CAPÍTULO I

1. REDES Y CABLEADO ESTRUCTURADO

El Capítulo 1, "Sistema de Cableado Estructurado", enfoca una introducción y definición del sistema propuesto, indicando los sistemas de cableado que se han venido empleando hasta la actualidad, analizando las ventajas de la utilización de cableado estructurado respecto a los sistemas de cableado tradicionales. Adicionalmente se profundiza en los subsistemas que forman parte del sistema completo de cableado estructurado con un estudio de las normas y estándares vigentes a nivel internacional.

También se trata "La Administración básica y Seguridad de la red", su definición, tipos de ataques a la red, firewalls, proxy y algunos aspectos generales de la misma.

1.1. REDES

1.1.1. Definición

"Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información." [1]

1.1.2. Beneficios

- ☑ Brinda una alta fiabilidad, al contar con fuentes alternativas de suministro. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo.

- ☑ Proporciona un medio de comunicación entre personas que se encuentran muy alejadas entre sí.

- ☑ Las redes se han convertido en una herramienta fundamental para las instituciones y empresas, las transacciones de operaciones son mayores y requieren de mayor agilidad y confiabilidad.

[1] Gibbs Mark, "Redes Para Todos", 2da Edición, México, 1995

1.1.3. Protocolos de Red

Definición

"Permite establecer una comunicación entre varios equipos o dispositivos, ya que estos equipos pueden ser diferentes entre sí." [2]

Por la diversidad de los protocolos existentes, para la presente investigación se ha partido desde los protocolos TCP/IP:

TCP/IP: Son los protocolos más importantes y comunes, utilizados por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí." [3]

A continuación se detallan algunas características del protocolo antes mencionado:

- ☑ Este tiene la operación de dividir al mensaje, enviándolo en pequeños paquetes que son numerados y luego trasladados por diferentes partes de la red.

- ☑ Es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

[2] Gibbs Mark, "Redes Para Todos", 2da Edición, México, 1995
[3] Comer Douglas, "Redes Globales de Información con Internet y TCP/IP", México, 1996

☑ Es el protocolo de comunicación más general que existe y se encarga de que la comunicación entre todos sea posible.

Tipos de Protocolos TCP/IP

De acuerdo a las necesidades de las autoras se llegó a determinar la importancia de los siguientes protocolos:

☑ **Protocolo TCP:** TCP es un protocolo "orientado a la conexión" que provee mecanismos confiables para la transmisión de paquetes.

☑ **Protocolo de Internet (IP):** Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos.

☑ **Protocolo DNS (Servicio de Nombres y Dominios):** Es un conjunto de protocolos y servicios sobre una red TCP/IP, permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos, en vez de memorizar y usar sus direcciones IP.

☑ **Protocolo SNMP (Protocolo de Gestión de Red Simple):** Se utiliza para administrar múltiples redes físicas de diferentes fabricantes.

☑ **Protocolo NFS (Sistema de Archivos de Red):** Es un sistema de archivos cliente - servidor distribuido, por medio de este los usuarios pueden compartir sus computadoras con otros usuarios.

- ☑ **Protocolo FTP (Protocolo de Transferencia de Archivos):** Permite copiar archivos entre computadoras.

- ☑ **Protocolo SMTP (Protocolo de Transferencia de Mensajes Simple):** Es un protocolo de servicio de correo electrónico, listas de correo, etc. y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP.

- ☑ **Protocolo POP3 (Protocolo de Correo):** Permite leer mensajes de correo electrónico que estén en una casilla de correo del server, permite ciertos manejos básicos, como borrar los mensajes, ver la cantidad y el tamaño de los mensajes antes de leerlos, entre otros.

- ☑ **Protocolo UDP (Protocolo de Datagramas del Usuario):** Se usa para programas que sólo envían mensajes cortos pero no confiables, y pueden reenviar el mensaje si una respuesta no se produce en un período corto de tiempo. Se utiliza en vez del TCP en algunas aplicaciones.

- ☑ **Protocolo DHCP (Protocolo de Configuración Dinámica del Host):** Sirve para configurar parámetros (dirección IP, DNS, Gateway, etc.) de las computadoras en forma dinámica.

