UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

"ACATLAN"

SEGURIDAD INFORMATICA EN LA RED DEL INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES.

T E S I S

QUE PARA OBTENER EL TITULO DE:

LICENCIATURA EN MATEMATICAS APLICADAS Y COMPUTACION

P R E S E N T A :

LUZ MARIA GARCIA ROMERO

ASESOR: M. EN C. SARA CAMACHO CANCINO.

UNAM
CAMPUS ACATLÁN

ACATLAN, ESTADO DE MEXICO. 1998

A mis padres por su gran apoyo cariño y comprensión:

MARGARITA ROMERO PINEDA

CRESCENCIANO GARCÍA GARCÍA

A mi hermano por ser mas que eso un amigo:

Dr. JOSÉ ANTONIO GARCÍA ROMERO

A un gran ser humano por su apoyo:

M. en C. JUAN CARMONA LEMUS

A mis familiares por su cariño y en especial a mi abuelita acaecida:

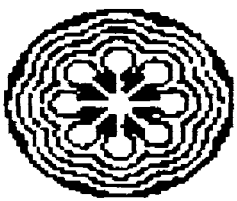
Carmen Pineda Díaz

A todos mis maestros y compañeros de la Universidad

A mis amigos por su alegría.

AGRADECIMIENTOS

A la **UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO** y en especial a la **Escuela Nacional de Estudios Profesionales " Acatlan "** por haberme brindado la oportunidad de obtener una excelente formación profesional.



ININ

Al **Instituto Nacional de Investigaciones Nucleares (ININ)**, y en especial al la **Gerencia de Informática, Departamento de Teleinformática** por el apoyo económico otorgado y la facilidad para utilizar sus instalaciones y equipo durante la elaboración de este trabajo.

A todos los profesores que dejaron en mi, una parte de sus conocimientos y que sin ellos nunca hubiera alcanzado esta meta.

A mis asesores:

M. en C. SARA CAMACHO CANCINO
M. en C. SALVADOR VIQUEZ CANO

por haberme brindado primeramente sus conocimientos y después haber asesorado este trabajo.

A los que me apoyaron con su amistad y conocimientos para desarrollar, mejorar y concluir el presente trabajo.

ING. LUCIA MENDOZA IÑIGUEZ
M. en C. JUAN CARMONA LEMUS
ING. JOSE LUIS CASTILLO ROMERO

SEGURIDAD INFORMÁTICA EN LA RED DEL INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES

Luz María García Romero[*] y M. en C. Salvador Viquez Cano[**]

Gerencia de Informática,
Departamento de Teleinformática,
Instituto Nacional de Investigaciones Nucleares.
Carretera Mexico-Toluca Km. 36.5, Ocoyoacac Estado de México.

R E S U M E N :

El presente trabajo describe una metodología en base a directrices para la red metropolitana del Instituto Nacional de Investigaciones Nucleares (ININ). Partimos por definir y describir aspectos básicos de redes, abarcando desde el surgimiento de bases de datos, hasta los distintos tipos de redes y lo que cada una de ellas implica (tanto en hardware como en software) para su interconectividad. Todo esto con el propósito de definir conceptos y propuestas de seguridad, mediante una buena administración de los recursos, el establecimiento de claras políticas de seguridad y detección de amenazas en cada parte que integra la red.

Además, se realiza un análisis de seguridad detectando los sitios de riesgo, se estudian cuales son las amenazas para cada uno de ellos, se determina la vulnerabilidad que corre cada sitio que conforma la red del ININ, y de acuerdo a ello se plantean contramedidas para cada amenaza, para que por último se engloben de manera general, los servicios que de seguridad se requieren y se deban implementar de acuerdo a las necesidades en la red del ININ.

---

[*] Pasante de licenciatura de la UNAM.
[**] Jefe del Depto. de Teleinformática

INDICE

LISTA DE ILUSTRACIONES

Ilustración **Página**

LISTA DE TABLAS

TABLA **Página**

INTRODUCCIÓN

Debido al auge que ha tenido el avance de la tecnología, la necesidad de manejar equipos con mayor capacidad y más aún el hecho de comunicarse, intercambiar opiniones, conocer y dar a conocer al mundo los avances en los distintos ámbitos ha provocado una inquietud, ¿cómo evitar que la información sea manipulada por quienes logren acceso a dicha información?. Distintas organizaciones han investigado y desarrollado múltiples formas de asegurar que la información no pierda su integridad así como eliminar el riesgo de perderla o ser accedida por personas no autorizadas.

"El Instituto Nacional de Investigaciones Nucleares (ININ) nació el 26 de enero de 1979. La misión del ININ es contribuir como Laboratorio Nacional a la investigación y desarrollo de las ciencias nucleares y sus aplicaciones, realizando investigación de excelencia y proporcionando servicios de calidad, además de contribuir a la formación de investigadores de alto nivel"[1].

Sus investigaciones y desarrollos requieren de equipos con altos recursos para lo cual mantienen una área de cómputo en la Gerencia de Informática con equipos de excelente nivel, tales como equipos Silicon Graphics, Impact's, Origin 2000, IBM y equipos PC distribuidos a todo el personal que lo requiere, todo esto conectado a 6.2 km. de cable de fibra óptica, cableado estructurado y enlace satelital punto a punto con la UNAM como nodo de Internet.

En sus grandes logros a causa de investigaciones reconocidas a nivel mundial el ININ maneja información confidencial e invaluable, por ello la Gerencia de Informática ha iniciado un proyecto de seguridad informática que proteja la información que se transfiera Intranet y mediante Internet, lo cual fue el origen del trabajo en cuestión.

El trabajo se encuentra estructurado en cuatro capítulos:

En el capítulo 1 se hace referencia a los primeros sistemas computacionales que dieron origen a las redes, de ahí su división en redes de área local, metropolitana y extendida, después, se hace referencia a los medios de conexión que existen y se explican algunas topologías y medios de interconectividad.

En el capítulo 2 se plantea la importancia que tiene una buena selección del hardware y software que integrará la red, el tomar en cuenta tanto los objetivos, la estructura y

[1]WEB: http://www.inin.mx. Instituto Nacional de Investigaciones Nucleares. 1997

necesidades para su mejor funcionamiento y aprovechamiento en la red, además se muestran algunos ambientes de comunicación y los protocolos que utilizan, dando pauta a lo que es el ambiente de Internet, la suite de protocolos que utiliza, sus direcciones, y por último los servicios que ofrece.

En el capitulo 3 de acuerdo a los riesgos que se observan en las redes informáticas se desglosan aspectos de administración para contribuir a una mejor seguridad, se describen algunos métodos que se pueden implementar y se plantean políticas de seguridad en la red.

En el capitulo 4 se describe la localización geográfica de cada edificio que conforma el Instituto así como su división en áreas de trabajo, se describen las actividades que se realizan y el tipo de información que se maneja en cada una de dichas áreas, para poder identificar las amenazas mas frecuentes a los recursos e información, se presenta la segmentación de la dirección para la conexión con Internet, conexión con la que cuenta el ININ y se hace el análisis de los riesgos que se corren en cada uno de los segmentos de la red, determinándose así que tipo de medidas se deben tomar para prevenir los distintos ataques, y por último se brindan conclusiones.

Pienso que la seguridad es importante, sin embargo el campo de aplicación es bastante amplio puesto que hay que tomar en cuenta tanto aspectos de hardware, software, administrativos, metódicos, e inclusive de conciencia de cada uno de los usuarios que tienen acceso a cualquier red informática, todo esto sin dejar de lado la relación costo - beneficio que implica el implementar todo un sistema de seguridad aunado a la disponibilidad en recursos para darle mantenimiento a dicho sistema.

El objetivo de éste trabajo es el de proponer una metodología en base a directrices que garanticen la integridad de la información en la red de área metropolitana del Instituto Nacional de Investigaciones Nucleares.

CAPÍTULO 1

Redes y sus servicios de conexión

1.1 HISTORIA DE LAS REDES

El almacenamiento y el análisis de información ha sido uno de los grandes problemas que ha enfrentado el hombre desde que inventó la escritura. No es, sino hasta la segunda mitad del siglo XX, que ha podido resolver parcialmente ese problema, gracias a la invención de la computadora.

Con la aparición de las terminales en la década de los 60, se logró una comunicación directa, y por tanto mas rápida y eficiente, entre los usuarios y la unidad central de proceso, pero se encontró un nuevo obstáculo: entre mas terminales y otros periféricos se agregaban al computadora central, se degradaba mas la velocidad de procesamiento.

Con la fabricación de equipos de menor tamaño y regular capacidad, a los que se les denominó microcomputadoras. Estos equipos basados en la tecnología del silicio y de la integración en miniatura permitió a los fabricantes de computadoras construir mayor inteligencia en máquinas mas pequeñas. Estas nuevas máquinas descongestionaron a las viejas máquinas centrales.

Alrededor de los años ochenta, con el surgimiento de las computadoras personales, surgió la necesidad de los usuarios por compartir recursos. Fue entonces, y es hasta hoy muy común que, en una organización, mas de un departamento haga uso de los mismos datos. Si cada persona tiene su propio programa de aplicación y un archivo de datos independientes, al momento de haber una modificación, no se reflejan los cambios de datos en los archivos hechos en una máquina en las otras. Esto lleva a tener datos inconsistentes y, por lo mismo, resultados poco confiables. Este problema se pudo solucionar en un principio con el intercambio de datos vía módem o con el intercambio de diskettes. Se buscaba entonces tener acceso a la información en todos los archivos y que las modificaciones se reflejarán en todas las maquinas al mismo tiempo.

La organización y el manejo de la información se llevaba a cabo mediante sistemas tradicionales de archivos; sin embargo, fueron muchas las desventajas que tenía, por ello se introdujo el concepto de sistema de base de datos que, en su forma mas simple, consiste de un conjunto de aplicaciones o módulos cuyas principales funciones son almacenar todos los datos de una organización y proporcionar a los usuarios las herramientas necesarias para accesarlos y manipularlos dentro de un ambiente confiable y eficiente.

En un sistema tradicional de archivos los archivos se crean para satisfacer diferentes necesidades, como se muestra en la tabla 1-1. Observamos que es muy probable que los datos se encuentren en mas de un archivo, debido a la redundancia que esto implica, se tiene como consecuencia altos costos de almacenamiento, e inconsistencia, esto se refiere a que, al actualizar un dato, no se hace lo mismo con todas sus copias.

SISTEMA TRADICIONAL DE ARCHIVOS	BASE DE DATOS
Redundancia e inconsistencia de los datos	Eliminar la redundancia e inconsistencia
Indisponibilidad de los datos	Limitar el acceso
Datos aislados	Independencia de los datos
	Rutinas de recuperación
	Lenguaje de consulta

Tabla 1-1 ASPECTOS QUE CUBRE UN SISTEMA TRADICIONAL DE ARCHIVOS Y UNA BASE DE DATOS.

Los datos necesarios para el funcionamiento de la empresa existen, pero de manera aislada en diferentes aplicaciones y, tal vez, con diferente formato, por lo cual no es fácil unirlos en un momento dado para obtener una información completa. Una de las soluciones es la duplicación de archivos con los mismos datos y en el mismo formato. Pasado el tiempo, estos archivos ya no son idénticos, ya que en cada aplicación se modifican los datos según las necesidades. Otra alternativa es la de "un archivo para toda". En este caso, todas las aplicaciones utilizan el mismo archivo, los datos están centralizados y no se duplican. Este fue el principio de los sistemas de bases de datos, pero no se puede hablar de dicho sistema como tal, sin un software encargado del manejo y seguridad de los datos.

Con la base de datos se prevé que un mismo dato se duplique. Si un dato tiene que duplicarse, el sistema debe ser capaz de mantenerlo actualizado. Debe contar con controles de seguridad para restringir el acceso a los datos a determinadas aplicaciones o usuarios. Algunos podrán modificarlos, otros sólo leerlos, otros crear nuevos archivos, etc. La independencia de los datos se logra cuando el programa de aplicación puede accesarlos, sin importar la forma en que se almacenaron. Las características físicas de almacenamiento deben ser transparentes para el usuario y para las aplicaciones. Garantizar la confiabilidad del sistema en caso de fallas. Debe permitir a los usuarios hacer consultas a los datos de manera interactiva, sin la necesidad de un programa de aplicación. En la tabla 1-1 se muestran algunas características generales de las bases de datos.

A esta época se le podría denominar la era del floppy disk, porque nuevamente había que transportar la información almacenada en la microcomputadora en diskettes. Por la poca capacidad de los diskettes se hacia difícil el manejo de grandes cantidades de datos, fue necesario fabricar dispositivos que permitieran almacenar mayores cantidades de información. El hecho de seguir pensando en medios con una alta capacidad para almacenamiento y que además fueran fácil de transportar a donde pudiera requerirse, aunado a otras razones como el poder compartir recursos de gran utilización y alto costo como impresoras, graficadores y pantallas de alta definición, todo esto llevó a diversos fabricantes y desarrolladores a idear las redes de computadoras.

1.2 SISTEMAS COMPUTACIONALES

En un principio, las redes de microcomputadoras se formaban por simples conexiones que permitían a un usuario accesar recursos que se encontraban residentes en otra microcomputadora tales como otros discos duros, impresoras, etc. Estos equipos permitían a cada usuario el mismo acceso a todas las partes de un disco y causaban obvios problemas de seguridad y de integridad de los datos. Empezaron a introducirse conceptos como File Server (servidor de archivos) un equipo que permite a todos los usuarios tener acceso a la misma información y compartir archivos con cierto grado de seguridad.

1.2.1 SISTEMA CENTRALIZADO

Están principalmente formados por mainframes, minicomputadoras y micros multiusuarios además de un número variable de terminales locales y remotas. Los usuarios comparten el poder de un procesador central. Una sola copia del software de aplicación corre en el CPU central. El sistema mantiene registros de la ejecución del programa para cada usuario. Las terminales enlazadas que necesiten usar la aplicación comparten el software y los datos en la memoria o el disco del sistema.

1.2.2 SISTEMA COOPERATIVO

Un tipo de procesamiento que la tecnología de las redes de computadoras ha desarrollado fuertemente es el sistema cooperativo, también llamado modelo cliente/servidor, en donde el servidor es el equipo con mas recursos y el cliente es aquel que solicita uno de esos recursos.

Uno de los beneficios de éste modelo se observa cuando se utiliza una aplicación que reside en el disco duro del servidor y varios clientes pueden obtener una copia y trabajar con ella al mismo tiempo. La desventaja mas grave es que el tráfico en el canal de comunicaciones entre el servidor y las estaciones de trabajo o clientes, se vuelve intenso, y puede degradar la eficiencia global del sistema. Puesto que la información entre el servidor y las estaciones de trabajo viajan, generalmente, por el mismo canal de comunicación.

Como se puede observar en la Ilustración 1-1, el canal de comunicaciones se utiliza sólo antes y después del procesamiento del archivo, evitando la degradación del medio.

1.2.3 SISTEMA DISTRIBUIDO

En éste sistema el procesamiento de la información se lleva a cabo en una forma descentralizada, es decir, el trabajo se distribuye entre las computadoras de la red[2]. El procesamiento de información en estaciones de trabajo conectadas a una red es un ejemplo de sistema distribuido. Cada estación corre su propia copia del programa y el sistema operativo de red sincroniza el uso de los recursos compartidos por las múltiples aplicaciones como se muestra en la Ilustración 1-2.

El procesamiento se lleva a cabo en una de las computadoras de la red (la que corre el proceso). El resto de los usuarios no experimentarán efecto alguno en su velocidad de respuesta, ya que la unidad de proceso del servidor se encargará únicamente de administrar los niveles de seguridad de los usuarios y los accesos a disco, nunca del proceso de información, que es la tarea que mas tiempo le quita a una computadora. Este proceso, especialmente en redes de computadoras donde el número de máquinas interconectadas es grande, trae a la luz el concepto de servicios distribuidos.

Los procesos distribuidos se presentan cuando existen varios servidores en la red y cada uno de ellos realiza tareas específicas. Algunos ejemplos típicos de servicios distribuidos son los servicios de impresión, de comunicaciones (gateways), de bases de datos, de administración de red, fax, correo electrónico, etc.

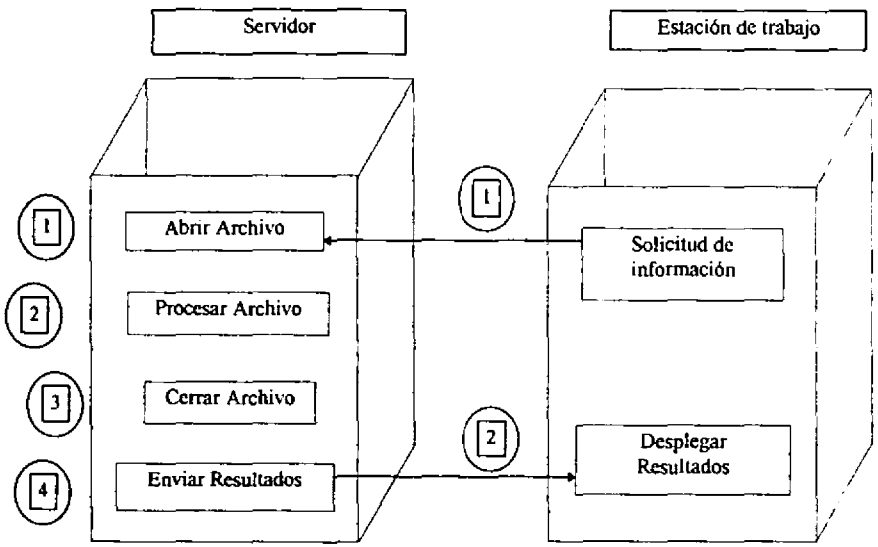


Ilustración 1-1 AMBIENTE DE SISTEMA COOPERATIVO (CLIENTE/SERVIDOR).

[2] SCHATT, Stan. A FONDO: REDES DE ÁREA LOCAL. Anzos, 1987. Pág. 19-20.

