de redes.- El disponer de un software multiusuario de calidad que se ajuste a las necesidades de la empresa. Por ejemplo: Se puede diseñar un sistema de puntos de venta ligado a una red local concreta. El software de redes puede bajar los costos si se necesitan muchas copias del software.

Trabajo en común.- Conectar un conjunto de computadoras personales formando una red que permita que un grupo o equipo de personas involucrados en proyectos similares puedan comunicarse fácilmente y compartir programas o archivos de un mismo proyecto.

Actualización del software.- Si el software se almacena de forma centralizada en un servidor es mucho más fácil actualizarlo. En lugar de tener que actualizarlo individualmente en cada uno de los PC de los usuarios, pues el administrador tendrá que actualizar la única copia almacenada en el servidor.

Copia de seguridad de los datos.- Las copias de seguridad son más simples, ya que los datos están centralizados.

Ventajas en el control de los datos.- Como los datos se encuentran centralizados en el servidor, resulta mucho más fácil controlarlos y recuperarlos. Los usuarios pueden transferir sus archivos vía red antes que usar los disquetes.

Uso compartido de las impresoras de calidad.- Algunos periféricos de calidad de alto costo pueden ser compartidos por los integrantes de la red. Entre estos: impresoras láser de alta calidad, etc.

Correo electrónico y difusión de mensajes.- El correo electrónico permite que los usuarios se comuniquen más fácilmente entre sí. A cada usuario se le puede asignar un buzón de correo en el servidor. Los otros usuarios dejan sus mensajes en el buzón y el usuario los lee cuando los ve en la red. Se pueden convenir reuniones y establecer calendarios.

Ampliación del uso con terminales tontos.- Una vez montada la red local, pasa a ser más barato el automatizar el trabajo de más empleados por medio del uso de terminales tontos a la red.

Seguridad.- La seguridad de los datos puede conseguirse por medio de los servidores que posean métodos de control, tanto software como hardware. Los terminales tontos impiden que los usuarios puedan extraer copias de datos para llevárselos fuera del edificio.

Las distintas configuraciones tecnológicas y la diversidad de necesidades planteadas por los usuarios, lleva a las organizaciones a presentar cierta versatilidad en el acceso a la documentación, mediante una combinación de comunicación sincrónica y asincrónica.

La comunicación sincrónica (o comunicación a tiempo real) contribuiría a motivar la comunicación, a simular las situaciones, cara a cara, mientras que la comunicación asincrónica (o retardada) ofrece la posibilidad de participar e intercambiar información desde cualquier sitio y en cualquier momento, permitiendo a cada participante trabajar a su propio ritmo y tomarse el tiempo necesario para leer, reflexionar, escribir y revisar antes de compartir la información.

3.8. COMPONENTES BÁSICOS DE UNA RED.

Servidor.- Es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones. Puede ser dedicado o no dedicado.

Estaciones de Trabajo.- Se pueden conectar a través de la placa de conexión de red y el cableado correspondiente. Los terminales ´tontos´ utilizados con las grandes computadoras y mini computadoras son también utilizadas en las redes, y no poseen capacidad propia de procesamiento.

Tarjetas de Conexión de Red (Interface Cards).- Permiten conectar el cableado entre servidores y estaciones de trabajo. En la actualidad existen numerosos tipos de placas que soportan distintos tipos de cables y topologías de red.

3.9. CABLEADO.

Una vez que tenemos las estaciones de trabajo, el servidor y las placas de red, requerimos interconectar todo el conjunto. El tipo de cable utilizado depende de muchos factores, que se mencionarán a continuación:

Los tipos de cableado de red más populares son: par trenzado, cable coaxial y fibra óptica.

Además se pueden realizar conexiones a través de radio o microondas. Cada tipo de cable o método tiene sus ventajas. Y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad.

3.9.1. CABLES DE RED

3.9.1.1. PAR TRENZADO

El cable de par trenzado es el tipo más habitual utilizado en redes.

El cable de par trenzado (10baseT) está formado por dos hebras aisladas de hilo de cobre trenzado entre sí. Existen dos tipos de cables de par trenzado: par trenzado sin apantallar (*unshielded twisted pair*, **UTP**) y par trenzado apantallado (*shielded twisted pair*, **STP**). Éstos son los cables que más se utilizan en redes y pueden transportar señales en distancias de 100 metros.

- El cable UTP es el tipo de cable de par trenzado más popular y también es el cable en una LAN más popular.
- El cable STP utiliza un tejido de funda de cobre trenzado que es más protector y de mejor calidad que la funda utilizada por UTP. STP también utiliza un envoltorio plateado alrededor de cada par de cables. Con ello, STP dispone de una excelente protección que protege a los datos transmitidos de interferencias exteriores, permitiendo que STP soporte índices de transmisión más altos a través de mayores distancias que UTP.

El cableado de par trenzado utiliza conectores Registered Jack 45 (RJ-45) para conectarse a un equipo. Son similares a los conectores Registered Jack 11 (RJ-11).

Entre sus principales ventajas tenemos:

- Es una tecnología bien estudiada
- No requiere una habilidad especial para instalación
- La instalación es rápida y fácil
- La emisión de señales al exterior es mínima.

Ofrece alguna inmunidad frente a interferencias, modulación cruzada y corrosión.

3.9.1.2. CABLE COAXIAL.

El cable coaxial se utiliza cuando los datos viajan por largas distancias.

El cable coaxial está formado por un núcleo de hilo de cobre rodeado de un aislamiento, una capa de metal trenzado, y una cubierta exterior. El núcleo de un cable coaxial transporta las señales eléctricas que forman los datos. Este hilo del núcleo puede ser sólido o hebrado. Existen dos tipos de cable coaxial: cable coaxial ThinNet (10Base2) y cable coaxial ThickNet (10Base5). El cableado coaxial es una buena elección cuando se transmiten datos a través de largas distancias y para ofrecer un soporte fiable a mayores velocidades de transferencia cuando se utiliza equipamiento menos sofisticado.

El cable coaxial debe tener terminaciones en cada extremo.

- El cable coaxial ThinNet puede transportar una señal en una distancia aproximada de 185 metros.
- El cable coaxial ThickNet puede transportar una señal en una distancia de 500 metros. Ambos cables, ThinNet y ThickNet, utilizan un componente de conexión (conector BNC) para realizar las conexiones entre el cable y los equipos.

El cable coaxial ofrece las siguientes ventajas:

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

Es una tecnología bien estudiada.

3.9.1.3. CONEXIÓN FIBRA ÓPTICA.

El cable de fibra óptica utiliza fibras ópticas para transportar señales de datos digitales en forma de pulsos modulados de luz. Como el cable de fibra óptica no

transporta impulsos eléctricos, la señal no puede ser intervenida y sus datos no pueden ser robados. El cable de fibra óptica es adecuado para transmisiones de datos de gran velocidad y capacidad ya que la señal se transmite muy rápidamente y con muy poca interferencia. Un inconveniente del cable de fibra óptica es que se rompe fácilmente si la instalación no se hace cuidadosamente. Es más difícil de cortar que otros cables y requiere un equipo especial para cortarlo.

Ofrece las siguientes ventajas:

- Alta velocidad de transmisión
- No emite señales eléctricas o magnéticas, lo cual redunda en la seguridad
- Inmunidad frente a interferencias y modulación cruzada.
- Mayor economía que el cable coaxial en algunas instalaciones.
- Soporta mayores distancias

Selección de cables

La siguiente tabla ofrece una lista de las consideraciones a tener en cuenta para el uso de las tres categorías de cables de red.