1.1.4. Servicios de Redes

Existen muchos servicios de redes pero a continuación se clasifica a los mismos de acuerdo a su importancia:

a. **Servicios de Archivos:** Este tipo de servicios incluyen varias aplicaciones, diseñadas para: almacenar, recuperar, trasladar datos de forma eficaz, realizan funciones de lectura, escritura, control de acceso y gestión de datos.

b. **Servicios de Impresión:** Son aplicaciones de la red que controlan y gestionan el acceso a las impresoras y a los equipos de fax. Estos servicios aceptan las solicitudes de tareas de impresión, interpretan los formatos de las tareas y las configuraciones de impresora.

c. **Servicios de Mensajes:** Los servicios de mensajes incluyen el almacenamiento, acceso y entrega de textos, binarios, gráficos, videos digitalizados y audios, estos servicios tratan de forma activa con las interacciones de comunicación entre los usuarios de computadoras, las aplicaciones de usuario, las aplicaciones de red o los documentos.

d. **Servicios de Aplicaciones:** Son servicios de red que ejecutan software para los clientes de la red; permiten a las computadoras compartir la potencia de procesamiento en lugar de simplemente compartir datos.

e. **Servicios de Base de Datos:** Proporcionan un almacenamiento o recuperación de base de datos basadas en el servidor que permitan a los clientes controlar la manipulación y presentación de datos.

1.1.5. Tecnologías de Redes

Hay diferentes tipos de tecnologías, pero para la presente investigación se van a analizar las más accesibles para la Institución.

Tabla 1.1 Características de las Tecnologías de redes

	Tecnologías de red		
	Ethernet	**Fast Ethernet**	**ATM**
Características	Velocidad de 10Mbps.	Velocidad de 100Mbps	Velocidad de 155,52 Mbps, la alternativa 622,08 Mbps
	Los datos pueden moverse entre Ethernet y Fast Ethernet sin traducción protocolar.	Soporta tanto a las aplicaciones de Ethernet como a las de token ring	Integra Lan y Wan
	Equipos relativamente económicos.	Ofrece un fuerte soporte para multimedia	Mejora la eficiencia y manejabilidad de la red
	Utiliza el protocolo CSMA/CD.	Utiliza el protocolo CSMA/CD	Transporta aplicaciones multimedia en tiempo real que combinen voz, video y datos.
	Limitaciones Topológicas.	Diseño y Configuración muy sencilla	Es compleja en la construcción de sus redes
	A medida que crece el Número de nodos instalados se congestiona la red.	Requiere de nuevas tarjetas adaptadoras hubs y switches	Los adaptadores para ATM son mucho más caros que los de 100BaseT
	Tipos: 10 Base 5, 10 Base 2, 10 Base T, 10 Base FL **(ver anexo2).**	Tipos: 100 Base-TX, 100 Base-T4, 100 Base-FX **(ver anexo 2).**	----------

Fuente: Grupo Investigador

Realizado por: Grupo Investigador

1.1.6. Intranet

Definición

"Una Intranet es una aplicación de tecnologías de Internet a las redes corporativas de área amplia (WAN) y de área local (LAN) de su empresa para tener acceso a la información con facilidad, rápida actualización y una administración de recursos sencilla".[4]

Características

Entre las características más importantes de un sistema de cableado estructurado destacan las siguientes:

- ☑ Menor tiempo de búsqueda y consulta de información.
- ☑ Ahorro en espacio y almacenamiento de documentos impresos.
- ☑ Eficiente manejo de información.
- ☑ Reduce costos en computadoras, programas y mantenimiento.