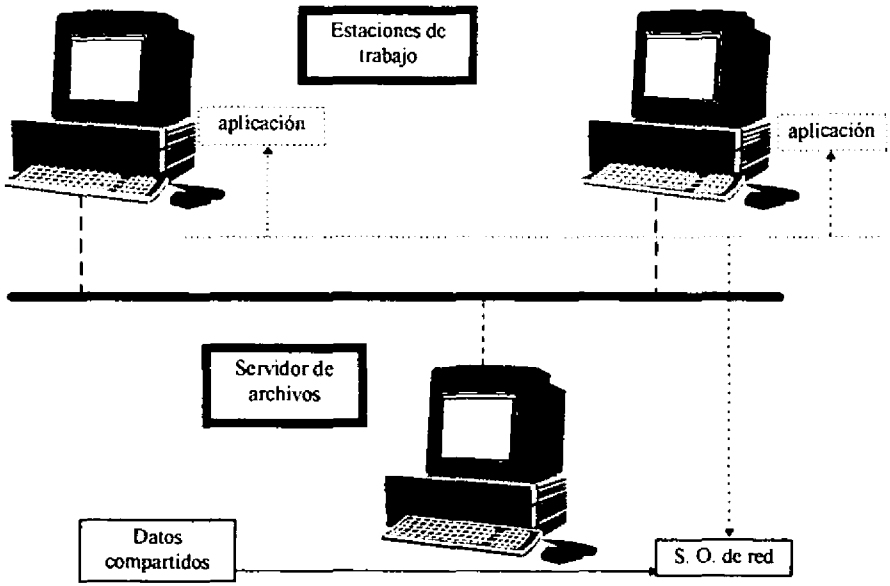


Ilustración 1-2 AMBIENTE DEL SISTEMA DISTRIBUIDO (descentralizado).

Una red de 40 o 50 nodos como son las estaciones de trabajo, computadoras personales, justifica el costo de dedicar computadoras a prestar servicios a las demás, inclusive en redes mas pequeñas, donde la velocidad de respuesta, es decir, el tiempo que tarda el nodo en solicitar una aplicación o archivo y en que el servidor envía dicha información, es una de las características mas importantes que ofrecen los servicios distribuidos.

1.3 TIPOS DE REDES

La red fue concebida para aumentar la productividad, dar mas capacidad a las herramientas electrónicas, poniendo cuidado en ofrecer seguridad y confiabilidad a tal grado que se pueda enviar las aplicaciones e información de la empresa o institución de un lugar a otro a través de la red.

1.3.1 REDES DE ÁREA LOCAL

Esta red esta compuesta por un conjunto de computadoras que se comunican entre si en un área geográficamente limitada, como puede ser un edificio[3]. Las redes de área local LAN (Local Area Network), se han convertido en la base de las redes de área amplia WAN (Wide Area Network), de las redes metropolitanas MAN (Metropolitan Area Network), entre otras.

[3] RAYA CABRERA, José Luis. REDES LOCALES Y TCP/IP. Alfaomega, 1997. Pág. 1-2.

1.3.1.1 COMPONENTES DE UNA RED DE ÁREA LOCAL

Las redes están compuestas de estaciones de trabajo, servidores, sistemas operativos de red, protocolos de comunicación y enlaces físicos como el cableado. El **SERVIDOR** es una computadora con gran capacidad de procesamiento que se encarga de administrar y compartir los recursos de la red y en el que reside el sistema operativo con el que se trabaja.

La labor principal del servidor es compartir los recursos que residen en él con las computadoras que se encuentran conectadas en la red. Un servidor puede contener programas y datos que todos los usuarios de la red puedan compartir y pueden estar dedicados a atender a los usuarios u operar como otra estación de trabajo mas, aunque esto no es lo mas recomendable.

Una **ESTACIÓN DE TRABAJO** es una máquina de usuario, que en ocasiones puede funcionar como una computadora personal. Se encuentra interconectada por medio de una tarjeta de interfase que permite que se comunique con otras estaciones de trabajo. Las estaciones de trabajo sin disco flexible son aquellas que operan y manejan los datos con las aplicaciones y software del servidor, mientras que las estaciones de trabajo que cuentan con unidad de disco flexible accesan la mayor parte del software y de los datos al servidor, tal es el caso de una computadora personal además de que tiene acceso al servidor puede tener sus propios paquetes y aplicaciones cargados en su propio disco duro.

El **SISTEMA OPERATIVO** se define como el conjunto de programas que administra las actividades de una computadora, mediante la asignación de los recursos y la creación de una interfase entre la computadora y los usuarios. El sistema operativo de red administra los recursos de los servidores y controla las actividades de la red, brindando funcionalidad, facilidad de uso, seguridad de los datos y seguridad de acceso.

El **PROTOCOLO DE COMUNICACIÓN** es el conjunto de normas y regulaciones que gobiernan la transmisión y recepción de datos en la red. Análogamente, el protocolo es el idioma que habla el equipo de computo y a través del cual puede comunicarse con otros sistemas. La funcionalidad, la facilidad de uso, la administración, la seguridad de los datos y la seguridad de acceso, dependen del sistema operativo, asi como existen diversos idiomas, también existen diversos protocolos.

Para entender mejor su aplicación es necesario comprender el modelo OSI (Open System Interconnection; Interconexión de sistemas abiertos) que se ilustra en la ilustración 1-3. Este modelo es la base del protocolo de comunicación en un sistema de red. El contenido de cada capa y el comportamiento tanto lógico como físico del envío y recepción de información, se describen a continuación.

MODELO OSI:

CAPA 1.- **FISICA**: Su función principal es la Transmisión de bits: cuando un extremo envía un valor 1 sea el que se reciba al otro lado y para ello contempla cuestiones como:

—¿Cuántos voltios se necesitan para representar un bit de valor 1 o 0?

—¿Cuántos milisegundos deberá durar un bit?

CAPA 2.- **ENLACE**: Esta capa transforma una línea de transmisión en una línea sin errores para la capa de red, esto es, partiendo la entrada de datos en bloques ó TRAMAS de algunos cientos de octetos, incluyendo un bit especial al inicio y al final de la misma. Si la trama no llega a su destino la capa de enlace emisora tiene que retransmitir. Lo mismo ocurre si el acuse de recibo por parte de la maquina destino se pierde y no llega al origen, entonces tiene que volver a enviarla. Además debe evitar que un transmisor muy rápido sature a uno muy lento por medio de procedimientos de regulación de flujo.

CAPA 3.- **RED**: Debe encaminar los paquetes del origen al destino para ello si es necesario crea tablas de rutas que se encuentran conectadas, además de que le sirven para ver la ruta mas conveniente, también le ayudan a evitar sobrecarga en la red. Por otra parte, deben controlar la congestión: si hay demasiados paquetes se formaría un cuello de botella y los paquetes obstruirían la red.

CAPA 4.- **TRANSPORTE**: Acepta los datos de la CAPA DE SESIÓN y los divide en unidades más pequeñas para pasarlos a la capa de red y asegurar que lleguen al otro extremo, con la mayor confiabilidad y rapidez. La conexión más común es la de canal punto a punto, en donde como se reciben los mensajes se envían, por ser una capa origen-destino o extremo a extremo (un programa en la máquina origen lleva una conversación con un programa en la máquina destino).

CAPA 5.- **SESIÓN**: Define el formato para el envió de datos a través de las conexiones.

CAPA 6.- **PRESENTACIÓN**: La representación local de los datos la convierte a una forma estándar y viceversa. La forma estándar utiliza un orden estándar de los bytes y una estructura de empaquetado convencional, independiente de cualquier arquitectura. Si la cantidad de datos es demasiada comparada con la capacidad de enlace de la red entonces comprime los datos para llevar a cabo la transmisión. Entre otras cosas se encarga del proceso de seguridad para mantener la privacidad y autenticación de la información que se esta manejando.

CAPA 7.- **APLICACIÓN**: Provee servicios de red para usuarios finales. Algunos ejemplos de aplicaciones de red son MAIL, FTP, TELNET, DNS, NFS.

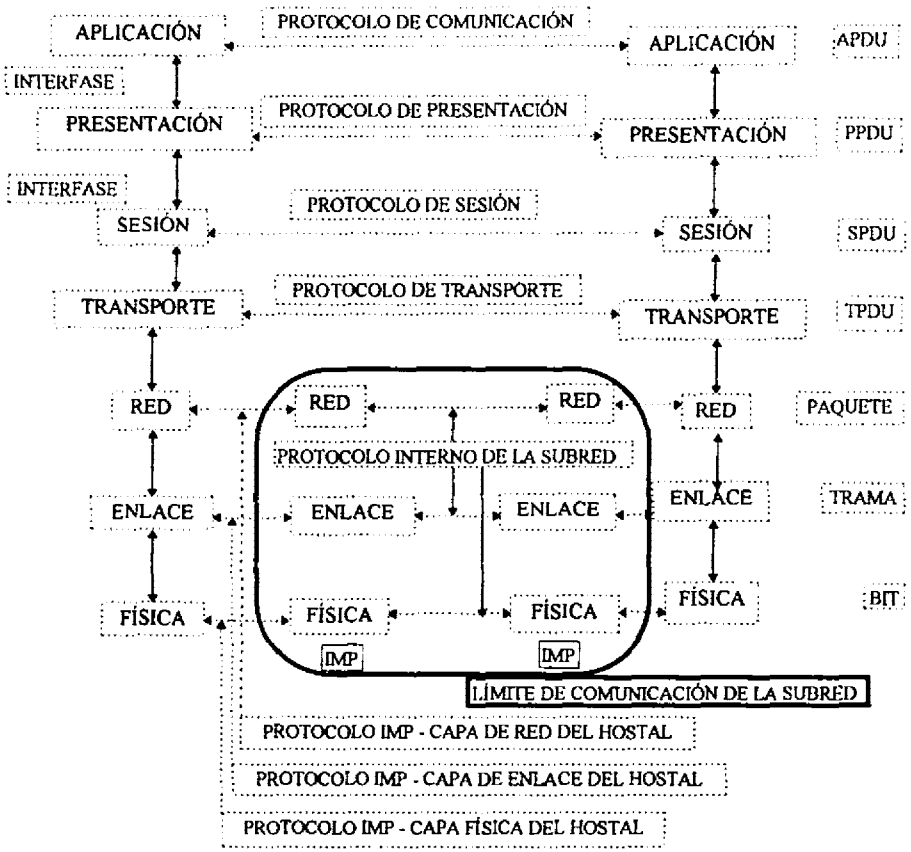


Ilustración 1-3 ARQUITECTURA DE RED BASADA EN EL MODELO OSI.

1.3.2 REDES DE ÁREA METROPOLITANA

Las redes de área metropolitana conocidas como MANs (Metropolitan Area Network) se constituyen cuando un conjunto de redes locales se comunican entre si en una misma área geográfica pequeña, como por ejemplo en una ciudad o provincia. Por lo tanto una red de área metropolitana puede existir en una empresa cuya matriz se ubica en la zona sur de cierta ciudad y además cuenta con sucursales en la zona norte, este y oeste de la misma ciudad.

Esta empresa utiliza redes de área local en cada oficina, pero al comunicarlas a todas contará con una red metropolitana y si esta situación se repite en una provincia cercana donde tenga sucursales como en Guadalajara y Monterrey al conectar las redes locales con las foráneas, se tendrá una red de área amplia.

1.3.3 REDES DE ÁREA AMPLIA

En sentido estricto, una red de área amplia es una red de redes, en la que se conectan varias redes locales mediante dispositivos que permiten su conectividad que es la unión de cada una de las partes de una red local para formar una red de área remota. Estos dispositivos pueden usar o no líneas telefónicas o servicios públicos de transmisión de datos o de dispositivos.

1.3.4 CONECTORES DE REDES DE ÁREA METROPOLITANA Y EXTENDIDA

Los conectores mas sofisticados para formar redes de área amplia o también redes de área metropolitana son denominados también cajas negras que permiten formar diferentes topologías y protocolos dentro de un mismo sistema heterogéneo entre ellos están los puentes, repetidores, ruteadores y gateways.

1.3.4.1 REPETIDORES.

Los repetidores proporcionan el medio mas sencillo y barato de interconectar redes locales, puesto que lee cada uno de los mensajes y hace una replica de ellos, para asegurarse que los mensajes sean totalmente legibles. Ilustrando, un repetidor coloca la copia del fax recibido en la charola correspondiente al destinatario. Además proporciona servicios de regeneración de señales, pues éstas se degeneran cuando pasan por un medio de transmisión. Dicha degeneración es en proporción directa a la longitud del cable. La pérdida de señal se conoce como atenuación. En caso de existir atenuaciones amplifica la señal recibida por un segmento de cable y retransmite (repite) la misma señal hacia otro segmento.

1.3.4.2 BRIDGES (PUENTES)

Los bridges son dispositivos de conexión un poco mas inteligente, puesto que mantienen registros detallados de la correspondencia (quien envía y quien recibe) pero no pueden procesar mas de dos paquetes de información a la vez. Por ejemplo: Si llegan 2 sobres al departamento de correspondencia, uno de ellos es de correspondencia interna, y el otro es un sobre dirigido a un cliente en otro Estado de la República, el bridge lee la dirección del destinatario, si es externo, coloca el sobre en la charola de "salida", si al leer la dirección del paquete el destinatario es local, a éste paquete lo coloca en la charola "local". Para que el puente reconozca cuales son destinos locales y cuales son destinos remotos, recordemos que los puentes trabajan con dos piezas de información a la vez: la dirección del destinatario y la dirección del remitente. Cada vez que el puente recibe un sobre, busca en la lista de "direcciones locales", la dirección del remitente. Si la dirección que busca no se encuentra en la lista la agrega. De esta manera va creciendo su lista de direcciones locales. Después busca en la misma lista, la dirección del destinatario, si la encuentra coloca el sobre en la charola "local", si no la encuentra, asume que es un destinatario externo y coloca el sobre en la charola de "salida".

1.3.4.3 RUTEADORES

Los ruteadores proporcionan un servicio de conexión aún mas inteligente. El ruteador puede manipular direcciones de remitente y destinatario, puede tomar decisiones en cuanto a cual es la mejor manera de enviar un documento, como se observa en la tabla 1-2. Sin embargo, esta ventaja tiene un costo. Por ejemplo: Si llegan dos sobres, uno de ellos es muy urgente y

debe ser entregado lo mas rápido posible a un cliente en otro estado de la república. El otro es muy grande, pero su contenido no es urgente. En cuanto el ruteador recibe el sobre que es urgente, decide cual es la compañía de mensajería que va a seleccionar para enviarlo a su destino. Para tomar la decisión de que mensajería utilizar para el envío de paquetes, debe tener en cuenta varios factores tales como: la velocidad a la cual entrega el proveedor, el costo, la prioridad, la capacidad del servicio de notificar si el paquete fue entregado o no y algunas otras garantías. En cuanto al sobre que es de entrega normal, debe también decidir como enviarlo, incluso debe decidir si abre el paquete y lo divide en paquetes más pequeños. En el caso de envío urgente, decide que servicio utilizar para enviarlo, tomando en cuenta cual es el destino y la urgencia. Con respecto al paquete normal, decide si abrirlo y hacer paquetes mas pequeños.

1.3.4.4 GATEWAYS (COMPUERTAS DE SALIDA)

Los gateways proporcionan el servicio de conexión mas inteligente. Por ejemplo, si tenemos un cliente que es alemán, nosotros preparamos en español, los documentos que le vamos a enviar y se los damos al Gateway, éste recibe los documentos y los traduce al alemán, en seguida envía el material a su destinatario. Los lenguajes que permiten a las computadoras comunicarse entre sí son los protocolos. Los gateways proporcionan un servicio de traducción entre los diferentes protocolos. Lo mas importante es que, los gateways, además de conectar dispositivos de una red con los de otra red, hacen posible la comunicación entre ellos.

1.4 LA VELOCIDAD DE TRANSFERENCIA

Es más importante estar consiente de la transferencia real de datos (through put) que de la velocidad máxima a la que un paquete viaja en ella. La transferencia real de datos varia considerablemente, dependiendo del hardware, del protocolo de acceso empleado y de la actividad en la red.

1.5 TRÁFICO

El número de estaciones y el tipo de aplicaciones definirá la magnitud de tráfico de la red. En las redes con una actividad ligera, la mayor parte del procesamiento se realiza en la estación de trabajo y requiere de poco acceso a los recursos comunes como disco duro, impresoras, etc. En otros casos los datos pueden leerse de la red, manipularse en la estación de trabajo, y luego salvarse en el disco compartido. Tales aplicaciones incluyen procesadores de texto, correo electrónico y hojas de calculo, entre otras.

RUTEADORES	BRIDGES (PUENTES)
Pueden ser avisados de la prioridad o urgencia de una entrega.	No son avisados (los dispositivos no conocen su existencia).
Accesan y utilizan varias fuentes de datos.	Sólo utilizan la dirección remitente y la dirección destino.

Tabla 1-2 VENTAJAS Y DESVENTAJAS ENTRE RUTEADORES Y BRIDGES (PUENTES).

RUTEADORES	BRIDGES (PUENTES)
Pueden abrir el sobre y manipular el contenido (fragmentar). De esta manera pueden partir un mensaje en paquetes cuyo tamaño sea aceptado por la red.	No tienen acceso a los sobres.
Pueden informar al usuario final de las condiciones de la red.	No pueden informar de las condiciones de la red.
Reenvían un sobre a un destino específico.	Colocan el sobre en una charola de salida.
Proporcionan diferentes "tipos" de servicios.	Tratan a todos los paquetes de la misma manera.
Proporcionan mayor seguridad debido a que pueden ser direccionados directamente y utilizan datos adicionales para implementar la seguridad. Los beneficios que proporcionan los ruteadores son mas notorios en la medida en que las redes aumentan de tamaño y complejidad.	Brindan menor seguridad.

Tabla 1-2 VENTAJAS Y DESVENTAJAS ENTRE RUTEADORES Y BRIDGES (PUENTES).

En las redes de carga mediana a pesada, con frecuencia se requiere el acceso al servidor. Las aplicaciones incluyen manejos de base de datos tales como entradas de ordenes, inventario y transacciones de contabilidad, clasificación, índice y generación de reportes, otras aplicaciones correrán programas que quizá manipulen cantidades considerables de datos, entre muchas otras aplicaciones, todo esto hace que el tráfico en la red sea lento.