Categorías	Utilizar si	No utilizar si
Par trenzado	Desea una instalación relativamente sencilla en la que las conexiones entre equipos sean simples.	Su LAN requiere un alto nivel de protección de las señales para aislarlas de ondas electromagnéticas que podrían interferir en la señal eléctrica transportada por el cable. Debe transmitir datos a larga distancia y a gran velocidad.
Coaxial	Necesita transmitir datos entre las mayores distancias posibles con cableado más económico.	Necesita cambiar los cables de red frecuentemente debido a reubicaciones.
Fibra óptica	Necesita transmitir datos seguros a gran velocidad y en largas distancias.	Su presupuesto es bajo. No tiene experiencia para instalar y conectar dispositivos adecuadamente.

3.9.1.4. CONEXIÓN INALÁMBRICA

Los componentes inalámbricos se utilizan para la conexión a redes en distancias que hacen que el uso de adaptadores de red y opciones de cableado estándares sea técnica o económicamente imposible. Las redes inalámbricas están formadas por componentes inalámbricos que se comunican con LANs.

Existen dos técnicas habituales para la transmisión inalámbrica en una LAN: transmisión por infrarrojos y transmisión de radio en banda estrecha.

• Transmisión por infrarrojos

Funciona utilizando un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben; si hay algo que bloquee la señal infrarroja, puede impedir la comunicación. Estos sistemas deben generar señales muy potentes, ya que las señales de transmisión débiles son susceptibles de recibir interferencias de fuentes de luz, como ventanas.

• Transmisión vía radio en banda estrecha

El usuario sintoniza el transmisor y el receptor a una determinada frecuencia. La radio en banda estrecha no requiere visibilidad directa porque utiliza ondas de radio. Sin embargo la transmisión vía radio en banda estrecha está sujeta a interferencias de paredes de acero e influencias de carga. La radio en banda estrecha utiliza un servicio de suscripción. Los usuarios pagan una cuota por la transmisión de radio.

Existen diferentes problemas para la comunicación inalámbrica

• La distancia que puede alcanzarse depende de la potencia del emisor y de la frecuencia de transmisión.
• En algunos casos las condiciones del aire (climáticas) pueden deteriorar la transmisión.
• La transmisión puede ser interceptada con mayor facilidad.

3.9.2. TOPOLOGIA:

Topología de red es la forma en que se distribuyen los cables de la red para conectarse con el servidor y con cada una de las estaciones de trabajo, ya que se pueden tender cables a cada estación de trabajo y servidor de la red, La flexibilidad de una red en cuanto a sus necesidades futuras se refiere, depende en gran parte de la topología establecida.

La topología es tanto física como lógica:

1. • La topología física describe cómo están conectados los componentes físicos de una red.
2. • La topología lógica describe el modo en que los datos de la red fluyen a través de componentes físicos.

Existen cinco topologías básicas:

1. • *Bus.* Los equipos están conectados a un cable común compartido.
2. • *Estrella.* Los equipos están conectados a segmentos de cable que se extienden desde una ubicación central, o concentrador.
3. • *Anillo*. Los equipos están conectados a un cable que forma un bucle alrededor de una ubicación central.
4. • *Malla.* Los equipos de la red están conectados entre sí mediante un cable.
5. • *Híbrida.* Dos o más topologías utilizadas juntas.

3.9.2.1. TOPOLOGÍA DE BUS

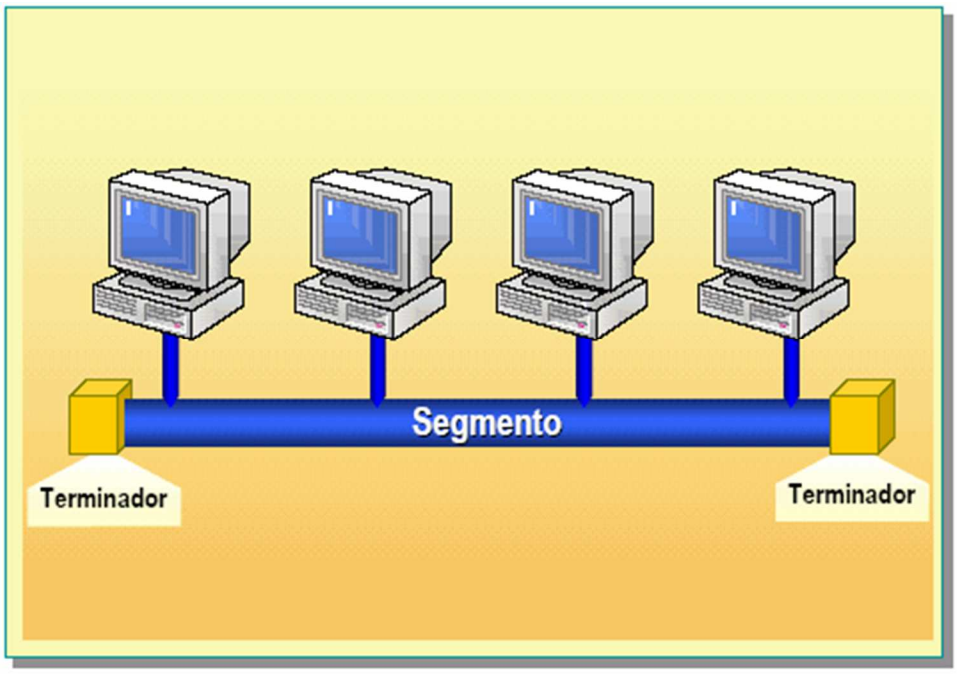
En una topología de bus, todos los equipos de una red están unidos a un cable continuo, o segmento, que los conecta en línea recta. En esta topología en línea recta, el paquete se transmite a todos los adaptadores de red en ese segmento. **Importante** Los dos extremos del cable deben tener terminaciones. Todos los adaptadores de red reciben el paquete de datos.

Si se produce una rotura en cualquier parte del cable o si un extremo no está terminado, la señal balanceará hacia adelante y hacia atrás a través de la red y la comunicación se detendrá.

El número de equipos presentes en un bus también afecta al rendimiento de la red. Cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus, y en consecuencia, la red irá más lenta.

Además, debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho *ruido*. Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente. Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.

La principal desventaja es: El cable central puede convertirse en un cuello de botella en entornos con un tráfico elevado. Es difícil aislar los problemas de cableado en la red y determinar que estación o segmento de cable los origina, ya que todas las estaciones de trabajo están en el mismo cable. Una rotura de cable hará caer el sistema.

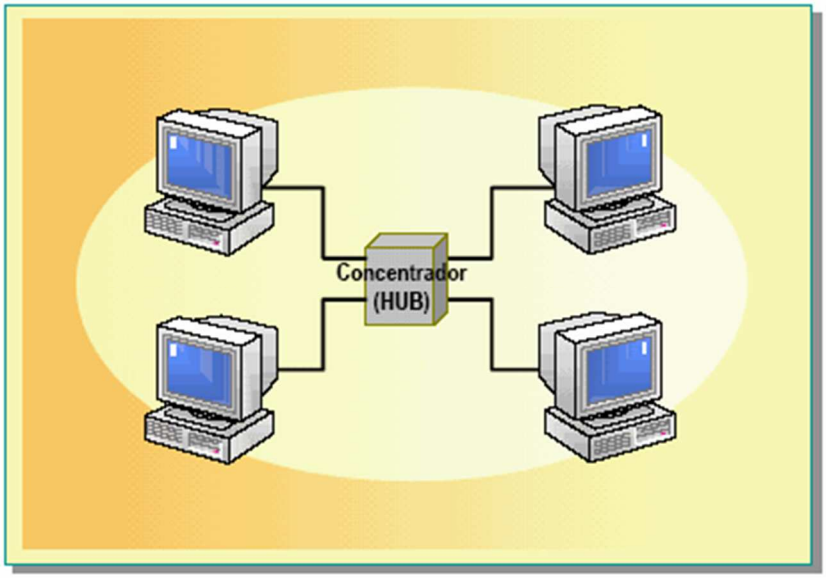


3.9.2.2. TOPOLOGÍA EN ESTRELLA

En una topología en estrella, los segmentos de cable de cada equipo en la red están conectados a un componente centralizado, o *concentrador*. Un concentrador es un dispositivo que conecta varios equipos juntos. En una topología en estrella, las señales se transmiten desde el equipo, a través del concentrador, a todos los equipos de la red. A mayor escala, múltiples LANs pueden estar conectadas entre sí en una topología en estrella.