1.2. CABLEADO ESTRUCTURADO

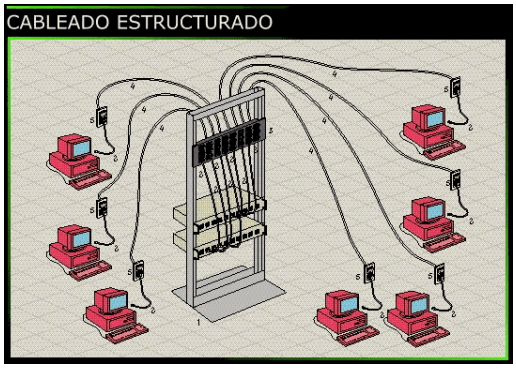
1.2.1. Definición

"Un sistema de cableado estructurado en LAN consiste en una infraestructura flexible de cables que puede aceptar y soportar sistemas de computación y de

[4] Servati AI, Bremner Lyn, "La Biblia de Intranet", México, 1998

teléfono múltiples, cada estación de trabajo se conecta a un punto central utilizando una topología tipo estrella, facilitando la interconexión y la administración del sistema.” [5]

Figura 1.1: Cableado Estructurado



Fuente: Daza Ramírez Farley

Realizado por: Grupo Investigador

1.2.2. Características:

Entre las características generales de un sistema de cableado estructurado se detallan las siguientes:

- ☑ Soporta múltiples ambientes de cómputo:
  - ☑ LAN’s (Ethernet, Fast Ethernet, Token-ring, Arcnet, FDDI/TP-PMD).
  - ☑ Datos discretos (Mainframes, minicomputadoras).
  - ☑ Voz/Datos integrados (PBX, Centrex, ISDN).
  - ☑ Video (señales en banda base, Ej. seguridad de edificios; señales en banda amplia, ej.: TV en escritorio).

[5] Lino Carrillo José, http://www.fm.uach.mx, 2003

- ☑ Simplifica las tareas de administración, minimizando las posibilidades de alteración del cableado.

- ☑ Efectivo en costo. Gracias a que no existe la necesidad de efectuar cableados complementarios, se evita la pérdida de tiempo y el deterioro de la productividad.

1.2.3. Componentes de Cableado Estructurado

- ☑ **Switches:** Son muy similares a los hubs, solo que no se comparte el ancho de banda. Un switch mediante memoria no volátil, permite que cada uno de sus puertos posea su propio ancho de banda.

- ☑ **Charola:** Es un conjunto integral junto con los rack ya que sirven de soporte para diferentes componentes, tales como: patch panel, concentradores, regletas, switch.

- ☑ **Panel de conexión / Patch Panel**: Es un medio de uso flexible y económico de interconectar entre el cableado vertical y el horizontal. Están formados por un soporte metálico y de medidas compatibles con rack de 19’.

- ☑ **Frente para Keystone / tapas / Faceplate:** Esta formada de un pieza plástica plana de soporte que es tapa de una caja estándar de electricidad

embutida de 5 x 10 cm. y permite encastrar hasta 2 keystone, formando un conjunto de conexión de hasta 2 bocas.

☑ **Patch Cord:** Están construidos con cable UTP de 4 pares flexible terminado en un plug 8P8C en cada punta de modo de permitir la conexión de los 4 pares en un conector RJ45.

☑ **Keystone/Jack Modular (Hembra RJ45):** Es un dispositivo modular de conexión monolínea, hembra, apto para conectar plug RJ45, que permite su inserción en rosetas y frentes de patch panels.

☑ **Roseta/Keystone:** Es una pieza plástica de soporte que se amura a la pared y permite encastrar hasta 2 Keystone, formando una roseta de hasta 2 bocas.

☑ **Organizadores:** Se utiliza para darle una organización en la distribución de cables en los racks. Estos organizadores están diseñados para poder organizar los cables tanto por la parte delantera como por la parte posterior del rack. Su diseño es muy compacto y las cubiertas pueden ser removidas para agregar o extraer cables fácilmente. Disponibles en color negro.

☑ **Cable UTP Sólido:** Posee 4 pares bien trenzados entre sí, sin foil de aluminio de blindaje, envuelto dentro de una cubierta de PVC. Es muy importante utilizar PC certificados a Nivel 5.

☑ **RACK de Pared o Piso:** Componente del cableado estructurado muy importante ya que soportan las charolas, junto con los componentes mencionados anteriormente.

☑ **Gabinetes / Armarios / Closet:** Permiten resguardar todos los componentes que se encuentran integrados en el rack.

☑ **Canaletas:** Las canaletas son accesorios muy importantes por los que debe cruzar el cableado, sea horizontal como vertical. El tamaño de las canaletas difiere de acuerdo a la cantidad de cables que pasan de un patch panel a otro.