1.6 TOPOLOGÍA

La topología de la red se refiere a como se establece y se cablea la red[4] como se puede observar en la ilustración 1-4. La elección de la topología afectará la facilidad de la instalación, el
costo del cable y la confiabilidad de la red. Tres de las topologías básicas de red son la estrella, el bus y el anillo. En las topologías de estrella, cada estación se conecta con su propio cable a un dispositivo de conexión central, bien sea un servidor o un concentrador o repetidor. Esta topología utiliza mas cable que las topologías de bus, pero es mucho mas fácil aislar las fallas. Si una estación funciona mal en la red, solamente se apaga la estación individual afectada. El resto de la red continua operando sin interferencia. La topología de estrella es ideal para muchas estaciones que se localizan a una gran distancia (alejadas). La flexibilidad de la estrella permite hacer una fácil instalación, y hace fácil agregar, relocalizar, o remover estaciones de la red. En las topologías de bus o lineales, todas las estaciones se conectan a un cable central llamado "bus".

[4] TODO SOBRE INTERNET. Marcombo, 1996. Pág. 23.

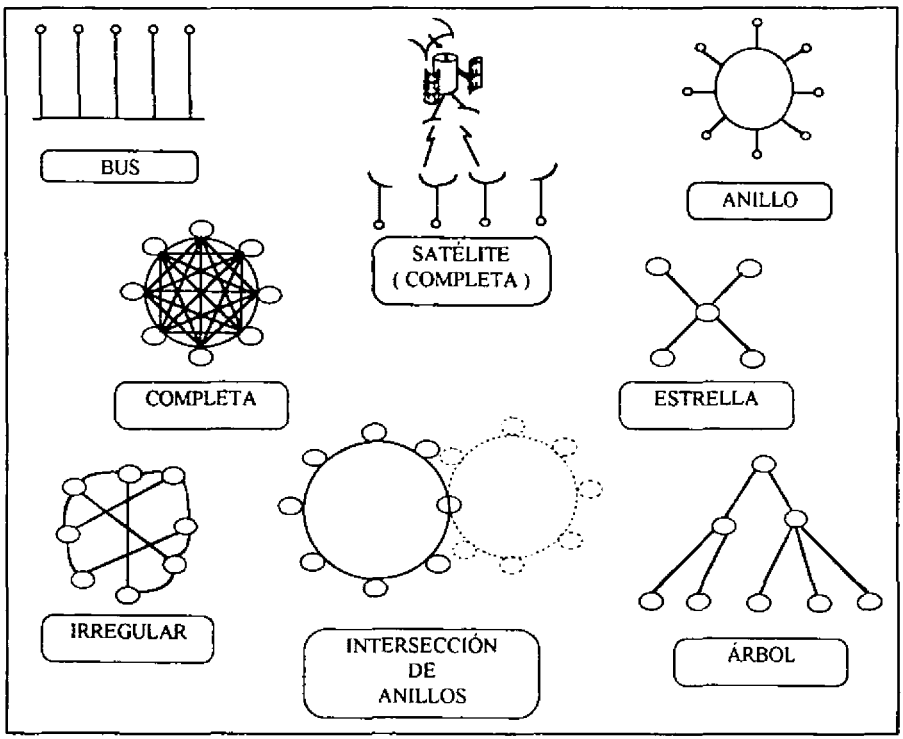


Ilustración 1-4 POSIBLES TOPOLOGÍAS EN RED.

1.7 CABLEADO

El propósito de la capa física consiste en transportar el flujo de bits de una máquina a otra. Normalmente, se utilizan varios medios físicos para realizar una transmisión. A continuación mostraremos algunos de los medios mas usuales de transmisión.

1.7.1 CABLE COAXIAL

El cable coaxial se conforma por un alambre conductor básico cubierto por una placa metálica que actúa como tierra. El alambre conductor y la tierra se encuentran separados por un aislante plástico y, finalmente, todo el conjunto esta protegido por una cubierta exterior, también aislante[5]. Como se observa en la ilustración 1-5

[5] SCHATT, Stan. A FONDO: REDES DE ÁREA LOCAL. Anzos. 1987. Pág. 37.

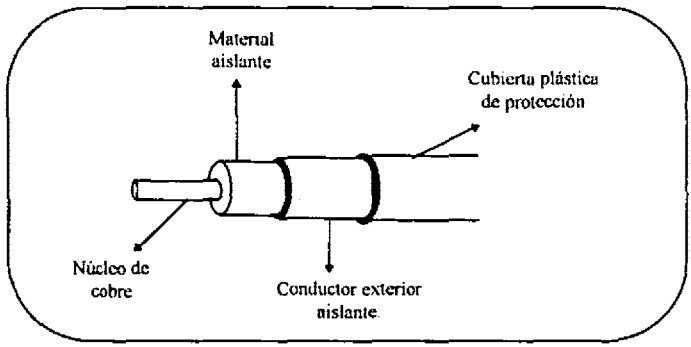


Ilustración 1-5 CABLE COAXIAL, UNA COMBINACIÓN DE ANCHO DE BANDA Y EXCELENTE INMUNIDAD AL RUIDO.

Las redes Ethernet de tipo bus se pueden implementar con dos tipos de cable coaxial. Una de ellas opera con cable coaxial delgado RG/58 A/U de 50 ohms, 0.2 pulgadas de diámetro y permite transportar una señal hasta 300 metros, también sin el uso de repetidores. La segunda alternativa es mediante la implementación del cable coaxial grueso de 50 ohms IEEE 802.3, de 0.4 pulgadas de diámetro, que permite manejar señales hasta 500 metros sin presentar algún tipo de atenuación que produzca errores en la comunicación.

1.7.2 PAR TORCIDO

El cable de par torcido se forma principalmente por dos alambres de cobre que se encuentran aislados como se ilustra en la ilustración 1-6 por una cubierta plástica y torcidos uno contra el otro[6]. Es esta característica la que los distingue con su nombre (Twisted Pair). Los cables con los conductores de cobre mas delgados y menos protegidos por un jacket están dentro de la clasificación de cables tipo UTP (Unshielded Twisted Pair; par torcido sin blindar). Son sumamente baratos, flexibles y permiten manipular una señal a una distancia máxima de 110 metros sin el uso de amplificadores. Los cables de conductores mas gruesos y muy bien cubiertos por un jacket son denominados del tipo STP (Shielded Twisted Pair; par torcido blindado). Estos últimos son mas caros y menos flexibles que los UTP, pero permiten un rango de operación de hasta 500 metros.

1.7.3 CABLE DE FIBRA ÓPTICA

La tercera tecnología de cables que se utiliza en las redes locales es la fibra óptica. Normalmente se emplea por tres razones básicas: para aquellos casos en donde las grandes distancias son un factor determinante para la implantación de una red local; cuando se requiere una alta capacidad de aplicaciones de comunicación y cuando el ruido o cualquier tipo de interferencia son factores a considerar. El cable de fibra óptica se compone

[6] SCHATT, Stan. A FONDO: REDES DE ÁREA LOCAL. Anzos, 1987. Pág. 36.

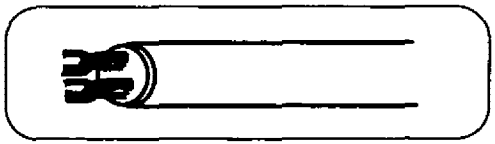


Ilustración 1-6 CABLE DE PAR TORCIDO (DOS PARES).

de una fibra muy delgada elaborada de dos tipos de vidrio con diferentes indices de refracción, uno para la parte interior y otro para la parte exterior[7] como se puede observar en la ilustración 1-7. Esta diferencia en la refracción previene que la luz penetre en una parte de la fibra óptica impidiéndolo desde la parte exterior evitando así la perdida de la información. La fibra óptica, a su vez, se encuentra cubierta por una placa aislante y protectora en la parte mas exterior para darle mayor integridad estructural al cable.

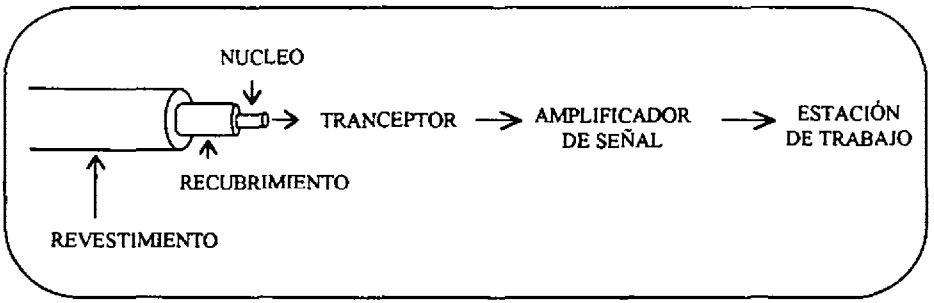


Ilustración 1-7 CABLE DE FIBRA ÓPTICA.

En la tabla 1-3 se muestran algunas caracteristicas generales de los cables que ofrecen mejores transmisiones de datos, y el que observamos que tiene mayor ancho de banda, y transmite la señal a una mayor distancia es el cable de fibra óptica.

1.8 ALIMENTACIÓN ELÉCTRICA.

Para el caso de una red local, es muy importante que tanto las estaciones de trabajo como el servidor cuenten con un voltaje regulado y también con una buena instalación de tierra fisica. No hay que olvidar que, al unir fisicamente una serie de computadoras personales (PC) por medio de una red, también se les esta uniendo eléctricamente. En caso de no contar con una tierra fisica, el voltaje de referencia de una computadora puede ser diferente al de la PC que esta al lado, lo que origina diferencias de voltaje indeseables que se pueden traducir en daños en las tarjetas de red o inclusive en daños para las propias computadoras.

[7] SCHATT, Stan. A FONDO: REDES DE ÁREA LOCAL. Anzos, 1987. Pág. 41.

	PAR TORCIDO	COAXIAL BANDA BASE	COAXIAL BANDA ANCHA	FIBRA ÓPTICA
Ancho de Banda	baja	moderada	alta	muy alta
Instalación	sencilla	fácil.	Fácil	dificil
Longitud	baja	moderada	alta	muy alta
Costo	barata	moderada	cara	muy cara
Fiabilidad de la transmisión	baja	alta	alta	muy alta
Interferencia	alta	moderada	baja	ninguna
Seguridad	baja	baja	moderada	alta
Topología	bus estrella anillo	bus	bus estrella	estrella anillo

Tabla 1-3 COMPARACIÓN ENTRE CABLES: PAR TORCIDO, FIBRA ÓPTICA Y CABLE COAXIAL

CAPÍTULO 2

Ambiente de comunicación e interconectividad en Internet

El server o servidor es el elemento mas importante dentro de una red, la máquina mas equipada que se tenga debe de utilizarse como tal. El hecho de que, en la mayoria de las redes, no se pueda utilizar como otra estación de trabajo mas, no debe influir en la decisión de asignarle la función de servidor. En el caso de redes mayores de 10 máquinas, no es aconsejable que el servidor se utilice como una estación de trabajo adicional, aunque sea posible. Si bien puede decirse que el servidor es el cerebro de la red, el cableado, cualquiera que este sea, y la instalación eléctrica son la columna vertebral. Si se puede tener una línea eléctrica independiente dedicada a las computadoras, bien aterrizada, esto evitará muchos problemas, en este tipo de instalaciones.

2.1 INSTALACIÓN DEL SOFTWARE ADECUADO EN LA RED

No faltan los que instalen una red y luego procedan a darle a cada usuario un programa monousuario para que lo usen dentro de ella. Con una red se debe tener o desarrollar software para red. De nada sirve tener máquinas interconectadas si no están compartiendo la información que contienen. Hay software que requiere una red rápida para funcionar eficientemente. Hay otro que requiere mucho espacio de almacenamiento. Otro mas, tiene limite en el número de usuarios. Si el software tiene requisitos en cuanto a características mínimas de máquinas, o equipo de hardware especializado, antes de adquirirlo, debe tenerse la seguridad de que la mayoria o todas las máquinas, van a poder utilizarlo. En caso contrario, se deberá evaluar si existe otro software, mas conveniente o en un caso extremo, cambiar el equipo existente, puesto que el anterior ya no va a poder cumplir con sus funciones. Lo mejor es utilizar los paquetes que se acomodan a las necesidades de la empresa y buscar software similar a lo que los usuarios ya conocen, para evitar gastos de tiempo y dinero en capacitación. Si se cambia un programa completamente se debe contar con alguna persona dentro de la empresa que lo conozca a fondo antes de instalarlo para todos los usuarios. Asi, este podrá apoyarlos en sus dudas.

2.2 EVALUACIÓN DE ALTERNATIVAS DE PROCESO PARA LA UTILIZACIÓN DE RECURSOS EN LA RED

Las redes de computadoras ofrecen gran flexibilidad en el área de procesamiento de información. La selección del tipo de procesamiento en las redes locales (basado en servidores o estaciones de trabajo) ofrece a los usuarios la posibilidad de escoger la alternativa de proceso que mejor se adapte a sus necesidades, tomándose en cuenta los factores tales como: rendimiento, confiabilidad, aplicaciones, etc. La creciente popularidad de las redes puede atribuirse directamente a dicha flexibilidad

2.3 OBJETIVOS DE LAS REDES

Como hemos podido observar es importante tener claros los objetivos por los cuales se desea instalar una red, así como las características propias de cada tipo de red, por ello, de manera general, daremos algunas de las cualidades que esta debe reunir.

a) Compartir recursos: El objetivo es hacer que los programas, datos y el equipo estén disponibles para que cualquier persona que tenga acceso a la red pueda consultarlos, sin importar la localización física de los recursos y del usuario.

b) Alta fiabilidad: Contar con fuentes alternas de suministro de información lo mas actualizada, es decir, todos los archivos podrían duplicarse en dos o tres maquinas, de tal manera que si una de ellas no se encuentra disponible (como consecuencia de un fallo del hardware), podría utilizarse alguna de las otras copias. La presencia de múltiples CPU significa que si alguna de ellas deja de funcionar, están las otras conectadas a la red que pueden ser capaces de encargarse de su trabajo, aunque el rendimiento global sea mucho menor.

c) Ahorro económico: Las computadoras pequeñas tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son algunas veces mas rápidas que la mas rápida de las computadoras, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas constituidos por poderosas computadoras personales, uno por usuario, con los datos guardados en una o mas máquinas que funcionan como servidor compartido.

Para dar una idea sobre algunos de los usos de redes que se consideran importantes veremos que son:

a) El acceso a programas remotos
b) El acceso a bases de datos remotos y
c) Facilidades de comunicación de valor agregado.

2.4 REDES ARCNET

La red Arcnet[8] utiliza el protocolo de acceso Token Passing y la topología de anillo, o bien en forma de estrella.

El paquete de información viaja a través de la red de un nodo a otro, en forma ascendente. Es decir, el paquete de información (token), por ejemplo, en una red de cuatro nodos primero parte del primer nodo pasando por cada uno de los demás (2,3,4) y regresa nuevamente al otro.

Se mencionó que Arcnet utiliza una topología de anillo, pero después de esta explicación es posible afirmar que se trata de un anillo modificado, ya que en verdad recorrerá los nodos en forma de anillo por ser un ciclo de atención a cada uno de ellos. Pero esto lo hará no en la posición física en que se encuentran, sino en el orden lógico que se le de a cada uno. Por tal razón, cada tarjeta lleva un número asignado de nodo, el cual tiene que ser distinto a

[8] RAYA CABRERA, José Luis. REDES LOCALES Y TCP/IP. Alfaomega, 1997. Pág 45.

cualquier otro en la red. Este número de nodo (node address) se direcciona fisicamente a cada tarjeta. Si existiesen dos nodos con números iguales en la red, como consecuencia, habría fuertes conflictos en la comunicación, inclusive podría no existir respuesta en nodo alguno, es decir, como comúnmente se dice, la red no levantaría. Cada mensaje incluye una identificación del nodo fuente y del nodo destino y sólo el destino puede leer el mensaje completo. En este tipo de red no es necesario que cada estación regenere el mensaje antes de transmitirlo al siguiente. Todas las estaciones tienen la capacidad de indicar inmediatamente si pueden o no aceptar el mensaje y, además, reconocen cuando ya se recibió.

En este tipo de red existe tanto el cableado coaxial como el cableado telefónico, siendo el primero el mas utilizado. Este tipo de redes se recomienda ampliamente cuando el trabajo o el procesamiento en la misma no es muy fuerte. El tráfico de la red no es tan importante como podría ser en el caso de que se utilizara algún procesador de palabras y/u hojas de cálculo, o bien, se corrieran programas generando enormes cantidades de datos.

2.5 REDES TOKEN RING

La transmisión de los datos en una red de tipo Token Ring se realiza mediante el "agente" de token; es decir, utiliza un protocolo denominado token passing (que significa paso de testigo[9]), en donde un nodo obtiene el privilegio de transmitir datos. Una estación transmisora captura el token (testigo), cambia el primer bit para identificarlo como un paquete de datos, añade los datos y una dirección y envía la señal "hacia la corriente". Cada nodo checa si los datos están direccionados a él; si no, el nodo retransmite los datos. Cuando el nodo direccionado recibe la información, verifica que ésta sea correcta, copia los datos, marca el paquete de datos como recibido y lo regresa al medio de transmisión. El nodo transmisor remueve el paquete de datos, regresando el original y añadiendo un token nuevo. Como se ve éste protocolo se basa en un esquema libre de colisiones, dado que el token se pasa de un nodo o estación al siguiente. Con esto se garantiza que todas las estaciones tendrán la misma oportunidad de transmitir y que un sólo paquete viajará a la vez en la red. En este método, el acceso a la línea de comunicación siempre esta libre para transmitir mensajes, por lo que se pueden tener tiempos de respuesta aún con gran cantidad de actividad en la red. Uno de sus inconvenientes es que, al llegar a un nodo, el nodo regenera el mensaje antes de pasarlo al siguiente. Esto origina una reducción en el rendimiento de la red pero se asegura una transmisión exitosa desde la primera vez que se envía el mensaje. Las fallas físicas tales como un rompimiento del cable, pueden causar que el nodo reciba una señal invalida de "su vecino de arriba" mas cercano.

2.6 REDES ETHERNET

Ethernet es el ambiente de comunicación entre microcomputadoras mas utilizado en la actualidad. Este tipo de red cumple con la norma IEEE 802.3[10], y probablemente es el que en mas industrias como empresas de iniciativa privada, fabricas, sector educacional, sector gobierno y científico se instala. Ethernet se puede utilizar con distintas opciones de cableado

[9] RAYA CABRERA, José Luis. REDES LOCALES Y TCP/IP. Alfaomega, 1997. Pág. 45
[10] SCHATT, Stan. A FONDO: REDES DE ÁREA LOCAL. Anzos, 1987. Pág. 53.

como es el cable coaxial grueso o delgado, cable UTP (Unshield Twisted Pair, cable de par torcido sin blindar) o fibra óptica.