Una ventaja de la topología en estrella es que si uno de sus equipos falla, únicamente este equipo es incapaz de enviar o recibir datos. El resto de la red funciona normalmente.

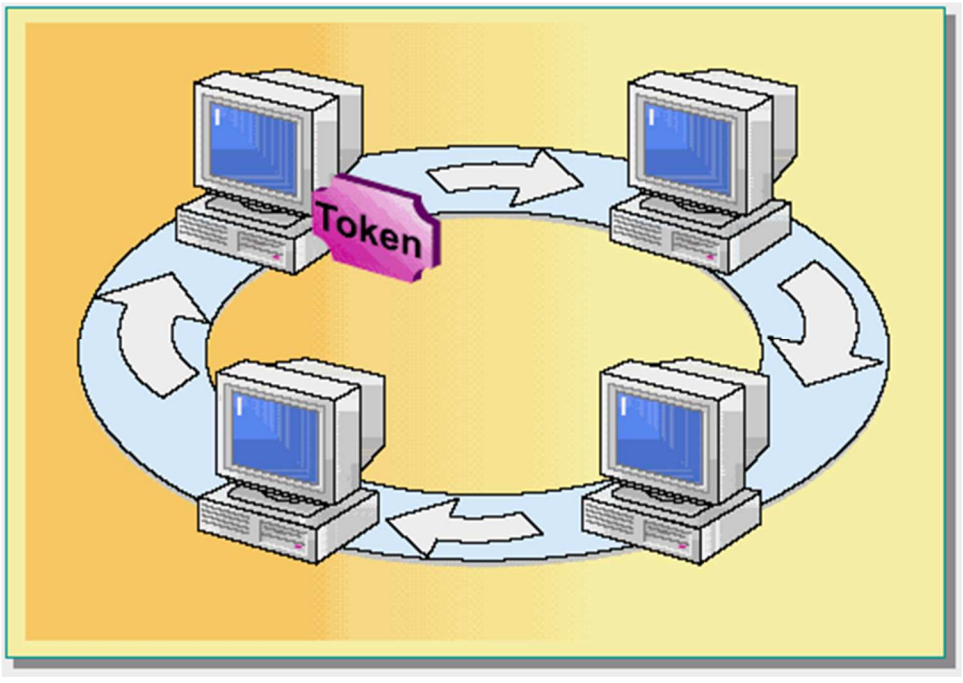
El inconveniente de utilizar esta topología es que debido a que cada equipo está conectado a un concentrador, si éste falla, fallará toda la red. Además, en una topología en estrella, el ruido se crea en la red.



3.9.2.3. TOPOLOGÍA ANILLO

Las señales viajan en una única dirección a lo largo del cable en forma de un bucle cerrado. En cada momento, cada nodo pasa las señales a otro nodo. Con la topología en anillo, las redes pueden extenderse a menudo a largas distancias, y el coste total del cableado será menor que en una configuración en estrella y casi igual a la bus. Una rotura del cable hará caer el sistema. Actualmente existen sistemas alternativos que evitan que esto ocurra.

La ventaja de una topología en anillo es que cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo, conservando la potencia de la señal. El inconveniente de una topología en anillo es que los equipos sólo pueden enviar los datos de uno en uno en un único *Token Ring*. Además, las topologías en anillo son normalmente más caras que las tecnologías de bus.

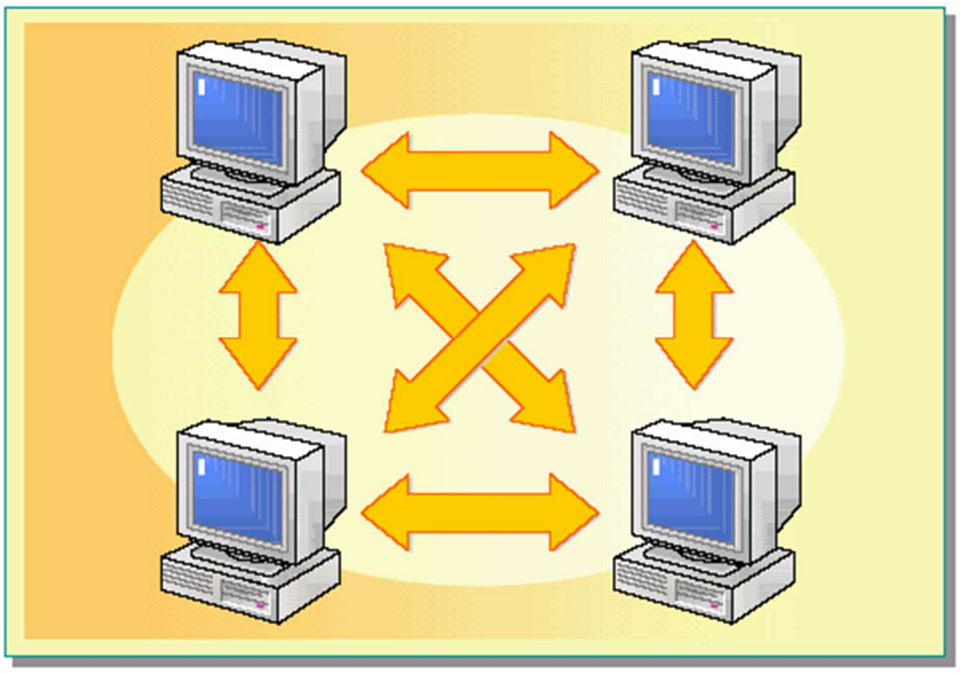


3.9.2.4. TOPOLOGÍA DE MALLA

En una topología de malla, cada equipo está conectado a cada uno del resto de equipos por un cable distinto. Esta configuración proporciona rutas redundantes a través de la red de forma que si un cable falla, otro transporta el tráfico y la red sigue funcionando.

A mayor escala, múltiples LANs pueden estar en estrella conectadas entre sí en una topología de malla utilizando red telefónica conmutada, un cable coaxial ThickNet o el cable de fibra óptica.

Una de las ventajas de las topologías de malla es su capacidad de respaldo al proporcionar múltiples rutas a través de la red. Debido a que las rutas redundantes requieren más cable del que se necesita en otras topologías, una topología de malla puede resultar cara.



3.9.2.4. TOPOLOGÍAS HÍBRIDAS

En una topología híbrida, se combinan dos o más topologías para formar un diseño de red completo. Raras veces, se diseñan las redes utilizando un solo tipo de topología. Por ejemplo, es posible que desee combinar una topología en estrella con una topología de bus para beneficiarse de las ventajas de ambas.

Importante: En una topología híbrida, si un solo equipo falla, no afecta al resto de la red.