☑ **Ponchadora:** Permite la conexión de blocks en el caso blocks 110 la herramienta es de doble acción, inserta y corta el cable. Las hojillas de estas herramientas están hechas de acero. Además pueden ser reemplazadas fácilmente, posee un disco giratorio para controlar la fuerza de impacto.

☑ **Crimpiadora:** Permite cortar el cable pelarlo y apretar el conector para fijar los hilos flexibles de cable a los contactos RJ45, RJ11. Puede ser utilizado para 4P-6P-6PDEC-8P-10P para cable sólido y trenzado. Fabricado de metal y mango recubierto con plástico.

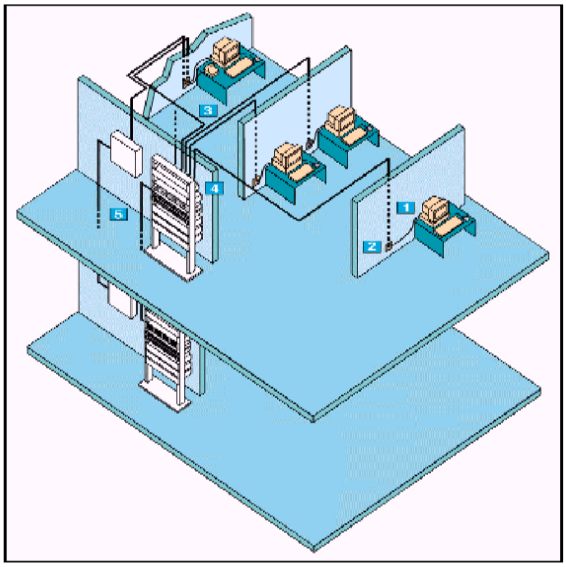
☑ **Comprobador/LAN TESTER:** Permite detectar fácilmente cables cortados o en cortocircuito, cables corridos de posición, piernas invertidas,

ideal para controlar cableados (no para certificar) por parte del técnico instalador de bajo costo y fácil manejo.

1.2.4. Estudios de los Subsistemas de Cableado Estructurado

A continuación se presenta los subsistemas que existen dentro de cableado estructurado: [6]

Figura 1.2: Subsistemas de Cableado Estructurado



Fuente: Martín Luis M.

Realizado por: Grupo Investigador

a. Cableado Horizontal: Incorpora el sistema de cableado que se extiende desde la salida de área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones.

[6] Lino Carrillo José, http://www.fm.uach.mx, 2003

b. **Cableado Vertical o BackBone:** Proporciona interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipo y cuartos de telecomunicaciones; incluye la conexión vertical entre pisos en edificios de varios pisos, medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

c. **Cuarto de Telecomunicaciones:** El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones, debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones.

d. **Cuarto de Equipo:** Es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen.

e. **Cuarto de Entrada del Edificio:** Consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto o espacio de entrada, puede

incorporar el "backbone" que conecta a otros edificios en situaciones de campus.

f. Área de Trabajo: Comprende las inmediaciones físicas de trabajo habitual (mesa, silla, teléfonos, ordenadores, zona de movilidad, etc.) del o de los usuarios. El punto que marca su comienzo en lo que se refiere a cableado es la roseta o punto de conexión.

1.2.5. Normas y Estándares Internacionales para Cableado Estructurado

Aquí se detallan los estándares y normas internacionales utilizadas por las autoras para el diseño e implementación de un sistema de cableado estructurado:

- ☑ **TIA/EIA-568 A.-** Cableado Estándar de Telecomunicaciones para Edificios Comerciales.
- ☑ **TIA/EIA-569.-** Estándar para Edificios Comerciales Rutas y Espacios (ductos y canalizaciones).
- ☑ **ANSI/TIA/EIA-570.-** Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Liviano.
- ☑ **TIA/EIA-606.-** Estándar de Administración para la infraestructura de telecomunicaciones en edificios comerciales.
- ☑ **TIA/EIA - TSB-67.-** Define las características de los aparatos de test portátiles destinados a la certificación de las instalaciones.