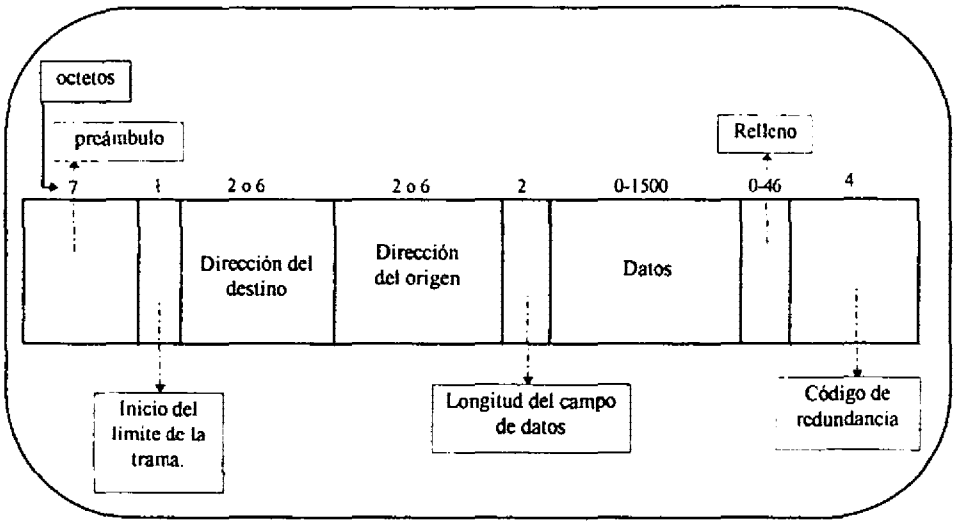


Ilustración 2-1 FORMATO DE LA TRAMA 802.3 PARA ESTÁNDAR DE CONTENCIÓN DE BUS PARA LAS REDES ETHERNET (CSMA).

Este tipo de redes utiliza una topología de bus lineal para cable coaxial o una topología de estrella para cableado UTP (o de base 10) o fibra óptica con un protocolo de acceso CSMA/CD (Carrier Sense Multiple Access/Colisión Detection: Acceso múltiple por detección de portadora/Detección de colisiones). En este tipo de red cada estación se encuentra conectada bajo un mismo bus de datos[11], es decir en una topología de bus lineal las computadoras se conectan a la misma línea de comunicación (cableado), para el caso de la topología tipo estrella los nodos se conectan a través de un centro de cableado mediante concentradores y por esta transmiten los paquetes de información hacia el servidor y/o los otros nodos. Cada estación se encuentra monitoreando constantemente la línea de comunicación con el objeto de transmitir o recibir sus mensajes. Si la línea presenta tráfico en el momento que una estación quiere transmitir, la estación espera un periodo muy corto (milisegundos) para continuar monitoreando la red. Si la línea esta libre, la estación transmisora envía su mensaje en ambas direcciones por toda la red. Cada mensaje incluye una identificación del nodo transmisor y el receptor que puede leer el mensaje completo, como se ilustra en la ilustración 2-1.

[11] TODO SOBRE INTERNET. Marcombo, 1996. Pág. 25-26.

Cuando dos estaciones transmiten sus mensajes simultáneamente una colisión ocurre y es necesaria una retransmisión hasta que la transmisión sea exitosa; así se impide la perdida de los datos. Ya que el nodo aún esta monitoreando, sabe que ha ocurrido una colisión, es decir, es capaz de detectar la colisión, e intentará de nuevo la transmisión del mensaje. El protocolo incluye las reglas que determinan cuanto tiempo tendrán que esperar los nodos o estaciones para realizar sus envíos nuevamente con la finalidad de impedir que se provoquen mas colisiones. La velocidad de transmisión de Ethernet es de 10 Mbps, por el contrario de lo que se pudiese pensar, conforme al tipo de comunicación, operación, y donde se tienen tiempos de respuesta constantes, su rendimiento es muy superior al de otro tipo de redes locales.

2.7 INTERNET

Internet se refiere a una conjunción de redes[12] que se concentran principalmente en los Estados Unidos, y muchas otras repartidas en todo el mundo. La mayoría de las redes que engloba Internet se comunican mediante la suite TCP/IP (Transmition Control Protocol/Internet Protocol; Protocolo de Control de Transmisión/Protocolo Inter-red), mediante el cual los usuarios utilizan servicios de correo electrónico SMTP (Send Message Transference Protocol; Protocolo de envío de mensajes), transferencia de archivos FTP (File Transfer Protocol; Protocolo de Transmisión de Archivos) y TELNET (Protocolo que en si mismo opera como aplicación de emulación de terminal), proceso a través del cual se pueden tener sesiones interactivas a una computadora remota.

La red Internet al tener una base tan grande a nivel mundial tiene objetivos muy claros y específicos como facilitar la posibilidad de compartir recursos entre las organizaciones participantes, como son las agencias de gobierno, instituciones educativas y corporaciones privadas; así como promover el interés y participación de investigadores y proveerlos de un ambiente de prueba para nuevos desarrollos en comunicación en redes.

2.7.1 TCP/IP COMO LA BASE DE INTERNET

Las redes de computadoras necesitan del empleo de un protocolo (que son los lenguajes que permiten a las computadoras comunicarse entre si), para que controlen y administren la forma o "lenguaje" en el que se comunican. Dado que existen diversos tipos de protocolos, las computadoras pueden establecer comunicación hacia otras con protocolos diferentes a través de un puente ó bridge, o bien, ruteadores. Para lograr la comunicación entre los equipos se utilizan tarjetas de interfase que normalmente son las que manejan el protocolo.

La Suite TCP/IP en que se basa Internet fue desarrollado entre 1973 y 1981, bajo el auspicio del Advanced Research Projects Agency (DARPA), ellos se encargaron del desarrollo del protocolo para TCP e IP[13]. El principal acierto del protocolo fue el haber desarrollado una arquitectura de comunicaciones sólida en caso de que la red o sus componentes sufrieran fallas, además de que puede acomodar múltiples servicios de comunicación sobre una gama de redes. A mediados de los 80, el protocolo se volvió muy popular en la comunidad comercial, y es uno de los protocolos mas utilizados. Actualmente TCP/IP esta disponible

[12] RAYA CABRERA, José Luis. Alfaomega, 1997. Pág. 141-143.
[13] Idem. Pág. 93-94.

para soportar desde computadoras personales hasta supercomputadoras. Aunque la mayor parte de los protocolos que integran TCP/IP (como se muestra en la ilustración 2-2) están bien definidos, su desarrollo e investigación continúan para mejorar y extender su capacidad

TCP/IP define formatos que comprenden el origen, destino, tamaño y tipo así como la forma en la que las redes deben recibir y retransmitir los paquetes cuantas veces sea necesario, así como las reglas para la transmisión y recepción de información independientemente del tipo de red o hardware. Este protocolo nos permite rutear la información de una máquina a otra. Este protocolo existe desde que existe (UNIX*). TCP/IP es el resultado del trabajo que se hizo para la agencia DARPA, y puede ejecutarse sobre TOKEN RING, ETHERNET y otras topologías de bus, líneas alquiladas de punto a punto y otras. El uso de éste protocolo se ha incrementado a una velocidad exponencial así como el número de conexiones con INTERNET.

Cada capa del conjunto de protocolos de la computadora origen se comunica con la misma capa de la computadora destino como se ve en la ilustración 2-3. Las capas al mismo nivel en la computadora origen como en la destino se consideran como semejantes "peers" al igual que las aplicaciones, y desde la perspectiva del software la transferencia se realiza como si las capas semejantes se enviarán directamente paquetes una con la otra.

2.7.1.1 DIRECCIONES FÍSICAS

DIRECCIONES IP Para un nodo es una dirección lógica, con la misma forma sin importar el tipo de red y es totalmente independiente a la configuración de esta o la del hardware. Esta formada de 32 bits que identifican a la red, al host o al nodo, en la misma. La dirección IP es representada en notación decimal por ejemplo 139.57.5.1[11] . Los nodos que usan los protocolos TCP/IP traducen la dirección destino IP a direcciones físicas MAC✓ de hardware para poder enviar paquetes a otros nodos de la red. Cada aplicación transmisora manda la dirección IP en el paquete y la aplicación receptora puede responder usando la dirección del transmisor incluida en el paquete IP. Debido a que las direcciones IP no son dependientes de alguna red en particular, pueden ser utilizadas para enviar paquetes de un tipo de red a otra. En cada tipo de red, el software TCP/IP hace la correspondencia entre direcciones IP y direcciones físicas en su propia red.

2.7.2 DIRECCIONES, REDES Y NOMBRES DE ANFITRION (PARA INTERNET)

El esquema de dirección esta controlado por el protocolo INTERNET que consiste en dos partes:

1. La porción de red: se usa para describir a la red a la que reside el anfitrión.
2. La parte del anfitrión: para identificar al anfitrión en particular.

---

* UNIX - Sistema Operativo de Red.

[11] RAYA CABRERA, José Luis. Alfaomega, 1997. Pág. 94

✓ MAC - Control de Acceso al Medio.

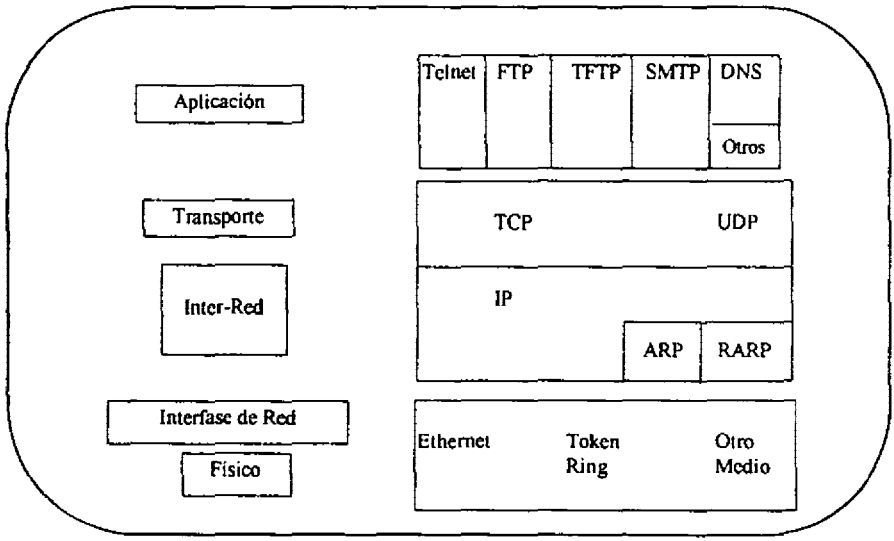


Ilustración 2-2 CAPAS QUE CONFORMAN TCP Y PROTOCOLOS MÁS COMUNES.

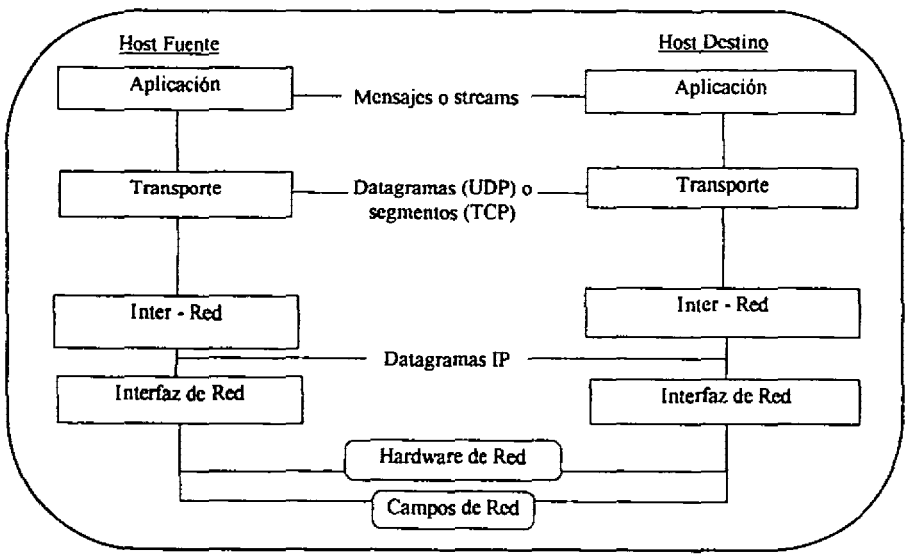


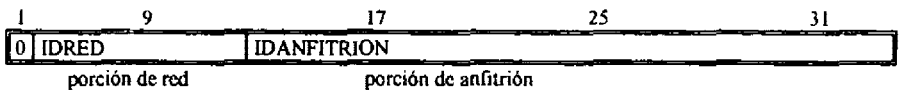
Ilustración 2-3 COMUNICACIÓN ENTRE CAPAS DEL MODELO TCP.

Cada dirección es distinta (no pueden existir dos iguales) y por lo tanto única. El protocolo INTERNET esta diseñado con un esquema de dirección flexible con una red mas grande con varios anfitriones, este esquema de direcciones introduce cuatro clases.

2.7.2.1 CLASES DE DIRECCIONES

Existen dos grupos, el primer grupo de direcciones son del tipo A, B, C son aquellas que se utilizan para identificar a las computadoras que comparten una red en común. Las del segundo grupo son la clase D o direcciones multiconectadas identifican a un conjunto de computadoras que comparten un protocolo común. Sin importar a que clase de dirección se refieren las cuatro clases consisten de 32 bits o 4 bytes (con 8 bits cada uno), cada byte puede tomar el valor desde 0 hasta 255.

DIRECCIÓN CLASE A

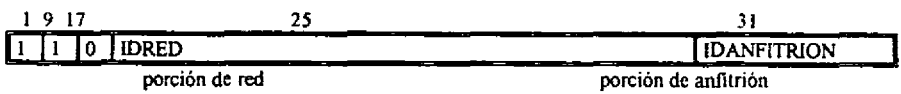


Hay 24 bits disponibles para especificar la dirección del anfitrión por lo que se pueden tener millones, y como el primer bit es ajustado a 0 entonces varia de 1 a 126 o bien 126 redes clase A con mas de 16 millones de anfitriones, puesto que las redes 0 y 127 están reservadas.

DIRECCIÓN CLASE B

Los primeros dos bits de la dirección de la red han sido ajustados a 1 y 0 para indicar que la dirección de la red tiene un rango desde 128 a 191, pudiendo direccionar aproximadamente 16 mil nodos por cada una. Los otros dos bytes serán para la porción de anfitrión.

DIRECCIÓN CLASE C



Utiliza tres bytes para la porción de la red y un byte para la porción de anfitrión. Lo que indica que puede haber más redes clase C aunque cada una con pocos anfitriones. Pueden haber 253 anfitriones para una red clase C. Y la porción de red varia de 192 a 254.

Se necesita una dirección IP para que un nodo se pueda comunicar con otros que empleen la serie TCP/IP, incluyendo a nodos en otras redes privadas así como a los que estén en Internet.

2.7.3 CONECTIVIDAD

Usualmente, el acceso a Internet se realiza a través de un nodo que tiene una conexión directa por medio de una línea telefónica analógica o digital al próximo nodo Internet adyacente y además cuenta con un nombre de dominio propio y dirección IP registrada en el NIC (Network Information Center: Centro de Información de Redes) ubicado en Menlo Park, California. Este tipo de nodos permiten mantener un servidor de FTP y el servicio de TELNET para sesión remota, así como servidores de noticias.

2.7.4 SERVICIOS QUE OFRECE INTERNET

Todos los nodos y redes de Internet, usan el protocolo TCP/IP Suite y cuentan con herramientas como son : TELNET para sesión interactiva remota, FTP para transferencia de archivos, SMTP para correo electrónico, además de otros servicios.

2.7.4.1 CORREO ELECTRONICO

Este servicio permite al usuario mandar mensajes electrónicamente a individuos o grupos de individuos. Los programas del sistema operativo que maneja el correo aceptan y almacenan mensajes que llegan de usuarios de otros nodos. Estos programas reciben el correo del nodo y lo distribuyen al usuario al cual va dirigido. La mayoría de los usuarios tienen un buzón personal de correo donde todos los mensajes recibidos se almacenan.

2.7.4.2 TRANSFERENCIA DE ARCHIVOS

La transferencia de archivos permite mover el archivo de una computadora remota a una local, aunque cada computadora tenga un sistema operativo y formato de almacenamiento diferente. Los archivos pueden ser de cualquier tamaño y pueden contener: datos, programas, reportes, etc.

2.7.4.3 ACCESO REMOTO

Con esta herramienta el usuario puede conectarse a una computadora que se encuentre en otro lugar dentro de Internet (remoto) desde una local. Una vez conectada y establecida la sesión con el nodo remoto, el usuario puede correr programas, capturar datos o hacer cualquier otra operación como si el nodo remoto fuera uno local.

2.7.4.4 ACCESO A BASE DE DATOS

Las redes con frecuencia ofrecen bases de datos centrales, que pueden consultarse desde cualquier nodo que este conectado a la red. En este caso una base de datos puede ser un directorio que contenga información de los usuarios de la red o artículos de un tipo específico. La mayoría de los nodos de Internet tienen disponibles colecciones de software, grabaciones de audio, publicaciones técnicas, normas, etc. Estos recursos podrán ser accesados por medio de las utilerías como TELNET y FTP del protocolo TCP/IP.

CAPÍTULO 3

Administración y métodos de seguridad para la protección de información en redes LAN, MAN y WAN

Para prever cualquier posibilidad de desastre es necesario que el personal de seguridad contemple los siguientes aspectos:

a) De uso general.- Funciones de contabilidad del uso de recursos y rendimiento, acceso a reportes.

b) Uso restringido.- Alarmas, configuración, detección y solución de fallas, registro de violaciones de seguridad, acceso de la base de datos de administración de redes.

c) Uso estrictamente restringido.- Alarmas de seguridad, control operacional, cambio de parámetros, diseño y planeación de redes, contraseñas (clave secreta de acceso) y perfiles de usuarios.

d) Control de ruteo. - Se trata de un método que consiste en reasignar a los usuarios el ancho de banda utilizado en la transmisión, es decir, cambiar la asignación anterior, lo cual asegura tener un alto nivel de seguridad, además de reducir riesgos en la transmisión.