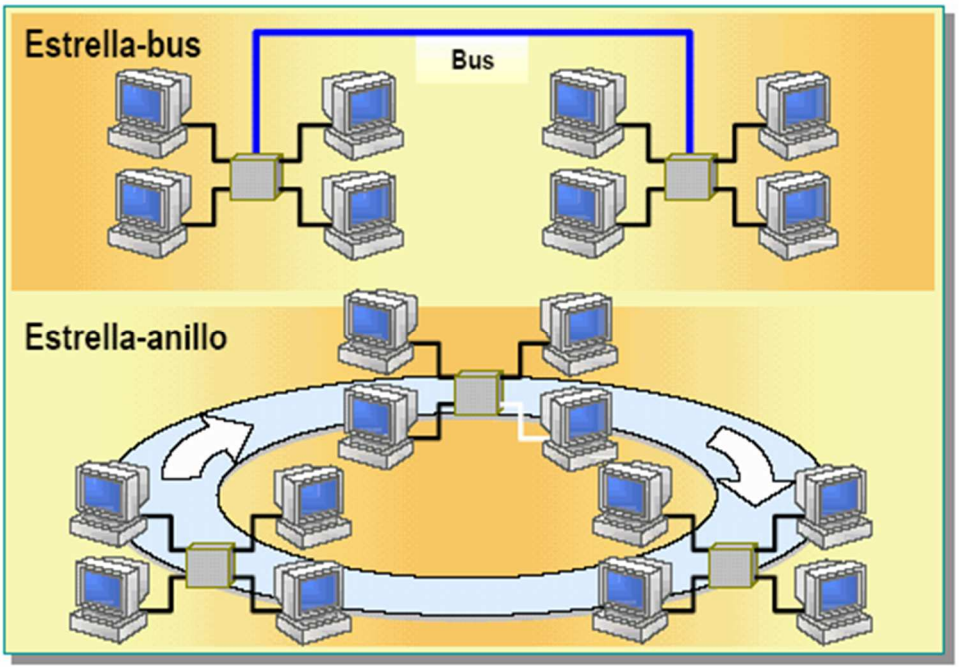
Normalmente, se utilizan dos tipos de topologías híbridas: topología en estrella-bus y topología en estrella-anillo.

Estrella-bus: En una topología en estrella-bus, varias redes de topología en estrella están conectadas a una conexión en bus. Cuando una configuración en estrella está llena, podemos añadir una segunda en estrella y utilizar una conexión en bus para conectar las dos topologías en estrella.

En una topología en estrella-bus, si un equipo falla, no afectará al resto de la red. Sin embargo, si falla el componente central, o concentrador, que une todos los equipos en estrella, todos los equipos adjuntos al componente fallarán y serán incapaces de comunicarse.

Estrella-anillo: En la topología en estrella-anillo, los equipos están conectados a un componente central al igual que en una red en estrella. Sin embargo, estos componentes están enlazados para formar una red en anillo.

Al igual que la topología en estrella-bus, si un equipo falla, no afecta al resto de la red. Utilizando el paso de testigo, cada equipo de la topología en estrella-anillo tiene las mismas oportunidades de comunicación. Esto permite un mayor tráfico de red entre segmentos que en una topología en estrella-bus.



3.10. PROTOCOLOS

Las placas de conexión de red están diseñadas para trabajar con un tipo de topología. La circuitería de la placa suministra los protocolos para la comunicación con el resto de estaciones de red a través del cableado. Un protocolo establece las directrices que determinan cómo y cuándo una estación de trabajo puede acceder al cable y enviar paquetes de datos. Los protocolos se diferencian por el punto en que reside el control y en la forma de acceso al cable.

3.10.1. INTERCONEXIÓN DE REDES.

Actualmente existe una gran variedad de redes no sólo por el número sino también por la diversidad de protocolos que ellas utilizan. Por tanto es necesario conocer la

naturaleza de las distintas redes y los distintos protocolos cuando se desea establecer conexión entre ellas.

En general se pueden presentar los siguientes casos de conexión entre distintas redes.

- Red de área local con red de área local.
- Red de área local con red de área extensa
- Red de área extensa con red de área extensa
- Red de área local con red de área local a través de una red de área extensa.

La red puede aumentar sus capacidades, tanto de interoperatividad como de cobertura, o simplemente incrementar el número de estaciones conectadas, mediante los siguientes dispositivos:

1. Repetidoras
2. Puentes o Bridge
3. Encaminadores o Ruteadores
4. Pasarelas o Gateway

3.10.2. MODELO OSI

La ISO (International Organisation for Standarisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos, en la página siguiente puedes verlo con más detalle.

Nivel 1.- Físico - Se ocupa de la transmisión del flujo de bits a través del medio. - Cables, tarjetas y repetidores (hub).

RS-232, X.21.

Nivel 2 - Enlace - Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos. - Puentes (bridges). HDLC y LLC.

Nivel 3 - Red - Establece las comunicaciones y determina el camino que tomarán los datos en la red. - Encaminador(router). IP, IPX.

Nivel 4 - Transporte - La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente. - Pasarela (gateway). UDP, TCP, SPX.

Nivel 5 - Sesión - Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones). - Pasarela

Nivel 6 - Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes. - Pasarela. Compresión, encriptado, VT100.

Nivel 7 - Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero). - X400

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas datos de control.

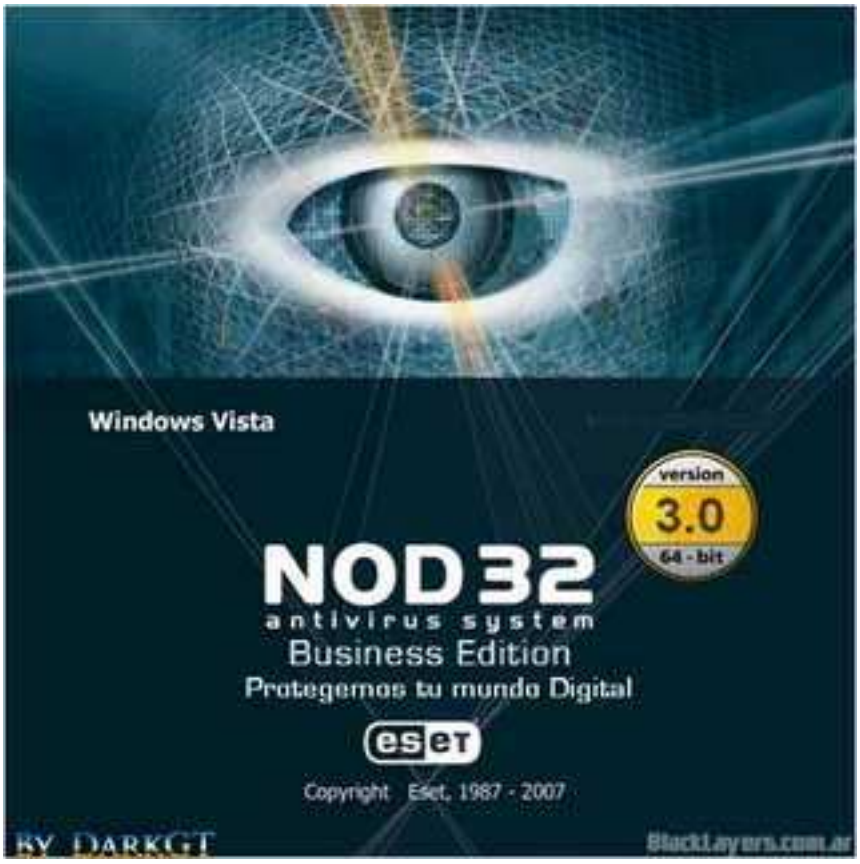
De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma, pues de enviar información en el modelo OSI tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Emisor	**Paquete**	**Receptor**
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

C7-C2 : Datos de control específicos de cada nivel.

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos **protocolos**. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.



HERRAMIENTAS DE SEGURIDAD

4. CONCEPTO DE HERRAMIENTAS DE SEGURIDAD

La Posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados. Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento en la seguridad en la comunicación a través de redes, especialmente Internet, consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información, más que en la seguridad en los computadoras, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, más que físicos.

4.1. AMENAZAS DELIBERADAS A LA SEGURIDAD DE LA INFORMACIÓN

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.