- ☑ **ANSI/TIA/EIA-607.-** Requerimientos para Telecomunicaciones de Puesta a Tierra y protección para telecomunicaciones en edificios comerciales.
- ☑ **TIA/EIA-TSB36A.-** Cables con pares trenzados 100W UTP y FTP.
- ☑ **TIA/EIA-TSB40A.-** Conector RJ45, empalmes por contactos CAD.
- ☑ **TIA/EIA-TSB 53.-** Cables blindados 150W y conector hermafrodita.
- ☑ **ISO/IEC 11801**.- Esta norma especifica un cableado genérico para uso en edificios comerciales que puede comprender uno o más edificios en un campus.

1.3. ASPECTOS GENERALES DE LA SEGURIDAD EN LA RED.

1.3.1. Seguridad en la Red

"Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado." [7]

Aspectos Principales de la Seguridad

Hay tres aspectos cuando se habla de la seguridad en una red de datos:

a. Vulnerabilidad: Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

[7] http://www.softdownload.com.ar, 2003

b. Amenaza: Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

c. Contramedida: Técnicas de protección del sistema contra las amenazas.

1.3.2. Debilidades del Sistema Informático

"Los tres primeros puntos conforman el llamado Triángulo de Debilidades del Sistema y son los principales elementos que se deben proteger en un sistema informático:" [8]

☑ **Hardware**: Conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado o tarjetas de red.

☑ **Software**: Sustracción de programas, modificación, ejecución errónea, defectos en llamadas al sistema, etc.

☑ **Datos:** Alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

☑ **Memoria**: Introducción de virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.

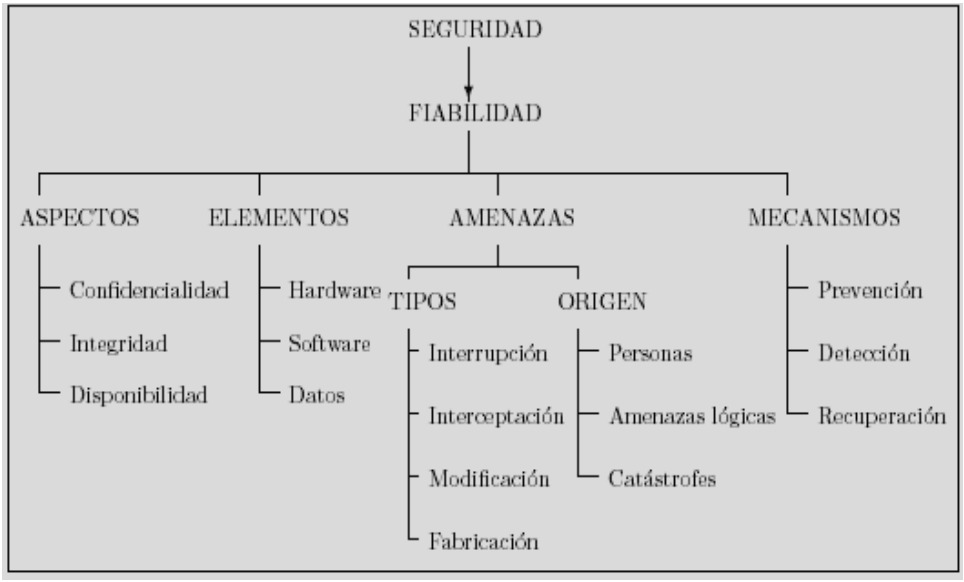
[8] Dr. Aguirre Jorge Ramió, Universidad Politécnica de Madrid , 2003

☑ **Usuarios**: Suplantación de identidad, acceso no autorizado, visualización de datos confidenciales, etc.

1.3.3. Tipos de Ataques y Seguridades

Habitualmente los datos constituyen el principal elemento a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar; sobre estos se pueden realizar multitud de ataques. Estos se pueden dividir en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación.