Existen diversos métodos que se pueden adecuar a un uso particular, de acuerdo al tipo de red y de la seguridad que se desee para proteger la información. Lo mas importante es que se establezca un sistema de seguridad ya que las consecuencias de no hacerlo pueden ser mas caras y desastrosas de lo que se calcula.

3.1 RIESGOS EN LA RED

La evolución en las redes informáticas han originado que mas personas accedan a la información desde diversas computadoras, en ocasiones, ubicadas en diferentes localidades geográficas. Esto propicia que sea difícil detectar el lugar de acceso, éste es un reto complicado para la seguridad informática de una empresa, en donde se esta exponiendo la integridad de los datos, el cuidado del equipo y su funcionamiento.

Cuando se diseña y administra una red, es necesario tomar en cuenta la gran cantidad de factores que pueden ocasionar fallas en el sistema. De ahí que se tenga que desarrollar un análisis de riesgos enfocado a los que representan: los usuarios finales, las estaciones de

trabajo, redes de área local o LAN, redes de área metropolitana MAN, redes de área amplia WAN, los sistemas operativos, dispositivos de interconectividad, manejadores de bases de datos, bases de datos y archivos, además de las aplicaciones. Estos aspectos se deben analizar y tomar en cuenta los riesgos que cada uno de ellos puedan ocasionar, tanto de manera individual como en conjunto.

Al no existir una definición respecto a la protección en el ambiente de redes, se debe tener especial cuidado en el nivel de conocimientos y confiabilidad de las personas que utilizan la red. Por ejemplo, en casos de violación que no son reportados inmediatamente o cuando las redes se supervisan a tiempo. Es importante hacer hincapié al respecto, ya que el 75% de las violaciones en redes, son ocasionadas por el personal que trabaja diariamente con los dispositivos de la red debido a la poca aceptación de la empresa a las ideas de incorporar niveles y sistemas de defensa, como: políticas y procedimientos de seguridad. Entre los problemas mas comunes se encuentran la falta de seguridad que propicia la proliferación de intrusos de software como: virus, intrusos que se hacen pasar como usuarios para modificar o alterar el funcionamiento y la información del sistema e infinidad de riesgos.

3.2 DIMENSIÓN DE PROTECCIÓN

La seguridad en una red se puede definir como un conjunto de reglas a seguir que implican políticas, así como estándares y procedimientos a nivel software y hardware, con el fin de garantizar la máxima protección de la red y de sus componentes, así como la mínima intrusión para evitar problemas en la administración de dicha red. Sin embargo, en la realidad cuando se administra la red, no se le concede la debida importancia a los procesos de seguridad.

3.3 PROTECCIÓN FÍSICA Y LÓGICA DE LA RED

La protección física de la red incluye la seguridad del edificio o lugar de ubicación de la red; seguridad del equipo de computo y de telecomunicaciones; así como de los usuarios, esto se puede lograr tomando las siguientes medidas:

a) Controlar el acceso del usuario al equipo. Restringir el acceso a la estación o a la PC que opcionalmente debe de estar sin unidad de disco externo para evitar contagio de virus o robo de información que de lugar a la piratería, comprometer al usuario con la seguridad mediante un documento escrito y firmado.

b) Colocar los servidores en áreas protegidas.

c) Proteger el sistema de cableado y los sistemas de interconectividad.

Una vez que los puntos se llevaron acabo la siguiente parte de seguridad es a nivel lógico. Es decir, la planeación y el diseño de la red debe incluir contraseñas (clave secreta de acceso), códigos de acceso, definición cerrada de grupos de usuarios, técnicas de encripción, etc.

3.4 ADMINISTRACIÓN DE LA CONFIGURACIÓN DE LA RED.

En este caso se debe conocer la información detallada de todos los elementos que conforman su red, el hardware y software, sus características, ubicación, número de serie, versiones. Cuando el tamaño y la ubicación física de las redes hace complejo llevar un control de sus elementos, resulta de gran importancia para el usuario de la red tener actualizado el mapa de la configuración de su red y los elementos que la componen.

3.5 ADMINISTRACIÓN DE LA SEGURIDAD.

El administrador debe controlar el acceso solamente de cuentas autorizadas a cualquier punto de la red. Se obtienen reportes de fechas y nodo de acceso a la red. De esta forma se logra garantizar el acceso sólo al personal autorizado y se minimiza el riesgo de daño a la misma.

3.6 ADMINISTRACIÓN DEL RENDIMIENTO.

El administrador debe monitorear la utilización de la red detectando sobrecargas o cargas muy bajas que afectan el buen funcionamiento del sistema. Debe analizar también las áreas donde el tráfico tiende a crecer. De esta forma se puede estar un paso adelante en las necesidades actuales y futuras de la red. Con la administración del rendimiento se logra eliminar una de las características mas comunes en las redes cuando no se prevé su crecimiento, provocando con esto cargas de trabajo en ciertos sectores de la red. Con un buen análisis del rendimiento y sin necesidad de invertir en hardware o software adicional se puede incrementar el rendimiento del sistema.

3.7 ADMINISTRACIÓN DE FALLAS.

La detección de fallas a tiempo es un punto muy delicado por el costo que implica tener al sistema fuera de operación. El objetivo es determinar lo mas rápido posible el punto de la red donde se presenta una falla para que esta se corrija lo antes posible, ya sea a través de la administración remota de la red, o bien si se requiere del personal de servicio que acuda al lugar donde se presento la falla con las refacciones correspondientes. Es importante lograr detectar las fallas en la red antes de que ocurran, de tal forma, que el usuario no se entere de que estaba por presentarse una y que fue corregida en forma remota.

3.8 FUNCIONES DE SEGURIDAD DEL SISTEMA OPERATIVO DE RED.

El acceso a los datos es responsabilidad del sistema operativo de red NOS (Network Operation System; Sistema operativo de red), el cual permite el acceso a servidores, sistemas operativos y aplicaciones a través de contraseñas Se trata de un método sumamente utilizado, donde sólo el usuario debe conocer una palabra que el sistema operativo le pedirá al momento de entrar a través de una cuenta de usuario a los servicios de la red, además de verificar su validación, tiempo de expiración y limitantes para dicha cuenta. Estos dos pasos, normalmente consecutivos, prevén que los intrusos intenten introducirse a los recursos al iniciar una sesión en red donde se debe teclear la cuenta del usuario que le ha sido otorgada por el administrador y despues, el sistema verificará si la cuenta necesita contraseña, de ser así, la pedirá. De acuerdo al número de caracteres de la contraseña es la dificultad que se tiene para violar este paso de acceso, la longitud mínima puede ser establecida por el administrador.

El utilizar estos pasos para acceder a la red beneficia los niveles de seguridad en los siguientes aspectos:

1. Se realiza la identificación del usuario y la verificación de su contraseña.

2. Se llevará un registro de accesos y reportes de violaciones de seguridad.

3. Se creará una interfase con las funciones de seguridad del sistema operativo y algún método instalado en la red con una función activa de monitoreo y control de accesos.

El control es responsable del acceso físico y lógico a los dispositivos de la red, así como de llevar a cabo auditorías periódicas de los distintos accesos que se tuvieron a que áreas y que dispositivos se utilizaron, además de saber desde donde se verificó el acceso. Para llevar a cabo dicha tarea y evitar conflictos existen herramientas que sirven para:

a) Autenticación cuando se envían datos.- Mediante claves de acceso al área desde donde se va a enviar información y conocer la clave de acceso a donde se enviará la información.

b) Control de acceso.- Existe la autenticación por atributos personales, que es un método que permite al usuario el acceso a la red o a una aplicación de la misma a través del reconocimiento de su firma, voz, color de ojos, palma de las manos, huellas digitales u otro rasgo característico particular del usuario. Estos son sistemas de seguridad muy avanzados y costosos, pero igualmente efectivos que:

1. Aseguran la confidencialidad de la información.

2. Evitan el análisis de flujo de tráfico.

3. Aseguran la integridad de la información.

4. Evitan tener que confirmar que efectivamente el emisor es quien dice ser, así como el receptor.

3.9 MÉTODOS DE SEGURIDAD

Propondremos sólo la utilización de Firewalls para seguridad en conexiones a Internet, es decir, vigilar tanto el acceso de usuarios como de información que sale y entra a la red. Por otra parte, propondremos la Criptografía como método que nos asegure la integridad en los datos y a su vez la autenticación (todo esto en conexiones tanto internas como cuando se utilice como medio de comunicación a Internet).

3.9.1 CRIPTOGRAFÍA

El programa de encripción actúa como el cable decodificador en su televisor. El programa codifica los datos con un código secreto de manera que nadie puede encontrar sentido al mensaje mientras se está transmitiendo. Cuando los datos alcanzan su destino, el mismo

programa decodifica la información. El problema es que los códigos pueden ser descifrados por personas que se enriquecen siendo más ingeniosos que los sistemas de seguridad informáticos. Estas personas, a veces conocidas como hackers[✓] , convierten el penetrar en otros sistemas en su hobby. Esa es la razón por la que las técnicas de encripción necesitan ser continuamente actualizadas.

A los hackers no les interesa las conexiones a Internet a través de una cuenta telefónica, más bien les interesan las grandes compañías privadas y las computadoras de los gobiernos. De cualquier manera, el mejor sistema de seguridad es el sentido común. Por lo que debemos asegurarnos de que estemos contactados con empresas respetables y de que los programas de encripción se usen en ambos lados.

Los riesgos que supone el realizar transacciones a través de la red no son mayores que a los que nos enfrentamos en cualquier otro campo en el que realicemos negocios o investigación. Aunque hoy en dia es relativamente seguro el hacer negocios en Internet, hay muchas compañías trabajando continuamente para el desarrollo y mejora de la tecnología necesaria para convertir el Web en un medio de transmisión completamente seguro.

Algunos de los proyectos en desarrollo actualmente, incluyen:

3.9.1.1 CRIPTOGRAFÍA DE LLAVE SIMÉTRICA

Hasta no hace mucho, para hacer segura la información transmitida a través de las redes públicas se usaba una técnica llamada criptografía de llave simétrica. Este método tiene que ver con la encripción y desencripción de un mensaje usando la misma 'llave', que debe ser conocida por ambas partes para mantenerla en privado. El mensaje se encripta bajo algún código de substitución o transposición como se mencionará mas adelante, una vez encriptado y enviado el mensaje la 'llave' pasa de una parte a otra a través de otra transmisión, con lo que se vuelve vulnerable en el momento de enviarla.

Los códigos de substitución reemplazan datos en un mensaje con otros símbolos en forma sistemática. La substitución monoalfabética reemplaza cada símbolo con otro del mismo conjunto ordenado (reemplazaremos en el siguiente ejemplo una letra por su tercera consecutiva dentro del alfabeto en la palabra HOLA bajo esta encripción quedaría KROD).

Los códigos de transposición permutan o reordenan los símbolos del mensaje pero no los cambia.

3.9.1.2 CRIPTOGRAFÍA DE LLAVE PÚBLICA

La criptografía de llave pública disminuye el riesgo de que la información privada sea interceptada y permite que las partes se identifiquen positivamente una a otra.

[✓] HACKER - Es el término coloquial con el que se conoce a los piratas informáticos, que burlan la seguridad de las redes y se introducen en ellas, sin el debido permiso, con el único fin de husmear en su interior con ninguna buena intención.

En la criptografía de llave pública se usan llaves separadas para encriptar y desencriptar un mensaje de manera que únicamente el mensaje encriptado es transmitido. Cada parte de la transacción posee un 'par de llaves', con una relación muy particular, que permite que una encripte un mensaje que sólo la otra podrá desencriptar. Una de estas llaves está disponible al público y la otra es una llave 'privada'. Un mensaje encriptado con la llave pública de una persona no puede ser desencriptado con la misma llave, pero puede ser desencriptado con la llave privada a la que corresponde. Si usted autoriza una transacción con sus usuarios usando su llave privada, el usuario puede leerla con la llave pública correspondiente y sabe que sólo usted pudo haberla enviado.

3.9.2 FIREWALLS

Se da el nombre de "firewall" a un concepto de seguridad en Internet que se basa en el principio de la seguridad que ofrecían los muros de ladrillo que se colocaban entre las paredes de dos edificios, evitando con ello la propagación del fuego en caso de incendio. En el caso de Internet y basándonos en esta analogía, se crean barreras de seguridad que controlan los accesos a la red y a la información de nuestros equipos.

El propósito de un firewall en Internet es el de proveer un punto de defensa y un acceso controlado y revisado a servicios, ambos dentro de una red privada. Esto requiere que un mecanismo, selectivamente, permita o bloquee el tránsito entre Internet y la red protegida. Los Routers pueden controlar el tránsito a un nivel de IP, permitiendo o negando el tránsito con base en datos como: dirección de destino o puerto. Para implementar un firewall que resguarde, hay que permitir por lo menos un IP directo (determinado a un Ruteador por ejemplo), en el tránsito entre Internet y la red protegida, el cual será quien seleccione: permitiendo o denegando el acceso a la red.

3.11 IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD

Para implementar un sistema de seguridad es importante tomar en cuenta:

Los procesos.- La seguridad es un objetivo estratégico para la organización por lo que es importante la dedicación de personas y recursos para este fin, así como definir los objetivos de la seguridad en la red. Hay que formular un sistema de seguridad que contenga un ciclo de monitoreo, detección, acción y reporte, así como aplicar alta seguridad a sistemas y procedimientos que contemple la administración de la red.

Los productos.- Evitar productos que pueden ser sustituidos, vulnerables o que puedan eliminarse fácilmente, además que faciliten la auditoría.

Las personas.- Se debe involucrar a todo el personal, cualquier persona que trabaje en la organización puede provocar o evitar fallas en la seguridad de la red, por lo que es necesario convencer a los usuarios de la gravedad de los daños ocasionados por las fallas en seguridad, así como condicionar el acceso a la red a aquellas personas que hayan reincidido en violaciones a la seguridad.

Estas son algunas de las recomendaciones que se deben tomar en cuenta en caso de enfrentarse a un enemigo de su información que tal vez pretenda arruinar el trabajo de implementación de métodos y dispositivos de seguridad. Aunque cualquier acción que tomemos parezca exagerada será un punto mas a nuestro favor.

3.12 POLÍTICAS DE SEGURIDAD

Además de los productos de seguridad y las regulaciones desarrolladas fuera de su organización, deberá trabajar en resolver los asuntos que podrán ser locales o restringidos a su organización o a un subgrupo de esta. Tales asuntos de seguridad incluyen políticas de seguridad y controles de contraseña.

Se puede establecer dos instancias principales para el desarrollo de políticas de seguridad en su máquina. Estas instancias principales forman la base de todas las demás políticas de seguridad y regulan los procedimientos especificados para ser implementados.

La primera instancia dice que aquello que no se permite en forma expresa, esta prohibido; es el primer paso a la seguridad. Esto significa que si su organización ofrece un grupo de servicios preciso y documentado por escrito, todo lo demás que no este especificado esta prohibido.

En cambio una segunda instancia dice que aquello que no este prohibido de manera expresa se permite. Esto significa que a menos que usted indique en forma escrita que un servicio no esta disponible, entonces todos los servicios estarán disponibles.

Sin importar que decisión tome, la razón para definir una política de seguridad, y como quiera restringir la disponibilidad de sus recursos es determinar que acción deberá tomarse en caso de que la seguridad de una organización se vea comprometida. La política también intenta describir que acciones serán toleradas y cuales no.

3.13 POLÍTICAS DE SEGURIDAD DEL SITIO

Una organización puede tener muchos sitios y cada uno contar con redes locales, si la organización es grande, es muy probable que los sitios tengan diferentes administradores de red, con diferentes metas y objetivos. Si estos sitios no están conectados por medio de una red interna, cada uno de ellos podrá tener sus propias políticas de seguridad. Sin embargo, si los sitios están conectados a una red interna, la política de red deberá agrupar las metas de todos los sitios que estén interconectados.

La política de seguridad del sitio debe tomar en cuenta la protección de los recursos de la red como estaciones de trabajo, computadoras personales, servidores, ruteadores, compuertas, puentes, repetidores, cableado, software para administración e información entre otros.

3.14 COMO IDENTIFICAR LOS RECURSOS.

Al realizar un análisis de riesgos, se deben identificar todos los recursos cuya seguridad esta en riesgo de ser quebrantada. Es muy importante identificar todos los recursos de la red que

podrán ser afectados por un problema de seguridad. En las tablas 4-3 y 4-4, se lista los recursos de red que deben ser considerados al estimar las amenazas a la seguridad general.

3.15 AMENAZAS A LOS RECURSOS DE RED

Se debe prever que se cometan los mas comunes riesgos hacia los recursos de la red, como:

a) Acceso no autorizado: Solo se permite el acceso a los recursos de la red a usuarios autorizados. A esto se le llama acceso autorizado. Una amenaza común es el acceso no autorizado a los recursos de computo, el cual puede ser de diversas formas, como utilizar la cuenta de otro usuario para obtener acceso a la red y a sus recursos. En general, el uso de cualquier recurso de red sin el permiso previo se considera acceso no autorizado.

b) Divulgación de la información: La divulgación de la información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Se deberá determinar el valor a la sensibilidad (el grado en que la información almacenada en las computadoras puede ser afectada fácilmente por agentes externos ya sea naturales o provocada con malas intenciones). A nivel de sistemas, la divulgación de un archivo de contraseñas en un sistema Unix puede hacerlo vulnerable a accesos no autorizados en un futuro.

c) Servicio denegado: Las redes enlazan recursos valiosos como computadoras, programas y bases de datos, y proporcionan servicios de los cuales depende una organización. La mayoría de los usuarios de esas redes confía en estos servicios para realizar de manera eficiente su trabajo. Si estos servicios no están disponibles, hay una perdida en productividad.

Es difícil predecir en que momento y forma aparecerá la negación de un servicio y pueden haber diversas maneras de que nuestros servicios de red se vean afectados por:

1. Los efectos de un paquete extraviado.
2. A causa del flujo de tráfico.
3. Puede ser fraccionada al inhabilitar un componente crítico de la red.
4. Un virus puede restar velocidad o inhabilitar un sistema de computo al consumir los recursos del sistema .
5. Los dispositivos para proteger la red podrían revertirse.