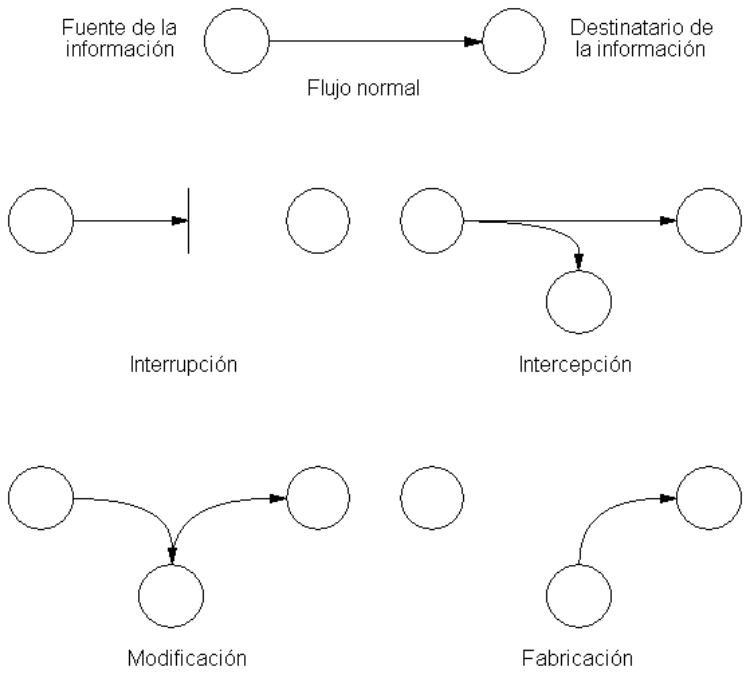
Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes (v. Figura):

- **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 una computadora. 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.

4.2. ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- **Control del volumen de tráfico** intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

4.3. ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de pesetas en la cuenta A” podría ser modificado para decir “Ingresa un millón de pesetas en la cuenta B”.

- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de **denegación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

4.4. SERVICIOS DE SEGURIDAD

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

- **Confidencialidad**: requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.
- **Autenticación**: requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que

asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

- **Integridad**: requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time-stamps.
- **No repudio**: ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.
- **Control de acceso**: requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.
- **Disponibilidad**: requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

4.5. MECANISMOS DE SEGURIDAD

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- **Intercambio de autenticación**: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.
- **Cifrado**: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). 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. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. 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. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

- **Integridad de datos**: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.
- **Firma digital**: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.
- **Control de acceso**: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.
- **Tráfico de relleno**: consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
- **Control de encaminamiento**: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.
- **Unicidad**: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

4.6. SOFTWARE EN SEGURIDAD DE REDES

El elevado volumen de sucesos de sistema que se genera diariamente es una valiosa fuente de información para los administradores de red para ayudarlos a monitorizar cambios de configuración, acciones administrativas, identificar errores de sistema y brechas de seguridad sospechosas. Esta es, sin embargo, una tarea abrumadora sin las herramientas apropiadas. Cuanto más grande es la red, mayor es su necesidad de una solución que le permita monitorizar, administrar y archivar miles de sucesos generados por dispositivos a través de redes heterogéneas.

4.6.1. ESCÁNER DE SEGURIDAD DE RED Y GESTIÓN DE VULNERABILIDAD

GFI LANguard es un programa de escáner de red y de seguridad utilizada por más de 20.000 clientes que les permite analizar su red y puertos para detectar, evaluar y rectificar vulnerabilidades de seguridad con el mínimo esfuerzo administrativo. Como administrador, tiene que tratar diferentemente problemas relacionados con problemas de seguridad, administración de parches y auditoría de red, a veces utilizando varios programas de escaneo. Sin embargo, con GFI LANguard estos tres pilares de la gestión de vulnerabilidad son abordados en un programa, permitiéndole tener una panorámica completa de su configuración de red y mantener seguro el estado de la red más rápida y eficientemente.

Gestión de vulnerabilidad

GFI LANguard realiza análisis de red utilizando bases de datos de vulnerabilidad basadas en OVAL y SANS Top 20, proporcionando más de 15.000 evaluaciones de vulnerabilidad cuando su red, incluyendo entornos virtuales, es analizada. GFI LANguard le permite analizar el estado de seguridad de su red y tomar acciones para asegurar la red antes de que esté comprometida.

Administración de actualizaciones

Cuando se completa un análisis de red, las capacidades de gestión de actualizaciones de GFI LANguard proporciona toda la funcionalidad y herramientas que necesita para instalar y administrar eficazmente las actualizaciones en todos los equipos a través de diferentes plataformas de sistemas operativos y productos Microsoft en 38 idiomas. Además de descargar automáticamente las actualizaciones de seguridad de Microsoft que falten, también puede implantar automáticamente las actualizaciones o service

packs de Microsoft que falten en toda la red al final de los análisis programados.

Auditoría de red

La función de auditoría de red de GFI LANguard le dice todo lo que necesita saber sobre su red recuperando información del hardware sobre memoria, procesadores, adaptadores gráficos, dispositivos de almacenamiento, detalles de placa base, impresoras y puertos en uso. Utilizando comparaciones básicas puede comprobar si se agregó/eliminó hardware desde el último análisis. GFI LANguard también puede identificar y generar informes sobre instalaciones de software no autorizado y proporcionar alertas o bien desinstalar automáticamente estas aplicaciones no autorizadas si son detectadas en la red.

4.6.2. MONITORIZACIÓN, ADMINISTRACIÓN, Y ARCHIVO DE SUCESOS

GFI EventsManager 8, es una solución de monitorización, administración y archivo de sucesos, soporta una amplia familia de tipos de sucesos como W3C, sucesos Windows, Syslogs y, en la última versión, traps SNMP generados por dispositivos tales como cortafuegos (firewalls), enrutadores y sensores. Proporcionando soporte para dispositivos de los 20 principales fabricantes del mundo así como dispositivos a medida, GFI EventsManager le permite monitorizar una amplia familia de productos hardware, generar informes sobre el estado operativo de cada uno y recoger información para el análisis. También puede seguir la actividad de los empleados en la red tales como cambios hechos en sus PCs, archivos accedidos durante el día, cumplimiento legal y regulador tal como SOX, PCI DSS, HIPAA y mucho más.

GFI EventsManager ayuda a su organización a dirigir las siguientes 4 areas:

- Seguridad del sistema de información y de la red: Detecte intrusos y brechas de seguridad
- Monitorización de la salud del sistema: Monitorice proactivamente sus servidores
- Cumplimiento legal y regulador: Una ayuda para cumplir con las regulaciones
- Investigaciones forenses: Un punto de referencia cuando algo va mal.

¿Por qué utilizar GFI EventsManager?

- Centraliza los sucesos Syslog, W3C, Windows y SNMP Traps generados por firewalls, servidores, enrutadores, switches, sistemas telefónicos, PCs y más.
- Incrementa el tiempo de actividad e identifica problemas mediante alertas en tiempo real.
- Monitorización y administración de toda la red rápida y económica.
- Auditoría SQL Server para SQL Server 2000, 2005, 2008 y también MSDE y SQL Express.
- Rendimiento sin igual de escaneo de sucesos de hasta 6 millones de sucesos por hora.
- Certificado para Windows Server 2008; Soporta Windows Vista.

Estos programas tienen todas las ventajas al ser utilizados pues ayudan a escanear en su totalidad toda la red, detectando todos los problemas con algún otro programa e intrusos que afecten el funcionamiento de cualquier computadora en cualquier red.

Sus principales ventajas son:

-pueden monitorear toda una red; información, daños, intrusos, etc.

-previene y actualiza todos los tipos de programas o vacunas de seguridad para el sistema o red en cuestión.

-busca cualquier actualización para la red, ya sea de información o de seguridad.

4.7. MANTENIMIENTO

4.7.1. MANTENIMIENTO DE HARDWARE

Se puede definir Mantenimiento del PC como una serie de rutinas periódicas que debemos realizar a la PC, necesarias para que la computadora ofrezca un rendimiento óptimo y eficaz a la hora de su funcionamiento. De esta forma podemos prevenir o detectar cualquier falla que pueda presentar el computador.