Figura 1.3: Visión global de la seguridad informática



Fuente: Grupo Investigador

Realizado por: Grupo Investigador

A continuación se da a conocer los principales ataques que se dan a una red informática:

a. **Herramientas de seguridad:** Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso la puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

b. **Diccionarios:** Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números encriptados, incluso con caracteres especiales hasta descubrir la combinación correcta de nombre y usuario de la víctima. Pues son programas de fuerza bruta.

c. **Puertas traseras:** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es usual entre los programadores insertar ‘atajos’ en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando; con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.

d. **Bombas lógicas:** Son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo una determinada fecha.

e. **Virus:** Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado *huésped*), de forma que cuando el archivo se

ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

f. Gusanos: Un gusano es un programa capaz de ejecutarse y propagarse por si mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

g. Caballos de Troya: Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.

h. Programas conejo o bacterias: Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.), produciendo una negación de servicio.

1.3.4. Métodos de Protección

Las políticas son el primer paso que dispone una Institución para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que

permite detener un posible ataque antes de que este suceda. A continuación se citan algunos de los métodos de protección más comúnmente empleados:

a. **Sistema de detección de intrusos:** Permiten analizar los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de información con la que han sido previamente alimentados.

b. **Sistemas orientados a conexión de red:** Monitorizan las conexiones que se intentan establecer en una red o equipo en particular. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alertar al administrador. En esta categoría están los cortafuegos y Wrappers (programa que controla acceso a un segundo programa).

c. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La “desventaja” de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

d. **Sistema de protección a la integridad de información:** sistemas que mediante criptografía (técnica de escritura tal que la información esté oculta de intrusos no autorizados) o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.

e. **Sistemas de protección a la privacidad de la información:** Herramientas que utilizan criptografía para asegurar que la información solo sea visible para quién tiene autorización. Dentro de este tipo de Herramientas se puede citar a Secure Sockets Layer (SSL.- Protocolo seguro de Internet) y los Certificados Digitales.

1.3.5. Tipos de Atacantes

a. **Pasivos:** Los atacantes pasivos son aquellos que fisgonean por el sistema pero no lo modifican o lo destruyen y los más importantes son:

- ☑ **Curiosos:** Son los atacantes más habituales de un sistema en red; personas que intentan conseguir mayor privilegio del que tienen o intentan acceder a sistemas a los que oficialmente no tienen permiso.

- ☑ **Crackers:** Es un programador experto que puede descifrar cualquier clase de programa y crear sus propios programas para desempaquetar otros.

- ☑ **Intrusos remunerados:** Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la entidad afectada.

b. **Activos:** Los atacantes activos son aquellos que dañan el objetivo atacado, o lo modifican en su favor y los más peligrosos se citan a continuación:

- ☑ **Terroristas:** Persona que ataca al sistema simplemente por causar algún tipo de daño en éste, es decir se puede intentar borrar las bases de datos, destruir los sistemas de ficheros de un servidor que alberga páginas *web*, etc.

- ☑ **Hacker:** Es él más peligroso de todos, porque puede entrar a cualquier parte de la red, son expertos en la programación y manejo del lenguaje UNIX, que es en lo que están basados los sistemas operativos de los servidores de una red.

- ☑ **Ex-empleados:** Generalmente, se trata de personas descontentas con la institución que aprovechan debilidades de un sistema que conocen perfectamente para dañarlo; pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran para la institución y dañarlo de la forma que deseen.

1.3.6. Firewall (Muros de Fuego)

"Un Firewall es un dispositivo que protege una red privada del resto de la red. La misión de los muros de fuego de Internet es garantizar la seguridad de nuestro equipo ante los peligros cibernéticos de la red del área local (LAN) o bien, mantener a los miembros de esa LAN al margen de las malignas intenciones de Internet." [9]

[9] Rodríguez G. Jorge E., Introducción a las Redes de Área Local, México, c1996

Los Firewall se utilizan con dos objetivos:

- ☑ Denegar el acceso a los piratas y gusanos.
- ☑ Permitir el acceso a empleados, niños autorizados, etc.

Para saber en donde ubicar un muro de fuego primeramente se tiene que:

- ☑ Indicar cuales son los servicios que usted necesita.
- ☑ Especificar el grupo de personas que necesitan esos servicios.
- ☑ Describir cuales de los servicios requiere cada grupo acceder.
- ☑ Por cada grupo se tiene que indicar como el servicio deberá ser mantenido seguro.
- ☑ Todas las otras formas de accesos serían una violación.

Figura 1.4: Forma de funcionamiento de un Firewall

Fuente: Global PCNet S.A. de C.V.