Gracias a circunstancias tecnológicas como la gran disponibilidad de computadoras y la amplia conectividad que ofrecen las redes actualmente, la necesidad de tener seguridad incorporada en aplicaciones que involucren comunicación de datos, tanto local como remota, nos lleva a buscar una forma metódica que ayude a encontrar soluciones prácticas a dicho problema.

CAPÍTULO 4

Análisis de seguridad

En general un análisis de seguridad puede empezar definiendo el valor de la información que viaja por la red y su sensibilidad, es decir, que tan importante (en costo) es la información que se maneja, bien por procesos de la empresa o por necesidad de compartir datos; luego en el análisis de riesgos, se empieza identificando las amenazas sobre las aplicaciones y lo mas importante será tratar de cuantificar los daños que pueden causar en caso de que las amenazas sean ejecutadas. Habiendo localizado dichas amenazas en la red, se procederá a los sitios vulnerables y por último a identificar y ejemplificar los procesos de reconocimiento de los peligros.

4.1 EL INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES Y SU PROBLEMÁTICA DE SEGURIDAD

Dada la distribución geográfica de los edificios del ININ en el Centro Nuclear como se puede observar en la ilustración 4-1, se construyó un sistema de comunicaciones con una red basada en fibra óptica, que sea la espina dorsal de la red: con un cable de aproximadamente seis punto dos kilómetros de longitud. Este cable estaría muy por debajo de los 45 kilómetros de alcance promedio antes de requerir repetidores activos.

Para el Servicio de Comunicaciones se utilizó fibra óptica en el circuito exterior y redes locales en cada edificio, con cableado a base de par torcido de alambre de cobre y de cable coaxial. Se realizó la conexión según la norma IIIE 802.3 tipo Ethernet, con adaptadores electro ópticos y atenuadores, tableros de distribución, puentes de distribución (repetidores selectivos de tráfico en lugar de repetidores simples), más los instrumentos de administración, análisis y reconfiguración de la red.

Existiendo conectividad y compatibilidad entre los conmutadores de la red y el sistema central de cómputo para alcanzar las siguientes metas:

a) El control de los costos de uso del sistema de comunicaciones.

b) La emisión de los reportes de uso de los servicios de la red.

c) Evitar inversiones adicionales en el logro de esta conectividad.

Para tomar una determinación más adecuada con respecto a que opciones se debían tomar para asegurar la información que en la nueva estructura de la red del ININ se manejaría

dadas las necesidades el Centro de Computo invitó a dos expertos en comunicaciones para obtener la orientación necesaria y poder definir con precisión el problema y su solución.

Uno de estos expertos tiene los conocimientos en redes telefónicas y en redes de fibra óptica que se necesitan para evaluar la red actual del ININ, y conoce de métodos de seguridad que podrían ser implementados sin ningún problema en la red .

El otro experto es fabricante mundial de equipo de comunicaciones y servicios de seguridad además suscribe contratos internacionales con una empresa de tarjetas de cargo y con un consorcio de bancos europeos, entre otros. Al mismo tiempo, a través de tres miembros del Centro de Computo del ININ, se establecieron conversaciones de definición con otro experto en redes digitales de comunicación mediante fibra óptica e implementación de seguridad.

Entre las propuestas algunas de las más importantes son las siguientes:

a) Se deben tener en cuenta las políticas y las necesidades de la empresa, así como la colaboración con todas las partes que conforman la administración de la red y que intervienen en los procesos que tienen que ver con la seguridad de información.

b) Nunca suponer que las soluciones anteriores que se hayan tomado para resolver los problemas de seguridad presentados sean suficientes para enfrentar los problemas en un futuro. Todo esto, es porque se debe tener en cuenta los avances tecnológicos y la astucia de los nuevos intrusos de cada día.

c) Tener en cuenta los costos contra la efectividad del programa que se va a desarrollar para la seguridad de la información.

d) La gente encargada de la administración de la red debe tener cierta madurez y conocimiento del gran riesgo al que esta sujeta la información si no se plantea e implementa alguna forma de seguridad a los accesos de información, para ello debe incluir en sus planes y en su presupuesto los gastos necesarios para el desarrollo de los programas de seguridad, también debe tener en cuenta que éste es un objetivo fundamental de todo proceso de desarrollo de la empresa, la persona encargada de la administración de la red debe especificar los niveles de seguridad y las responsabilidades de las personas relacionadas con las aplicaciones distribuidas, pues tanto software, equipos y personas en su conjunto forman un complemento importante para el buen funcionamiento de todo programa de seguridad.

e) También hay que tener en cuenta la sobrecarga adicional que los mecanismos y contramedidas puedan tener sobre la red, sin olvidar los gastos adicionales que se invierten por su implementación.

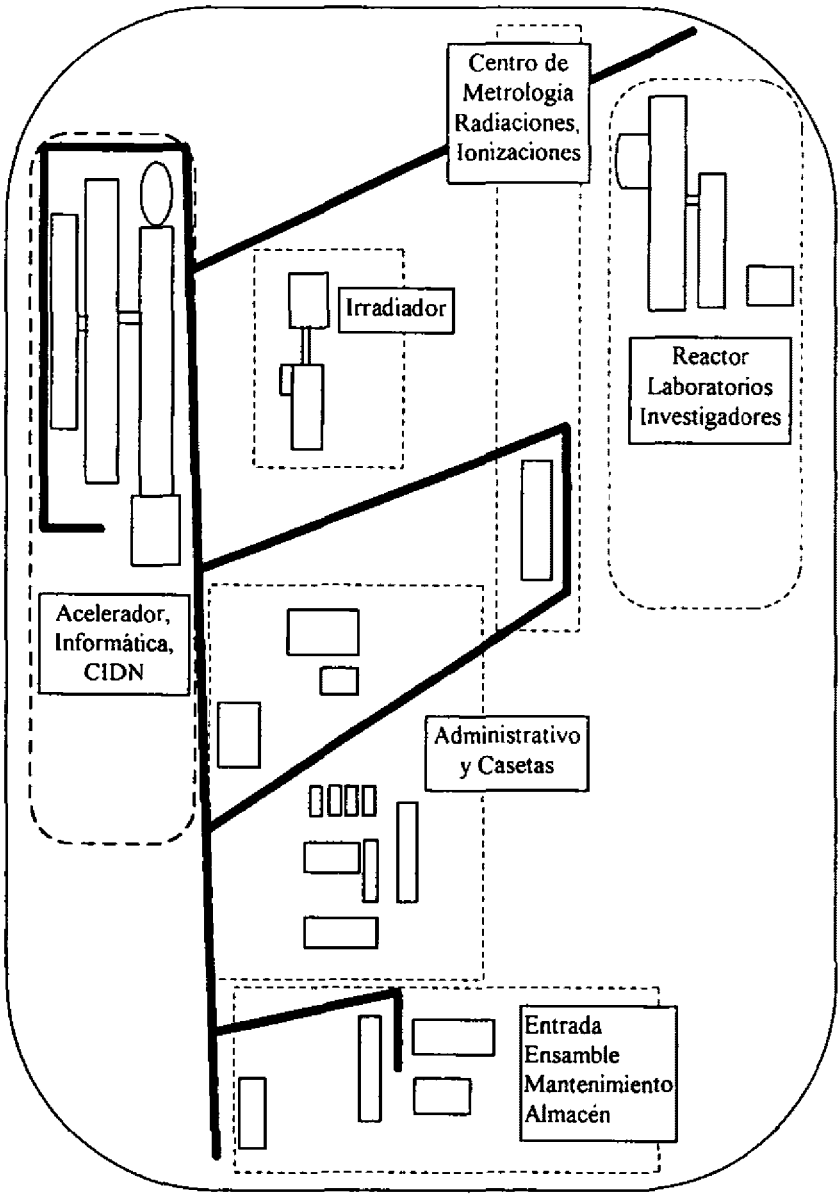


Ilustración 4-1 ESTRUCTURA FÍSICA DEL ININ.

4.2 ANÁLISIS DE RIESGOS

Con el análisis de riesgos que se realizó en la red del ININ, se pudo determinar las necesidades y la funcionalidad de las aplicaciones respecto a la seguridad.

4.2.1 INICIANDO UN ANÁLISIS DE RIESGOS

El análisis empieza con el supuesto de nuestra red sin riesgos ni amenazas los cuales pretendemos identificar; los riesgos de inseguridad en la red pueden ser definidos como el resultado de la descomposición y análisis de los puntos criticos de la red, que consiste en una descomposición del sistema, en sus partes. Estas partes cubren: software, hardware, personas y servicios de comunicación. Por ejemplo, una descomposición para el ININ de los elementos a proteger podría ser como se indica en la Tabla 4-1. Este análisis esta enfocado a identificar con precisión aquellas partes que los riesgos potenciales del sistema pueden impactar: el secreto, la integridad y la operación continua de las aplicaciones. Aquí es cuando, por primera vez, debemos pensar en las medidas de contingencia que se deben tomar para enfrentar los riesgos de las partes identificadas.

PARTES DEL SISTEMA	ELEMENTOS A PROTEGER
Personas	Vidas humanas.
Activos Cuantificables	Edificios, Muebles, Aire acondicionado y calefacción, Electricidad, Sistemas de control de incendios, Equipos electrónicos e Instrumentos experimentales y de medición
Hardware	Routers, Workstations, concentradores, Módem, cableado, , scanners y plotters, Impresoras Drives de cinta y discos, procesadores, tarjetas, teclados, estaciones de trabajo, computadoras personales, unidades de disco, líneas de comunicación, servidores.
Software	Sistemas operativo de red, Programas, utilerias, programas de comunicación, Aplicaciones como bases de datos, procesadores de texto y hojas electrónicas, Protocolos de comunicación y lenguajes de programación.
Datos	Datos de discos duros, diskettes, CD ROM's y cintas.
Conexiones de red	Ethernet 802.3, TCP/IP.

Tabla 4-1 DESCOMPOSICIÓN DEL SISTEMA EN EL ININ.

4.2.2 VALORACIÓN DE LA SENSIBILIDAD

Una vez realizada la identificación de las partes, la valoración de la sensibilidad (el grado en que la información almacenada en las computadoras pueden ser afectada fácilmente por agentes externos ya sea naturales o provocada con malas intenciones) nos lleva a darle un valor (que en algunos casos representará un costo en otro llevará a errores) a la información que se maneja, el valor se le puede dar por la importancia que tiene ya que son datos que se requieren para procesos especiales o bien por la precisión que representan y también debemos evaluar que tan críticos son: la información y los demás elementos de la organización como el software, hardware, y el valor de los servicios que provee la aplicación. Cuando hablamos de valor debemos tener claro que a la información y a los servicios de red se les debe asociar un monto simbólico, mientras que el software y el hardware se evalúan en dinero, por otra parte al término sensibilidad lo definimos por que tan vulnerable puede ser cada elemento a las amenazas, todo esto de acuerdo a los criterios que se describen a continuación.

a) Confidencialidad: La cual se refiere a proteger la información que se maneja en la red del ININ tanto del personal como de los investigadores. por medio de la red se transfieren datos de reportes de desarrollo de investigaciones, datos de nomina y asuntos de personal de accesos no autorizados, la finalidad es proteger la "revelación" de la información que viaja por los circuitos de un tercer atacante que intente capturar los datos o manipularlos según su conveniencia.

b) Integridad: El servicio de integridad es el que permite que la información sea adecuada, completa y auténtica en el momento de ser procesada, presentada, guardada o transmitida. En el caso del ININ transmitir datos de control de cualquier asunto relacionado con nomina o aspectos de investigaciones o que tenga que ver con asuntos de personal al ser enviados por la red, mínimo desea que estos no lleguen manipulados porque las consecuencias finales podrían ser desastrosas. En algunos casos mantener y garantizar esta característica es mas importante que la confidencialidad.

c) Disponibilidad: Como su nombre lo indica la disponibilidad se refiere a que todos los servicios de red se puedan prestar en determinado momento. Un esquema típico con el cual se maneja la disponibilidad es el de dos dominios. El primero coloca un valor a la información que se puede destruir completamente y nunca mas volverá a ser consultada. El segundo coloca valores de disponibilidad por ejemplo: el servicio de impresora esta disponible por 1 hora, 2 horas o lo contrario no esta disponible por 3 horas, etc.; este último dominio conocido como "over time" sirve para encontrar umbrales de disponibilidad; por ejemplo, "si después de 3 horas no esta disponible el servidor hay que programar un procedimiento manual".

Los anteriores conceptos nos llevan a pensar lo complejo y completo que debe ser nuestro proyecto de seguridad por el hecho que dentro del ININ el peso de los anteriores factores puede variar de forma indistinta.

4.2.3 AMENAZAS

Las amenazas se pueden clasificar en tres categorías:

4.2.3.1 AMENAZAS NATURALES.

Las amenazas naturales, incluyen principalmente, cambios naturales, que pueden afectar el desempeño de los elementos de la aplicación o a los sistemas de información que se manejan en la red[14]; en el ININ se observaron como posibles amenazas:

a) Descargas eléctricas por la zona que esta rodeada de bosque.

b) Que los equipos electrónicos se encuentren físicamente cerca de equipos que requieren de altas temperaturas o que manejen altos grados de radiación.

c) Que los equipos se encuentren cerca de aparatos con alto grado de magnetismo.

4.2.3.2 AMENAZAS ACCIDENTALES.

Las amenazas catalogadas dentro de las accidentales son las mas comunes y en la red del ININ se detectaron las siguientes:

a) Si un usuario teclea un login y una contraseña incorrecta, no debería tener acceso al sistema, sin embargo, si lo logra se determina como ERROR DE USUARIO.

b) Si un operador tenía su sesión abierta y olvidó salir del sistema, cualquier otro usuario con acceso físico a la máquina en cuestión de segundos podría hacer estragos causando entonces ERRORES DE LOS OPERADORES.

c) EN INSTALACIONES Y CONFIGURACIONES: Si el administrador modificó los archivos de inicialización de ciertos servicios y no activo los mecanismos de seguridad debidos, lo que resultó finalmente es un servicio sin seguridad; o bien, denominado ERROR ADMINISTRATIVO.

d) Si hay una trasferencia cuyos datos deberían estar encriptados y no lo están causará DATOS MAL PREPARADOS.

e) Si las impresoras están mal direccionadas y un documento confidencial fue enviado por impresión a un sitio donde no debería, nos dará ERRORES DE SALIDA.

f) Si el sistema de archivos se daño y una contraseña fue borrada o cambiada por otra nos causará ERRORES DEL SISTEMA.

g) ERRORES EN LAS COMUNICACIONES que podrían hacer que fácilmente se viole la confidencialidad de los datos, si una emanación electromagnética daña la dirección de destino de un mensaje, estos datos pueden ser revelados a personas indebidas.

[14] RAYA CABRERA, José Luis. REDES LOCALES Y TCP/IP. Alfaomega, 1997. Pág. 61.

4.2.3.3 AMENAZAS DELIBERADAS.

Las amenazas deliberadas tanto activas como pasivas son peligrosas para todo el sistema. Las activas incluyen accesos no autorizados, modificaciones no autorizadas, sabotaje, etc.; las cuales siempre o casi siempre involucran un "hacker"

Las amenazas pasivas son de naturaleza mucho más técnica y dentro de estas encontramos: emanaciones electromagnéticas[15] que pueden dañar la información sobre la red, microondas de interferencia, ruptura del cableado e información mal protegida o disponible sin ningún tipo de control (por olvido, error, etc.).

Como hemos podido observar en el análisis de las amenazas se trató de cubrir todos los puntos débiles de las aplicaciones para mantenerlas ágiles y con la facilidad de servicios disponibles el mayor tiempo posible con la debida supervisión de seguridad

ELEMENTO DE RED	AMENAZA
Sistema Operativo de Red	Acceso no autorizado. Modificación no autorizada. Negación de un servicio. Robo de información
Módems	Acceso de un hacker. Introducción de software peligroso. Revelación de los passwords de la estación
Estaciones de Trabajo	Acceso físico a las estaciones sin autorización. Robo o destrucción de información.
Servidores de RED	Acceso no autorizado y modificación . Acceso no autorizado por un hacker.
Ruteadores y Concentradores	Modificaciones de la configuración que causan negación de servicios y/o acceso a recursos adicionales

Tabla 4-2 ELEMENTOS IMPORTANTES DE LA RED DEL ININ Y SUS AMENAZAS.

4.3 DISEÑO

Es ahora el turno de definir especificamente cual es la vulnerabilidad a las amenazas identificadas y el grado del riesgo, se controlará planteando soluciones mediante

[15] RAYA CABRERA, José Luis. REDES LOCALES Y TCP/IP. Alfaomega. 1997. Pág. 61.

mecanismos de seguridad y/o medidas para contrarrestar las fallas que implican enormes riesgos, todo esto para evitar la ejecución de las principales amenazas dados los riesgos.

4.3.1 DETERMINACIÓN DE LA VULNERABILIDAD A LAS AMENAZAS

Para determinar la vulnerabilidad (cuanto perjudica el que se pierda o manipule determinado tipo de información), primero daremos un nivel de riesgo a cada amenaza, para ello se debe combinar la probabilidad de que la amenaza ocurra con la debilidad de la aplicación hacia dicha amenaza (carencia de recursos que no permitan el acceso a quien no lo debe tener) Para asignar un "peso" a cada amenaza por cada elemento de una red; hay que considerar 3 categorías de vulnerabilidad o posibilidad de ocurrencia como (1= baja, 2= media y 3= alta) que se asignaran a cada elemento de acuerdo a su debilidad a una amenaza como se mostrará mas adelante en la tabla 4-3. Para nuestro caso que es una aplicación distribuida adoptamos este método en donde simplemente asignamos un grado de vulnerabilidad para la aplicación por cada amenaza encontrada.