4.7.2. RAZONES PARA HACER UN MANTENIMIENTO A UNA COMPUTADORA

Las computadoras funcionan muy bien y están protegidas cuando reciben mantenimiento. Si no se limpian y se organizan con frecuencia, el disco duro se llena

de información, el sistema de archivos se desordena y el rendimiento general disminuye.

Si no se realiza periódicamente un escaneo del disco duro para corregir posibles errores o fallas, una limpieza de archivos y la desfragmentación del disco duro, la información estará más desprotegida y será más difícil de recuperar.

El mantenimiento que se debe hacer, se puede resumir en tres aspectos básicos importantes, los cuales son:

Diagnóstico.

Limpieza.

Desfragmentación.

4.7.3. DIAGNOSTICO

La computadora trabaja más de lo que normalmente se cree. Está constantemente dando prioridad a las tareas, ejecutando órdenes y distribuyendo la memoria.

Sin embargo, con el tiempo ocurren errores en el disco duro, los datos se desorganizan y las referencias se vuelven obsoletas.

Estos pequeños problemas se acumulan y ponen lento el sistema operativo, las fallas del sistema y software ocurren con más frecuencia y las operaciones de encendido y apagado se demoran más.

Para que el sistema funcione adecuadamente e incluso para que sobre todo no se ponga tan lento, se debe realizar un mantenimiento periódico.

Asegurándonos de incluir en la rutina del mantenimiento estas labores:

- Exploración del disco duro para saber si tiene errores y solucionar los sectores alterados.
- Limpieza de archivos.
- Desfragmentación el disco duro.

4.7.4. LIMPIEZA

Para garantizar un rendimiento optimo y eficaz de la computadora, debemos mantenerla limpia y bien organizada.

Debemos eliminar los programas antiguos, programas que no utilicemos y las unidades de disco para liberar la memoria y reducir la posibilidad de conflicto del sistema.

Un disco duro puede presentar diversas deficiencias, que casi siempre se pueden corregir estas son:

- Poco espacio disponible.
- Espacio ocupado por archivos innecesarios.
- Alto porcentaje de fragmentación.

Se debe eliminar los archivos antiguos y temporales. Además, entre más pocos archivos innecesarios tenga la computadora, estará más protegida de amenazas como el hurto de la identidad en Internet.

Cuando el espacio libre de un disco se acerca peligrosamente a cero, la computadora entra en una fase de funcionamiento errático: se torna excesivamente lenta, emite mensajes de error (que en ocasiones no especifican la causa), algunas aplicaciones no se inician, o se cierran después de abiertas, etc.

Como factor de seguridad aceptable, el espacio vacío de un disco duro no debe bajar del 10% de su capacidad total, y cuando se llega a este límite deben borrarse archivos innecesarios, o desinstalar aplicaciones que no se usen, o comprimir archivos.

Todas las aplicaciones de Windows generan archivos temporales.

Estos archivos se reconocen por la extensión .tmp y generalmente existe uno o varios directorios donde se alojan.

En condiciones normales, las aplicaciones que abren archivos temporales deben eliminarlos cuando la aplicación concluye, pero esto a veces no sucede cuando se concluye en condiciones anormales, o Windows "se cuelga" o por una deficiente programación de la aplicación.

Estos archivos temporales deben borrarse del disco duro.

Existen otro tipo de archivos que pueden borrarse, y no son temporales: la papelera de reciclaje, el caché de Internet (Windows\temporary internet files) y algunas carpetas que permanecen el disco después que se baja o se instala un programa.

El caché de Internet debe borrarse si resulta estrictamente necesario, ya que después de borrado no podrán verse las páginas visitadas sin estar conectado.

Debe hacerse mediante la función explícita del navegador, y además ajustarse el tamaño del caché.

Un usuario experimentado puede intentar otras posibilidades, como por ejemplo eliminar DLL duplicadas, instaladores, datos de aplicaciones desinstaladas, etc.

Debe obrar con mucho cuidado cuando haga esta "limpieza profunda" y si no hay plena seguridad de que un archivo en cuestión puede ser borrado, no debe eliminarlo de la papelera de reciclaje hasta comprobarlo, pudiendo reponerse a su ubicación original si resultara necesario.

En general lo que se debe realizar son estas labores:

- Eliminar los programas antiguos y archivos temporales.
- Eliminar la información obsoleta
- Asegurarnos de guardar de manera segura la información.
- Eliminar las entradas de registro inválidas y los accesos directos dañados.

4.7.5. DESFRAGMENTACIÓN

De todos los componentes de una computadora, el disco duro es el más sensible y el que más requiere un cuidadoso mantenimiento.

La detección precoz de fallas puede evitar a tiempo un desastre con pérdida parcial o total de información (aunque este evento no siempre puede detectarse con anticipación).

Alto porcentaje de fragmentación: Durante el uso de una computadora existe un ininterrumpido proceso de borrado de archivos e instalación de otros nuevos.

Estos se instalan a partir del primer espacio disponible en el disco y si no cabe se fracciona, continuando en el próximo espacio vacío.

Un índice bajo de fragmentación es tolerable e imperceptible, pero en la medida que aumenta, la velocidad disminuye en razón del incremento de los tiempos de acceso al disco ocasionado por la fragmentación, pudiendo hacerse notable.

Todas las versiones de Windows incluyen el desfragmentador de disco.

El proceso de desfragmentación total consume bastante tiempo (en ocasiones hasta horas), y aunque puede realizarse como tarea de fondo no resulta conveniente la ejecución simultanea de otro programa mientras se desfragmenta el disco, debiendo desactivarse también el protector de pantalla.

4.7.6. CONSIDERACIONES SOBRE LA LIMPIEZA DE UNA COMPUTADORA

Es fundamental limpiar una computadora usada antes de comenzar a desarmarla, utilizando por ejemplo una aspiradora con pico fino y un pincel para retirar el polvo.

Nunca utilice solventes derivados del petróleo ni alcoholes para limpiar los frentes y carcasas de computadoras y monitores. Utilice un paño húmedo con un poco de detergente, o con algún tipo de limpiador universal, tomando en cuenta no pulverizar el limpiador sobre los elementos de la computadora, sino sobre el paño.

Ciertos elementos ameritan un desamado más completa para retirar el polvo de su interior: disqueteras, CD-ROM, unidades de cinta, fuente de alimentación, y el conjunto disipador-ventilador de las CPU (sí se separara el disipador del procesador, es imprescindible reponer la grasa siliconada en caso de que esta exista, si no existe debemos ponerla.).

No se deben tocar los conectores de borde de las tarjetas y módulos de memoria con los dedos pues la humedad y la grasitud de ellos forman depósitos que a la larga corroen los contactos. Más aún, es aconsejable limpiar todos los conectores de borde mediante el uso de un trozo de papel tisúes.

Todo ambiente donde se trabaje con computadoras debe ser lo más limpio posible de polvo y otros contaminantes, incluyendo particularmente el humo del tabaco (es notorio el color amarillo que toman los plásticos de los monitores situados sobre escritorios de usuarios fumadores).

4.7.7. CONSIDERACIONES SOBRE EL DESARMADO DE UNA COMPUTADORA

Documente cuidadosamente los siguientes ítems:

Posición de las tarjetas en los distintos slots (el cambiar de posición ciertos tipos de tarjetas puede provocar conflictos de recursos en la configuración de Windows.

Conexiones entre el gabinete y el motherboard (fuente, LEDs indicadores, pulsadores e interruptores, etc.)

Orientación de los flats que salen del motherboard (IDEs, disqueteras, puertos serie, paralelo, etc.), ya que no todos los motherboards tienen claramente marcada cual es la pata 1 de estos conectores, y no siempre disponemos de los manuales, cosa que siempre es importante tratar de obtener.