Realizado por: Grupo Investigador

1.3.7. Proxy

"Un Proxy es un programa que permite o niega el acceso a una aplicación determinada entre dos redes. Los clientes proxy se comunican sólo con los servidores proxy, que autorizan las peticiones y las envían a los servidores reales, o deniegan y las devuelven a quien las solicitó." [10]

1.3.8. Recomendaciones Generales en la Seguridad

- ☑ Comprobar periódicamente el nivel de seguridad con el que se esta conectado (scan de puertos, antivirus, firewall, datos sensibles en la configuración de cuentas).
- ☑ Realizar periódicamente copias de seguridad de los datos.
- ☑ Tener especialmente cuidado cuando se descargue software de sitios dudosos.
- ☑ Instalar y tener siempre activo un Antivirus y, por supuesto, actualizarlo periódicamente.
- ☑ Instalar un firewall y estar atento a las actualizaciones.
- ☑ Configurar en principio cualquier programa, y en especial el navegador de Internet, en el nivel más alto de seguridad que permita.
- ☑ No elegir claves de menos de seis caracteres, y combinar mayúsculas, minúsculas, números, signos de puntuación o cualquier cosa que nos permita el teclado.

[10] Rodríguez G. Jorge E., Introducción a las Redes de Área Local, México, c1996

- ☑ Realizar normas y políticas de seguridad interna en la organización y distribuirlas al personal de la misma.
- ☑ No apuntar claves ni compartirlas con otras personas.
- ☑ No utilizar contraseña de acceso en otros sistemas, especialmente juegos en red o equipos Windows.
- ☑ Nunca ejecutar programas que nos envíen por correo o que se consiga a partir de fuentes poco fiables (como un 'amigo').
- ☑ Ante cualquier actividad sospechosa que se detecte es recomendable ponerse en contacto con el responsable de seguridad o el administrador, a ser posible por teléfono o en persona.

1.4. ADMINISTRACIÓN DE LA SEGURIDAD PARA GRUPOS Y USUARIOS

1.4.1. Administración de la Red

Una gran cantidad de estaciones de trabajo necesita de la administración de redes para manejar y controlar las redes y los componentes asociados al hardware y al software.

Tipos de Modelos

Con la llegada de las LANs (Local Area Network) existen dos modelos de redes de computadoras:

a. **Modelo Cliente – Servidor:** Un cliente requiere un servicio de un servidor que está preparado para proporcionar dichos servicios a los clientes que lo necesitan.

b. **Modelo Peer–to–Peer:** No existen roles fijos como cliente y servidor, cualquier computadora puede, en un determinado momento, ser un cliente o un servidor.

Objetivos de la Administración de Red

Existen un sin número de objetivos pero a continuación se citan los más importantes según el criterio de las autoras:

- ☑ Tener Alta disponibilidad de la red
- ☑ Reducir costos operacionales de red
- ☑ Reducir cuellos de botella en la red
- ☑ Incrementar flexibilidad de operación e Integración
- ☑ Incrementar eficiencia
- ☑ Facilitar el uso de la red
- ☑ Poseer seguridad en la información.

1.4.2. Herramientas de Administración

"Las herramientas de administración de red normalmente dependen de agentes SNMP (Protocolo de Gestión de Red Simple) que se ejecutan en estos

dispositivos y ofrecen información a la consola de administración o al servidor. Sin embargo, pocas de estas herramientas ofrecen información sobre el nivel de servicios de la red; en su lugar, dependen de otros productos o empresas." [11]

"Windows XP Profesional posee algunas herramientas que facilitan el uso de una interfaz estándar para la configuración, administración, y alguna supervisión de los servicios de red. Entre los servicios se incluyen DHCP, WINS, y DNS. Algunas de las novedades que incorporará Windows XP son los estándares IP Security (IPSec) para la autentificación, integridad, y encriptación de tráfico a nivel de red, y soporte QoS (Quality of Service) dentro de la pila de red y el Directorio Activo." [12]

a. DNS: El Sistema de Dominio de Nombres es básicamente una base de datos distribuida de computadoras que forman parte de una red. Esto facilita el control local de la totalidad de segmentos de la base de datos, lo que permite que cada segmento esté disponible a través de la red por un esquema de cliente – servidor.