La localización de los edificios, el manejo de la información, las relaciones laborales, el manejo de los sistemas entre otras fueron razones que nos llevaron a identificar las diversas actividades que en cada área se desempeñan para poder determinar el riesgo que corren y según lo observado:

En INFORMÁTICA como se muestra en la ilustración 4-3, se encuentran equipos tales como: Terminales, Computadoras Personales y workstations, así como tres servidores y una Concentración de PC's. Su principal actividad es compartir recursos de software y de hardware. Es responsable de las comunicaciones confiables de voz y datos, administra y restaura las fallas en la red que trabaja bajo la plataforma Unix, da mantenimiento al equipo Módem, mantiene y restaura a cada uno de los Servidores. Elabora y da mantenimiento a los diversos sistemas, apoya a los investigadores con la parte programativa en los diversos lenguajes y los ayuda a paralelizar los programas que manejan grandes cantidades de información, cuando éstos lo requieren, maneja y mantiene el conmutador, entre otras actividades.

Las actividades en el área ADMINISTRATIVA como se presenta en la ilustración 4-4 son: En Seguridad física: Control de acceso a empleados, visitantes y clientes, registro de acceso a instalaciones así como seguridad en instalaciones. En el Almacén general: se utiliza el Código de barras, aquí se encuentra una gran concentración de información de entradas y salidas, esta área requiere compartir información con el Administrativo. En la Dirección general y dirección de administración: existe una gran concentración de información administrativa, se mantienen enlaces a equipo central para manejo de información presupuestal y contable. Se lleva además el control de caja y se elabora la generación de información al exterior. En las Casetas: se elabora la generación de información administrativa, de adquisiciones, personal, comercialización, servicios generales, asuntos internacionales, auditoria, correspondencia y archivo, organización y métodos, además se requiere un alto volumen de comunicación de voz, y necesita compartir información con administración, y por último el área de Mantenimiento: da seguimiento de órdenes de trabajo y coordina tareas de grupo de trabajo.

En el área de INVESTIGACIÓN Y APOYO como se ve en la ilustración 4-5 comenzamos con el CIDN (Centro de investigación y documentación nuclear) que es quien realiza comunicaciones al exterior, lleva el control de usuarios, permite la consulta a bases de datos Internacionales, realiza la generación de perfiles de interés, lleva el control de préstamo de libros, permite la transferencia de archivos, y con su página en INTERNET permite de manera remota hacer búsquedas de libros, revistas o artículos de investigación científica. El Irradiador tiene una alta concentración de investigadores y equipos de apoyo para ellos, además llevan a cabo intercambio de datos con el exterior, realizan búsqueda de información en bancos de datos internacionales y requieren de equipos de medición comunicados a PC's (computadoras personales). En el Acelerador y ensamble evalúan la calidad del ensamble, por lo que es una zona de riesgo y seguridad, realizan un control de producción en proceso de calidad, existe una alta concentración de información generada por el proceso y análisis de la fabricación, manejan información para seguridad radiológica y requieren de una red interna de supervisión. Por último en el Reactor y laboratorios existe una gran concentración de personal científico y administrativo que requiere de comunicación entre equipos de medición y PC's, además tienen constante comunicación al exterior, aquí también se localizan grandes concentraciones de datos para seguridad radiológica y datos de cajas de medición en esta área se realizan servicios externos e internos y se da seguimiento de proyectos.

En el área de SERVICIOS véase ilustración 4-6 se encuentra Ingeniería y electrónica, así como Talleres se encuentra la unidad de Ingeniería y desarrollo de equipos, se da seguimiento de ordenes de trabajo, se realiza un banco de información del estado de desarrollo de equipos para jefes de proyectos y administración, se elabora el diseño y adaptación de instalaciones y se lleva a cabo el diseño CAD y CAM por computadora. En el Irradiador gammas se encuentra el área de servicio, se lleva el control de producción en proceso y se encuentran las alarmas de seguridad radiológica. En Comercialización se lleva el estado de prestación de servicios externos, se lleva el control de éstos servicios y se promueve servicios al exterior. Por último en Metrología se tiene una unidad de comunicaciones confiables, se esta llevando acabo la construcción de ducto en esta área, se mantiene una unidad de servicio, se lleva acabo la emisión de certificados, se recopilan datos por comunicaciones entre PC's y equipos de medición se llevan a cabo servicios de proceso y se realizan mediciones de radiaciones alfa, beta, gama y neutrones.

4.3.2 LA COMUNICACIÓN FUERA DEL ININ (VOZ, DATOS E IMAGEN)

El ININ obtuvo dos direcciones clase C para su conexión con INTERNET mediante la UNAM, las cuales se tuvieron que segmentar como se muestra en la ilustración 4-2.

Los lugares a los que efectúa comunicaciones de envió y recepción de voz, datos e imagen es hacia los siguientes lugares:

DENTRO DEL D. F.: ININ-DF, UNAM, IPN, CINVESTAV, IMP, IIE, CFE, Conacyt, UAM, CNSNS, INFOTEC, INEGI, Oficinas de gobierno, etc.

DENTRO DEL PAÍS : Laguna Verde, Dos Bocas Veracruz, Maquixco, UAEM, IIE Palmira, Otras Universidades y Centros de Investigación

AL EXTERIOR DEL PAÍS: HACIA ESTADOS UNIDOS Y CANADÁ: GE Willmington, Los Alamos, ANL, Universidad de Notredame, etc.

HACIA AMERICA LATINA Y EL CARIBE: Argentina, Colombia, Brasil, Cuba, Chile, etc.

HACIA EUROPA: OIEA, INIS, Universidades, etc.

HACIA JAPÓN, COREA, RESTO DEL PACÍFICO

PARA USO AL INTERIOR DEL PAÍS: Plan de emergencia Radiológica externa, Laguna Verde, Maquixco, CNSNS

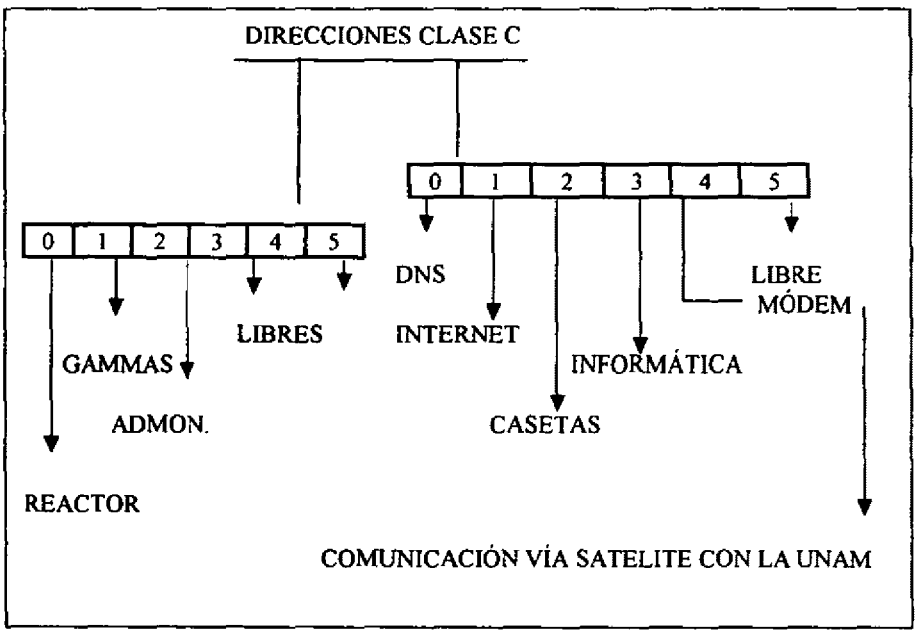


Ilustración 4-2 SEGMENTOS DE LAS DIRECCIONES CLASE C PARA LA CONEXIÓN A INTERNET EN EL INSTITUTO NACIONAL DE INVESTIGACIONES NUCLEARES.

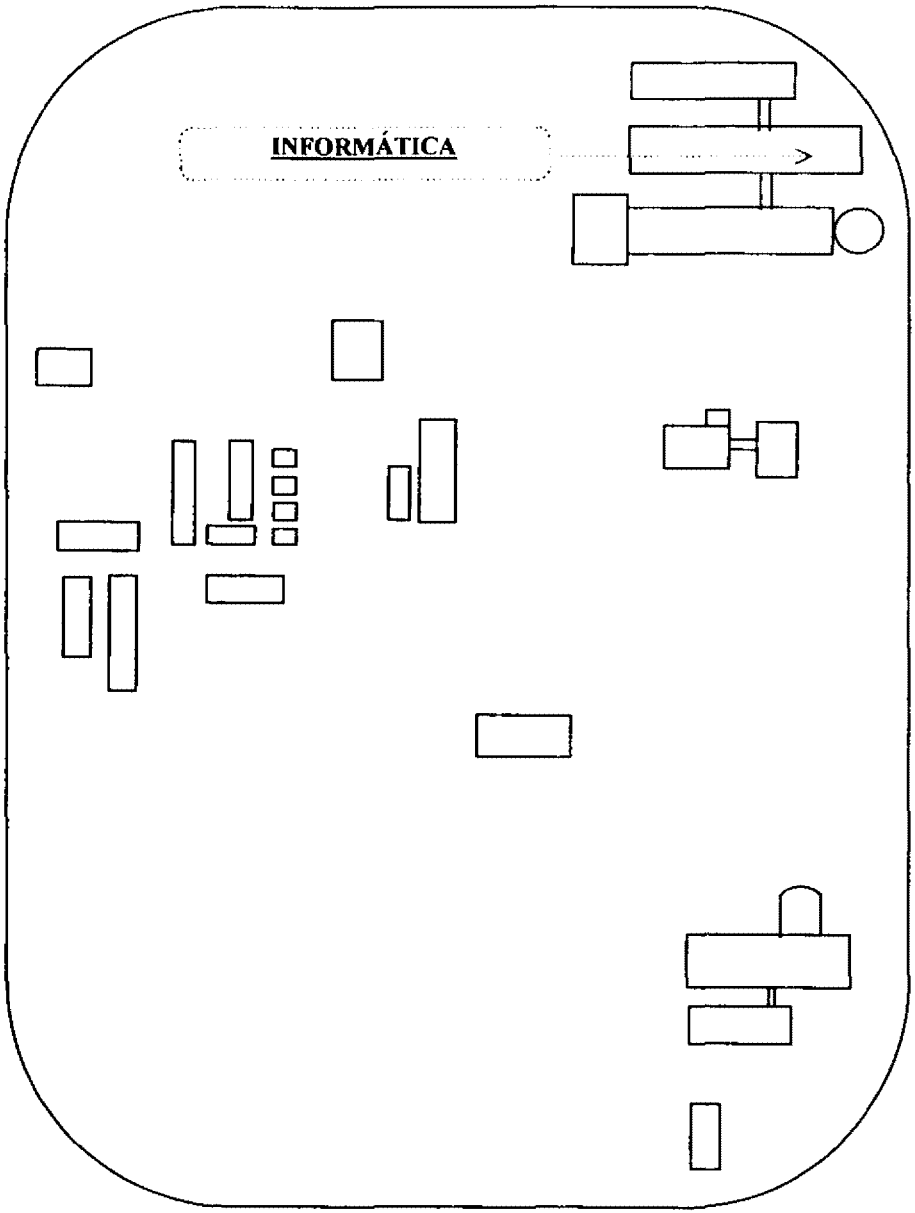


Ilustración 4-3 ÁREA DE INFORMÁTICA EN EL ININ.

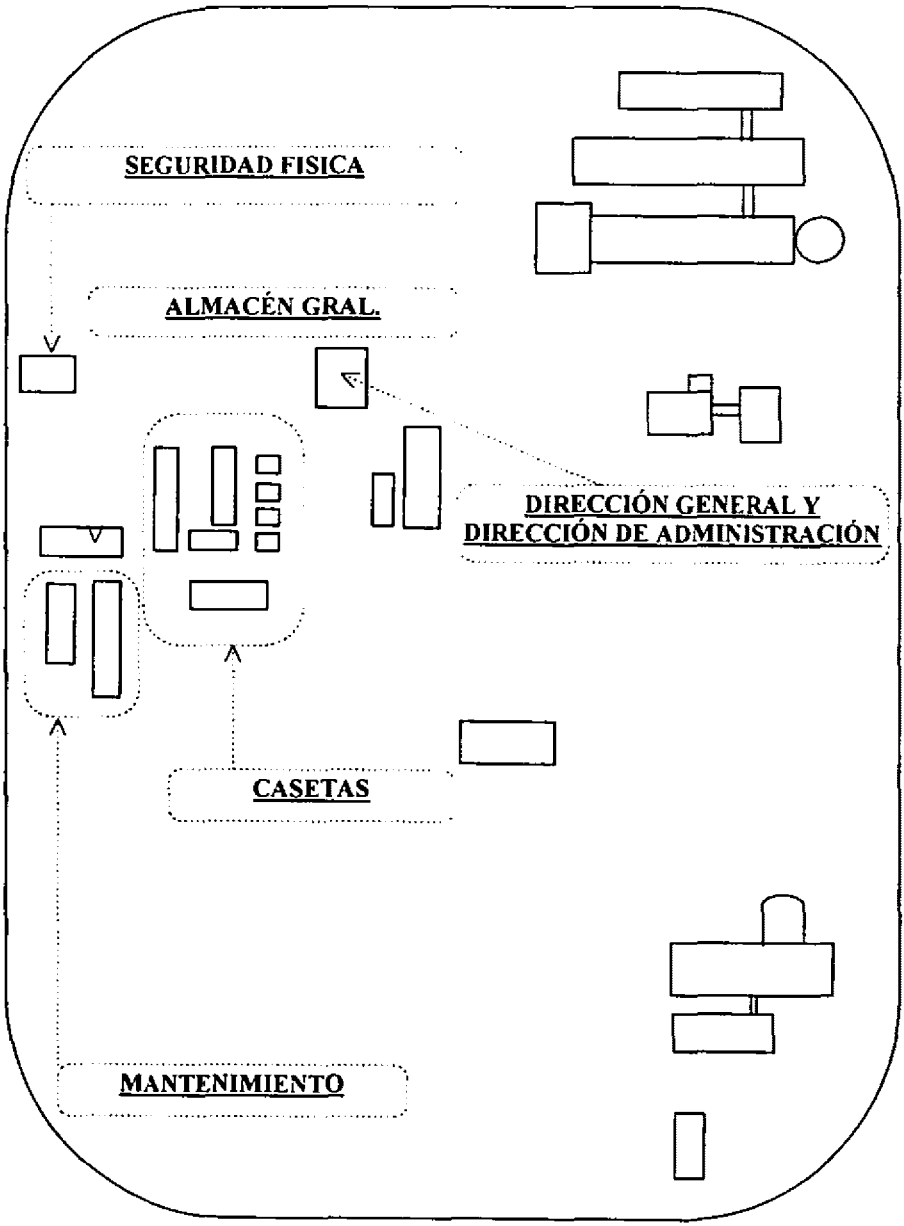


Ilustración 4-4 ÁREA ADMINISTRATIVA EN EL ININ.

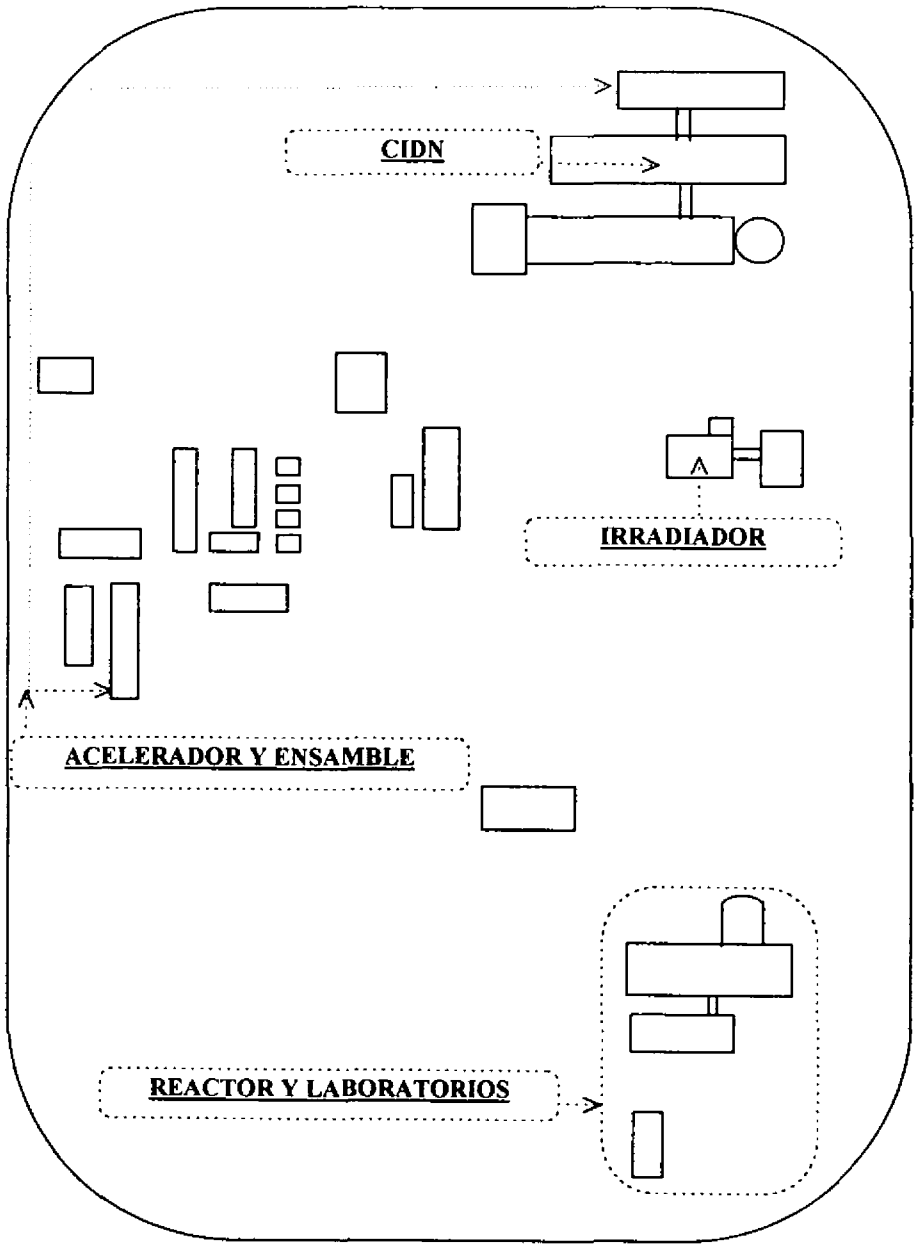


Ilustración 4-5 ÁREA DE INVESTIGACIÓN Y APOYO EN EL ININ.