Tenga un especial cuidado con los discos duros (son particularmente sensibles a los golpes, especialmente en la tapa y del lado del controlador)

Mantenga su mesa de trabajo limpia y ordenada. No se aconseja trabajar sobre fieltro o moquette, por dos motivos: la electricidad estática que pueden generar, y la facilidad que poseen para retener partículas metálicas. La cármica o similares, metal, vinílico, etc., son superficies adecuadas.

Tenga un especial cuidado con los bordes interiores de los gabinetes. Muy a menudo dichos bordes son realmente filosos, pudiendo provocar profundos cortes en muy molestas ubicaciones como yema de dedos o articulaciones de los mismos. Para eliminar los mismos use el canto de un destornillador o una lima tipo cola de ratón.

4.7.8. MATERIALES PARA REALIZAR UN MANTENIMIENTO

ALCOHOL ISOPROPILICO

DESTORNILLADORES

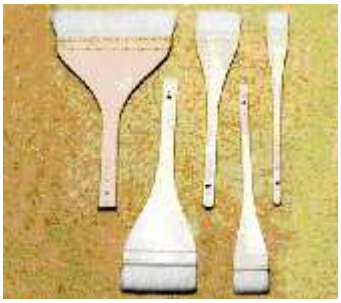
LLAVES DE EXAGONO

PINZA

MULTIMETRO

LINTERNA PEQUEÑA

BROCHA



TRAPO

SOPLADOR

MANILLA ANTIESTATICA

4.7.9. PASOS PARA REALIZAR UN MANTENIENTO

1. Buscar un buen lugar de trabajo.
2. Apagar equipo.

- Desconectar.

3. Abre el equipo.

- Ficha técnica, con los datos reales del equipo.

4. Descargar la energía estática, esto se hace usando una manilla estática o colocando nuestras manos en el piso por 5 segundos.
5. Desconecta componentes, teniendo en cuenta la posición de los cables para evitar percances.
6. Soplo la motherboard, esto se debe hacer a una distancia prudente, no acercar el soplador mucho a la motherboard.
7. Limpio ranuras con el limpia circuitos, este también se le puede echar a la motherboard y ranuras de d.d y c.d para mantener la limpieza.
8. Limpio contactos de tarjetas; las tarjetas tienen en su parte inferior unos contactos, lo podemos notar de color dorado, echamos el alcohol isopropilico en un copito y lo llevamos el mismo a los contactos de las tarjetas limpiando la mugre que se acumula en dichos contactos.
9. Conecto componentes (cables, tarjetas, etc.), como lo habíamos dicho antes, en el lugar donde se encontraban anteriormente.
10. Limpiar carcasa y monitor echando el limpia carcasas en el lugar y frotando con un trapo.
11. Limpiar teclado y Mouse, este también se puede hacer con el limpia carcasas pero echando el limpia carcasas en el trapo y evitando que este último se vuelve un grumo.

4.7.10. FICHA TÉCNICA

Antes de comenzar con el mantenimiento de su máquina, el equipo contenía los siguientes dispositivos:

- MOTHERBOARD_____
- PROCESADOR_____
- COOLER_____
- MODULOS DE MEMORIA RAM_____
- TARJETA DE VIDEO_____
- TARJETA DE RED_____
- MODEM_____
- DISCO DURO_____
- CD ROM_____
- PUERTOS USB_____
- MONITOR_____
- TECLADO_____
- MOUSE_____
- REGULADOR_____
- FORROS_____
- IMPRESORA_____
- SCANER_____
- CAM_____
- MICROFONO_____
- FLOPPY_____
- PARLANTES_____
- CHASIS (CPU)_____
- FUENTE DE PODER_____

- OTROS_____

FIRMA CLIENTE_____

NOTA: La ficha técnica se debe realizar con el propósito de evitar posibles desacuerdos, por ejemplo, la computadora tenía un Mouse óptico y aparece con un Mouse normal (de bolita).

CONCLUSIONES

Básicamente se dio a conocer el funcionamiento de las computadoras, tipos, protocolos a seguir de una red, ya que es muy importante saber cuáles son las necesidades de cualquier persona o empresa que llegue a utilizarlas, ya que son una necesidad para todos, pues todas ellas pueden formar redes enormes (gigantes), y de ellas obtener información, documentos de suma importancia o comunicarse con diferentes personas al mismo tiempo, además de cubrir grandes distancias.

Para todo esto se requiere saber de las necesidades de la computadora y la red en general, en la computadora los tipos de programas que podemos encontrar para poder observar el funcionamiento de la misma y si hay algún virus en ella para que la escanee, si hay virus destruirlo y en dado caso que se necesite obtener un actualización del programa en la red; y para la red, saber cantidad de usuarios o computadoras a conectar, para poder utilizar alguna topología y sus protocolos.

En base a todo esto necesitamos administrar bien nuestra red ya que hay software, la competencia de nuestro negocio (empresas) o personas (hackers), que siempre van a querer destruir nuestra información y documentación esencial para nosotros, administrar es con respecto a proteger, poner contraseñas, además de saber quién, hora y en qué fecha entra en nuestra computadora o red.

Claro para ello es muy importante la seguridad en la computadora, pues como ya se sabe hay muchos y diferentes tipos de virus que pueden dañar nuestro equipo, entonces por consiguiente hay muchos programas de escaneo y protección para que no esté vulnerable nuestra computadora y así poder conectarnos a una red o internet para obtener nuestra información o proteger documentos importantes para nosotros.

Sobre todo para poder tener una mayor y muchísimo mejor seguridad en nuestra red empezando por nuestra computadora es hacer que toda persona o usuario le dé el mejor uso de nuestro sistema, ya que es nuestro trabajo, de él depende el mejoramiento, la eficiencia, que nuestro trabajo se mas rápido y relajado, y con el podemos superarnos en el mismo.

GLOSARIO

100BaseFx: Especificación Fast Ethernet (IEEE 802.3) para fibra óptica en topología estrella.

100BaseTx: Especificación Fast Ethernet (IEEE 802.3) para cable multipar trenzado en topología estrella.

10Base-2: Especificación Ethernet (IEEE 802.3) que utiliza tipo de cable coaxil RG-58 muy económico y probado. Topología en bus.

10Base-5: Especificación Ethernet (IEEE 802.3) que utiliza cable coaxil RG-8 o RG-11, utilizado originalmente en la primeras etapas de desarrollo. Topología en bus.

10Base-FL: Especificación Ethernet (IEEE 802.3) que utiliza fibra óptica en topología en estrella.

10Base-T: Especificación Ethernet (IEEE 802.3) que utiliza cable multipar trenzado en topología estrella.

A

ATM (Asynchronus Transfer Mode): ATM es una tecnología de conmutación y multiplexado de alta velocidad, usada para trasmitir diferentes tipos de tráfico simultáneamente, incluyendo voz, video y datos.

B

Backbone: Enlace troncal usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías.

Bridge: Dispositivo usado para conectar dos redes y hacer que las mismas funcionen como si fueran una. Típicamente se utilizan para dividir una red en redes más pequeñas, para incrementar el rendimiento.

Bus Topology: Topología de Bus: En una topología de Bus cada nodo se conecta a un cable común. No se requiere un hub en una red con topología de bus.

C

Cable Coaxil: Se trata de un cable de cobre rodeado de aislación, un conductor secundario que actúa como ¨ tierra ¨ y una cubierta de plástico externa.

Cable: Conducto que conecta dispositivos de la red entre sí. El tipo de cable a utilizar depende del tamaño de la red y la topología de la misma.

E

Ethernet: Ethernet fue desarrollado en PARC con la participación de Robert Metcalfe fundador de 3Com, es un set de standars para infraestructura de red.