[11] Rodríguez G. Jorge E., Introducción a las Redes de Área Local, México, c1996
[12] http://www.windowstimag.com, 2003

b. QoS (Quality of Service**). –** Es una forma de garantizar el ancho de banda disponible por conexión, y normalmente se asocia con aplicaciones multimedia o con aplicaciones que requieren una entrega en tiempo real.

c. IPSec. – Le permite especificar la autentificación y encriptación de la comunicación de red entre un conjunto de dispositivos definidos de red para asegurar la privacidad.

1.4.3. Funciones de la Administración

Tomando en cuenta la importancia de la administración la misma se subdivide en las siguientes funciones: [13]

a. Administración de datos: Las funciones de Administración aseguran que los datos de las personas (como archivos y documentos personales) sean accesibles fácilmente, estén disponibles rápidamente y siempre protegidos, para que de esta manera los usuarios puedan acceder a sus datos desde cualquier máquina ya sea que se conecten, o se encuentren en línea o fuera de línea.

b. Accesibilidad de los datos: Los datos pueden seguir a una persona cuando la persona se mueve a otro computador en la red. Esto proporciona una mayor accesibilidad ya que las personas pueden utilizar cualquier máquina en la red para acceder a sus datos.

[13] http://www.evidalia.com, 2004

c. **Disponibilidad de los datos:** Las funciones de Administración aseguran que los datos de las personas residan tanto en el computador local como en el servidor. La memoria caché local mantiene datos en el computador local aún cuando esté desconectada de la red y que los datos estén disponibles para las personas incluso cuando trabajen fuera de línea.

d. **Protección de los datos:** Los administradores pueden dar una protección mejorada de los datos del usuario al asegurar que la información del mismo, este protegida a través del respaldo manejado por el administrador de servidores de red.

1.4.4. Normas y políticas de utilización de la red

a. Normas de Uso

☑ El uso de un código es estrictamente personal. Bajo ninguna circunstancia un usuario debe permitir que su código sea empleado en actividades fuera de su control directo.

b. Políticas Específicas

☑ Los servicios deben usarse para fines académicos y de investigación: No debe usarse la red para uso personal o ajeno a tales fines.

☑ No se permite la transmisión de archivos demasiado grandes. Si es necesario, un archivo o documento será particionado en segmentos, ya que mediante esta norma se pretende evitar saturaciones en la red.

☑ El uso de mensajes interactivos debe ser discreto. No se recomienda hacer uso frecuente de estos mensajes, ya que pueden causar congestiones en los servicios de la red.

☑ No debe usarse el sistema en forma inútil, enviando mensajes o archivos sin sentido práctico; además se evitará la violación de ciertos lineamientos generales en el uso de Internet en referencia a las restricciones que existen a correos masivos, piratería o plagios y copias de software.

☑ Es responsabilidad de cada usuario colaborar para que los servicios de la red mantengan un buen desempeño y poner en conocimiento al administrador de la misma en su institución según corresponda, de las situaciones irregulares o problemas que detecte.

☑ El usuario debe proteger la seguridad de su cuenta. Se le dará carácter de privada y confidencial a la contraseña o Password y que en lo posible no será compartida con terceras personas.

c. Políticas Generales

☑ Cada miembro que se incorpore a la red como usuario de sus servicios, debe acogerse a las políticas de la misma; enmarcando su participación dentro del espíritu de cooperación y desempeño.

☑ Todo el personal que utilice los servicios de la red deberá conocer las normas sobre su uso. La ignorancia de las mismas no exonerará de las responsabilidades asignadas.

☑ Las autoridades académicas, administrativas y de manera específica el Rectorado de la Unidad Educativa deberán difundir estas políticas entre los usuarios de los recursos y bienes informáticos.

d. Política de Funcionamiento

Cuando se necesite hacer uso de algún recurso que requiera de un ancho de banda fuera de proporción en relación con el ancho de banda utilizado por la red y que por consiguiente afecta en forma significativa a todos los usuarios de la misma, se debe coordinar con la administración a fin de asignar un horario específico que ayude a obtener el mejor desempeño posible de dicho recurso.