F

Fast Ethernet: Un nuevo estándar de Ethernet que provee velocidad de 100 Megabits por segundo (a diferencia de los 10 megabits por segundo de las redes Ethernet).

FDDI (Fiber Distributed Data Interface): Interfaz de datos distribuidos por fibra óptica . Se trata de una red de 100 Megabits por segundo en topología en estrella o anillo muy utilizada en backbones, hoy desplazada por nuevas tecnologías como ATM.

Firewall: Una computadora que corre un software especial utilizado para prevenir el acceso de usuarios no autorizados a la red. Todo el tráfico de la red debe pasar primero a través de la computadora del firewall.

G

Gateway: Dispositivo utilizado para conectar diferentes tipos de ambientes operativos. Tipicamente se usan para conectar redes LAN a minicomputadores o mainframes.

H

Hub: Concentrador. Dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la red.

I

Internet: Internet se define generalmente como la red de redes mundial. Las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado, TCP/IP (Transmission Control Protocol/ Internet Protocol).

Intranet: Las Intranets son redes corporativas que utilizan los protocolos y herramientas de Internet. Si esta red se encuentra a su vez conectada a Internet, generalmente se la protege mediante firewalls.

L

LAN: Local Area Network o red de área local: Se trata de una red de comunicación de datos geográficamente limitada (no supera por lo general un radio de un kilómetro).

N

Network: (red) Una red de computadoras es un sistema de comunicación de datos que conectar entre si, sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Network Interface Card: Tarjetas adaptadoras ubicadas dentro de las computadoras que especifican el tipo de red a utilizar (Ethernet, FDDI, ATM) y que a través de ellas son el vínculo de conexión entre la computadora y la red.

Network Operating System: Un sistema operativo que incluye programas para comunicarse con otras computadoras a través de una red y compartir recursos.

Nodo: Un dispositivo de la red, generalmente una computadora o una impresora.

P

Par trenzado: Cable similar a los pares telefónicos estándar, que consiste en dos cables aislados "trenzados" entre sí y encapsulados en plástico. Los pares aislados vienen en dos formas: cubiertos y descubiertos.

Protocolo: Un conjunto de reglas formales que describen como se trasmiten los datos, especialmente a través de la red.

R

Repetidor: Un dispositivo que intensifica las señales de la red. Los repetidores se usan cuando el largo total de los cables de la red es más largo que el máximo permitido por el tipo de cable. No en todos los casos se pueden utilizar.

Router – Ruteador: Dispositivo que dirige el tráfico entre redes y que es capaz de determinar los caminos más eficientes, asegurando un alto rendimiento.

S

Server (servidor): Sistema que proporciona recursos (por ejemplo, servidores de archivos, servidores de nombres). In Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

Star Ring Topology – Topología Estrella: En las topologías Star Ring o estrella, los nodos radian desde un hub. El hub o concentrador es diferente dependiendo de la tecnología utilizada Ethernet, FDDI, etc. La mayor ventaja de esta topología es que si un nodo falla, la red continúa funcionando.

Switch: Un dispositivo de red capaz de realizar una serie de tareas de administración, incluyendo el redireccionamiento de los datos.

T

Token ring (red en anillo): Una red en anillo es un tipo de LAN con nodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje.

Topología: La "forma" de la red. Predominan tres tipos de tecnologías: Bus, Estrella y Anillo.

Trascend Networking: Tecnologías de 3Com para la construcción de grandes redes corporativas. Consiste en tres elementos principales, rendimiento escalable, alcance extensible y administración del crecimiento.

W

WAN- Wide Area Network: Red de área amplia: Una red generalmente construida con líneas en serie que se

extiende a distancias mayores a un kilómetro.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

1.- HUERTA, Antonio Villalón. Seguridad en Unix y redes (Versión 2.1)

2.- ALDEGANI, Gustavo Miguel. Seguridad Informática. MP Ediciones. 1° Edición.

3.- McCLURE, Stuart. "hackers Secretos y Soluciones Para la Seguridad en Redes". Editorial McGRAW – HILL.

4.- HERNANDEZ, Claudio. Hackers "los piratas del chip y de internet".

5.- VICTOR A. ARTEAGA SERRANO, "nuestra comunicación vía satélite",Editorial: Libros de México. 1982.

6.- MICHAEL M. A. MIRABITO, "Las nuevas tecnologías de la comunicación"Editorial: Gedisa. 1998.

7.- JOHN R.PIERCE Y A. MICHAEL NOLL, "Señales. La ciencia de la telecomunicaciones", Editorial: Reverté. 1995.

8.- MISCHA SCHWARTZ, "Redes de telecomunicaciones. Protocolos, modelado y análisis", Editorial: Addison-Wesley Iberoamericana, 1994.

9.- JOSE M. CABALLERO, "Redes de banda ancha", Editorial: Alfaomega-marcombo, 2000.

10.- GARY KESSLER Y PETER SOUTHWICK, "RDSI. Conceptos, funcionalidad y servicios", Editorial: McGRAW – HILL, 2001.

11.- ANTONIO CASTRO Y RUBEN JORGE FUSARIO, "TELEINFORMÁTICA para ingenieros en sistemas de información" VOL. 1 y 2, Editorial Reverté, 1999.

12.- ENRIQUE HERRERA PEREZ, "Introducción a las telecomunicaciones modernas", Editorial: Limusa, 1998.

13.- ROSA LORRIO MONTESINOS, "RDSI", 1997. http://www.solocursos.net/rdsi-sickey14243.htm

14.- ANTONIO GOMEZ MELLADO Y LUIS MIGUEL MARÍN TRECHERA, "Servicios RDSI", http://thales.sica.es/rd/Recursos/rd97/Otros/52-3-o-rdsi.html#Servicios

15.- "Introducción a las redes", http://www.saulo.net/pub/redes/a.htm

16.- "Protocolos de RDSI", http://trabajo.us.es/-isabel/publicaciones/tema8.pdf

17.- http://internet- solutions.com.co/ser_fisica_logica.php

18.- http://salvador.edu.ar/molina.htm#Niveles de Seguridad

19.- Trabajo sobre DELITO INFORMÁTICOS desde la Universidad de El Salvador, Octubre 2000 (PDF) http://www.e-libro.net/E-libro -viejo/gratis/delitoninf.pdf

20.- http://delitosinformaticos.com/trbajos/hackcrack.pdf

21.-www.angelfire.com/ga/metalsystem/ terminología_tecnica_del_hacker.html

22.- http://cfbsoft.iespana.es/cfbsoft_es/seguridad/

23.- http://www.el-hacker.com/foro/index.php/topic,24010.0.html

24.- www.caece.edu.ar/cursos/docs/

25.- Revista red “la seguridad en manos de otros”, julio 2004, pag. 6

26.- Dr. Iván Seperiza Pasquali LOS VIRUS INFORMÁTICOS, ELECTRÓNICOS O COMPUTACIONALES. http://isp2002.co.cl/virus.htm

27.- MARTINEZ, Oscar. “VIRUS INFORMÁTICOS”, http://www.geocities.com/ogmg.rm/

28.- http://zonavirus.com/datos/articulos/167/tipos_Virus.asp

29.- http://mundopc.net/cursos/virus/virus13.php

30.- Seguridad en centros de cómputo. Políticas y procedimientos. Editorial Trillas.

31.- http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO/SITIOS.htm

32.- http://seguridad.lci.ulsa.mx/POLITICAS_DE_SEGURIDAD_Alberto_Basalo.doc

33.- www.hackemate.com.ar/tools/

34.- http://www.delitosinformaticos.com/especial/seguridad/pgp.shtml

35.- http://www.microsoft.com/spain/windowsxp

36.- Digital Communications. Jonh G. Proakis, 4° Edicion, Editorilal: McGRAW –HILL