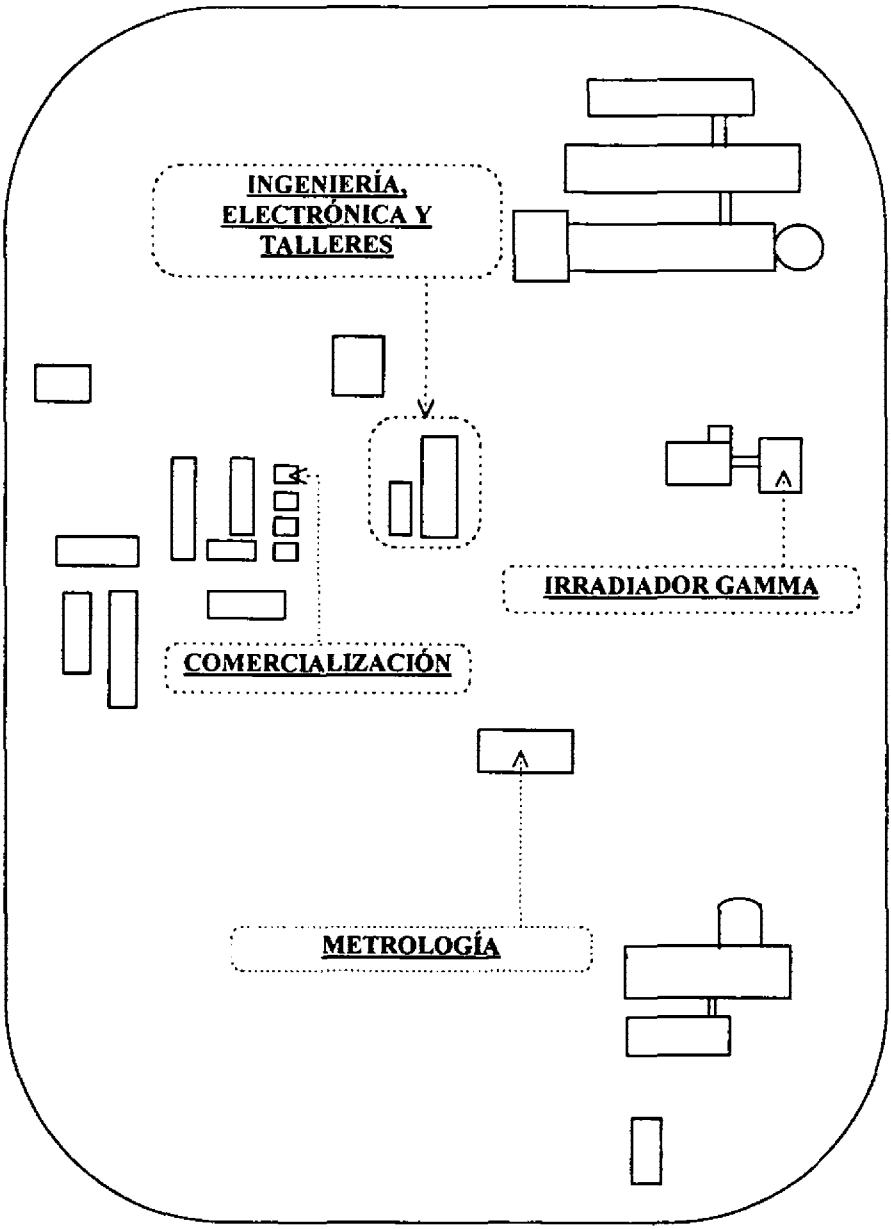


Ilustración 4-6 ÁREA DE SERVICIO EN EL ININ.

Como se puede observar el ININ se encuentra en constante comunicación con los continentes del mundo intercambiando información valiosa mediante INTERNET, por ello es necesario tomar medidas no tan sólo a nivel interno de la red sino también para la utilización del medio (INTERNET).

Para determinar el nivel de riesgo deben considerarse la severidad de la amenaza y el nivel de vulnerabilidad a la amenaza. Determinamos la severidad de acuerdo a las perdidas económicas que se producirían si la amenaza es perpetrada, todo esto siguiendo los resultados de la tabla 4-3.

APLICACIONES EN ANALISIS	OCURRENCIA DE UNA AMENAZA		
	Usuarios	Medio fisico	Natural
REACTOR	.6	.3	.1
GAMMAS	.5	.3	.2
ADMINISTRACIÓN	.6	.2	.2
CASETAS	.5	.3	.2
INFORMÁTICA	.4	.3	.3

Tabla 4-3 MATRIZ DE VULNERABILIDAD PARA AMBOS SEGMENTOS DE RED SEGÚN LA CONEXIÓN A INTERNET.(las ocurrencias están dadas en probabilidad).

4.3.3 APLICACIÓN DE MEDIDAS A LOS PROBLEMAS ENCONTRADOS

De acuerdo a la tabla 4-3 se encontró que las amenazas que generan los principales riesgos para ambos segmentos son los usuarios para lo cual es definitivamente necesario encontrar mecanismos (contramedidas) que ayuden a disminuir este riesgo a sus niveles mínimos o en algunos casos a eliminarlo por completo. Se debe tener en cuenta que dichas medidas tienen tres capacidades que incluyen: mecanismos de prevención, mecanismos de detección y mecanismos de corrección. Así mismo hay que considerar que existen medidas que pueden contrarrestar varias amenazas y a la vez tener 2 o 3 de las anteriormente mencionadas, en cuyo caso, es importante no recargar con medidas redundantes nuestro sistema. La tabla 4-2 de la parte del análisis será complementada ahora para producir una tabla donde se resuma en forma práctica cada elemento para elegir las medidas de acuerdo a las necesidades requeridas en cada parte de la red y las amenazas que producen los riesgos a atacar (ver Tabla 4-3).

ELEMENTO DE RED	AMENAZA	CONTRAMEDIDA
Sistema operativo de Red	• Acceso no autorizado • Modificación no autorizada • Negación de un servicio (ejemplo. introducción de software peligroso) • Robo de información	• Servicio de Identificación y Autenticación • Manejo de Password • Prohibición de acceso por módem
Módems	• Acceso de un hacker • Revelación de los passwords de la estación. • Introducción de software peligroso	• Servicio de Identificación y Autenticación • Alarmas en los cables para detectar intrusos. • Utilización de métodos de Encripción. • Limitar el acceso físico
Estaciones de Trabajo	• Acceso físico a las estaciones sin autorización • Robo o destrucción.	• Encripción y passwords dinámicos. • Control de acceso físico.
Servidores de red	• Acceso no autorizado y modificación	• Servicios de Identificación y autenticación
Ruteadores y Concentradores	• Modificaciones de la configuración que causan denegación de servicios y/o acceso a recursos adicionales.	• Restricción de acceso basado en un esquema bien manejado de passwords dinámicos. • Acceso restringido a dispositivos basado en el principio del menor acceso

Tabla 4-4 ELEMENTOS IMPORTANTES DE LA RED DEL ININ, AMENAZAS Y SUS CONTRAMEDIDAS.

Como se pudo observar de acuerdo a la tabla 4-4, los servicios de seguridad que se requieren son aquellos que puedan brindar a la red del ININ:

a) Confidencialidad: este servicio se encarga de proteger los datos transmitidos con el fin de evitar su revelación a personas no autorizadas (posibles atacante).

b) Integridad: el servicio de integridad pretende garantizar que los datos recibidos sean exactamente como los enviados por una entidad autorizada, es decir, durante la transmisión no existieron alteraciones (modificaciones, duplicaciones, inserciones, etc.) que afectaran el mensaje transmitido. Opcionalmente se pueden requerir mecanismos suficientes que permitan hacer la recuperación de datos destruidos por cualquier eventualidad.

c) Autenticación: como su nombre lo indica el servicio de autenticación está orientado a certificar que una comunicación es auténtica, dicho de otra manera es asegurar a un receptor S y que un emisor C sean realmente quien dicen ser. Así se asegurará que ningún tercero (atacante) ha interferido la comunicación y ha suplantado la identidad de uno de los verdaderos interesados. Colocamos las letras C y S puesto que muy frecuentemente sucede que la figura del emisor aparece como la de un cliente solicitando un servicio de un servidor, más aún cuando hablamos dentro del campo de las redes que soportan aplicaciones cliente/servidor y aplicaciones distribuidas.

d) Control de Acceso: en general con el control de acceso se quiere brindar protección contra el uso no autorizado de los recursos, o sea, se desea controlar: quien tiene acceso a un recurso, bajo que condiciones es posible dicho acceso y, finalmente, que puede hacer un posible usuario de un recurso si tiene acceso a este. En el ámbito de redes estos recursos bien pueden ser máquinas (host) cuyo acceso es controlado.

Como se mostró en la tabla 4-3 en varias de las contramedidas a las amenazas que se pudieron detectar y de acuerdo a los servicios de seguridad que se requieren, aunado a nuestro problema no olvidado de comunicación con el exterior mediante INTERNET se propone cubrir dos aspectos de seguridad:

El primero requiere la utilización de métodos de encripción en donde se observó que la vulnerabilidad de la información fue más alta; asignar áreas específicas a los servidores, es decir, áreas con alto nivel de vulnerabilidad en un servidor y aquellas que no resultasen tan vulnerables entonces manejarlas con otro servidor, sin olvidar que se requiere que todos los usuarios de la red que cuenten con áreas de trabajo en cualquiera de los servidores deben de contar con passwords y limitar ellos mismos el acceso a los demás usuarios con atributos a sus archivos y a sus directorios, a su vez exigir a los usuarios la depuración de sus áreas (mediante respaldos de su información) y bloqueo de aquellas cuentas que tengan ya vencimiento de utilización y por último tener una controlada asignación de IP para cada equipo electrónico y la configuración de red actualizada todo esto por escrito y con lo que respecta al acceso que se tiene a Internet emplear firewalls para el registro de la información que entra y sale y cuestionar ¿quién tiene acceso a la red del ININ y para qué?.

El segundo dadas las condiciones climáticas del Centro Nuclear, como primera medida es necesario dotar a cada una de las extensiones, servidores y equipos workstations con protectores contra descargas de rayos en la red por la inducción que éstos provocan, aunque se sabe que la fibra óptica es inmune a estos fenómenos. Ya que se tratará de una red de cableado mixto, esta precaución se hace indispensable. En 1986 se registraron daños severos a diez terminales conectadas al controlador de comunicaciones del sistema central,

que también resultó dañado junto con el computador mismo, debido a la inducción causada por la descarga de un rayo sobre el cable multipar telefónico que conectaba al conmutador con el controlador mencionado, todo esto para evitar nuevos riesgos.

Con las medidas anteriormente mencionadas se pretenden cubrir aspectos que sólo para el caso de aquella información que se consideró como confidencial se utilicen medidas de seguridad especificas, los mismos usuarios no deben permitir intrusos en sus áreas de trabajo (vía red), y por último, algunos de esas amenazas la propia naturaleza las impone, hay que prevenirlas.

4.4 COMPARACIÓN Y EVALUACIÓN DE LA METODOLOGÍA PROPUESTA PARA LA SEGURIDAD EN LA RED DEL ININ.

A continuación en la Tabla 4-5 se realiza el análisis de la metodología propuesta, en base a los resultados obtenidos en la implementación de la mayoría de los pasos.

Cabe hacer mención que la metodología como tal no se propuso, sin embargo, se fue construyendo en base a lo propuesto en la investigación para elaborar un buen proyecto de seguridad, y detectando las necesidades de seguridad en la red del ININ.

El éxito de cualquier proyecto parte de la plena conciencia en la investigación de seguridad que se realiza en la red que se desee implementar y de ahí, depende de la responsabilidad con que se lleve a cabo la implementación de las medidas que se tomen, para que los resultados sean los esperados.

ANÁLISIS	PASOS PROPUESTOS	PASOS REALES	RESULTADOS
		CONTEMPLAR ASPECTOS	
1 Se requiere llevar acabo una buena adquisición, asignación y administración de los equipos. 2. Se debe hacer un estudio previo que nos informe de las necesidades de los recursos que los usuarios requieren.	Configuración de la red.	1. En 1997 se llevó acabo un estudio con expertos y se implementó la red. 2. De acuerdo a los equipos existentes se reasignaron y se adquirieron nuevos. 3. Se diseñó la más optima configuración física y lógica de la red en el ININ.	1. Permite una mejor adquisición y asignación física y lógica de los equipos de acuerdo a su utilización. 2. Observamos una mejor administración de la red. 3. Se detectan con mas rápidez las fallas. 4 Se preve el crecimiento en la red.
1) Las amenazas son provocadas por los usuarios, pero también por el medio natural. 2) El ININ se encuentra a una altura considerable, rodeado de zona boscosa, lo que trae consigo, corrientes de aire y tormentas eléctricas que dañan los equipos.	1) Colocar los servidores en áreas protegidas. 2) Proteger al sistema interconectividad.	1) Se adquirió una planta para evitar los altibajos de energía eléctrica. 2) Se colocaron antenas pararrayos en lugares estratégicos. 3) Los servidores y los ruteadores se encuentran físicamente protegidos. 4) Se cuenta con un sistema de enfriamiento en caso de incendios.	1) Se ha disminuido el daño a equipos cuando se presentan tormentas eléctricas, aunque todavía peligran algunos en la red. 2) Cuando se incrementa la temperatura a niveles no permisibles en donde se encuentran los servidores, el sistema de enfriamiento ha controlado la temperatura.

Tabla 4-5 **COMPARACIÓN ENTRE LA METODOLOGÍA DE SEGURIDAD SUGERIDA Y LA METODOLOGÍA REALIZADA EN EL ININ.**

ANÁLISIS	PASOS PROPUESTOS	PASOS REALES	RESULTADOS
		CONTEMPLAR ASPECTOS	
1. Es necesario controlar el tiempo de vida de cuentas temporales (becarios). 2. Se deben cancelar las cuentas conforme su fecha de vencimiento para crear nuevas. 3. Se requiere disponer de el mayor espacio en memoria y controlar mejor que recursos se requerirán.	Asignación de perfiles de usuario	1. Se asignaron las cuentas en los distintos servidores. 2. Se especificó que actividades realiza cada servidor. 3. A cada cuenta se le especificó que recursos requieren utilizar, fechas de iniciación y de expiración.	1. Se lleva un mejor control administrativo de los recursos. 2. Se aprovecha mas la capacidad de los equipos. 3. Se evita posibles conexiones de usuarios que ya no tienen permiso de conectarse a la red. Nota: aún no se cuenta con un mecanismo automático que cancele dichas cuentas.
1) Se debe asignar a cada equipo que servicios debe prestar, ésto para evitar que un mismo servidor preste diversos servicios. 2) Se requiere de administración personal por cada servidor.	Control operacional de los principales equipos que conforman la red.	1) Se determinaron las funciones de servidores, de tal manera que cada persona sólo tiene acceso a los recursos que requiere. 2) Se asignaron permisos de utilización de acuerdo a sus actividades laborales. 3) Se asignaron administradores para cada uno de los servidores.	1) No se tiene fácilmente acceso a otro tipo de aplicaciones, restringiendo en gran parte el acceso a áreas confidenciales. 2) La asignación de administradores personales por cada servidor, mejoró la administración de dichos equipos.

Tabla 4-5 COMPARACIÓN ENTRE LA METODOLOGÍA DE SEGURIDAD SUGERIDA Y LA METODOLOGÍA REALIZADA EN EL ININ.

ANÁLISIS	PASOS PROPUESTOS	PASOS REALES	RESULTADOS
		CONTEMPLAR ASPECTOS	
Se requiere detectar que usuarios se conectan a la red mediante la realización de una bitácora de actividades.	Funciones de uso de recursos.	Se están desarrollando procesos para llevar un control de uso de los recursos, estableciendo normas.	1. Nos brinda los servicios de identificación y autenticación. 2. El administrador puede llevar una bitácora de actividades en la red. 3. Se restringe el acceso a la red.
1) Es necesario detectar que sectores de la red requieren de mayor atención. 2) Detectar que servidores y aplicaciones están prestando mas servicios.	Funciones de uso de rendimiento.	El administrador de cada servidor en la red lleva acabo el monitoreo constante de los equipos de supercomputo.	Permite prevenir en un futuro la saturación de los medios de interconectividad en ciertas áreas en la red.
Es de primordial importancia detectar a tiempo la intrusión de hackers informáticos.	Mecanismos para la detección de intrusos. (observación: continúa como propuesta la utilización de firewalls para la detección de hackers informáticos a nivel Internet.)	1°. Se limitó el acceso a las áreas en los servidores mediante el manejo de passwords. 2°. Se distribuyó la información de acuerdo a su confidencialidad en los servidores. 3°. Se están desarrollando procesos de control para el acceso a reportes.	1°. Se han logrado detectar intrusiones internas indebidas en ciertos sectores de la red. 2°. Se han tomado medidas cuando se detecta manipulación indebida de información, tales como sanciones temporales o definitivas.

Tabla 4-5 COMPARACIÓN ENTRE LA METODOLOGÍA DE SEGURIDAD SUGERIDA Y LA METODOLOGÍA REALIZADA EN EL ININ.

ANÁLISIS	PASOS PROPUESTOS	PASOS REALES	RESULTADOS
CONTEMPLAR ASPECTOS			
Se debe evitar el costo que implica el tener al sistema fuera de operación, además se debe evitar la repercusión que implica a terceros.	Detección y solución optima de fallas tanto en hardware como en software en la red.	1. Los administradores se encargan del monitoreo de la red para detectar las posibles fallas en la misma. 2. Se requiere personal para dar soporte y mantenimiento al hardware y software.	1. Se ha podido dar solución a las fallas que se han presentado en menor tiempo. 2. Se han evitando en parte la repercusión en costos y rendimiento en la red.
Se observó que algunas de las áreas que no contaban con passwords, los hackers las utilizaban para infiltrarse a la red. Es necesario tomar medidas para restringir estas áreas.	Cada área de usuario deberá utilizar contraseñas por cada servidor.	1) Se establecieron normas de restricción de cuentas. 2) Se bloqueo aquellas que no contarán con claves de acceso (passwords).	1) Se disminuyó el riesgo de perder integridad en la información. 2) Se disminuyó la sobrecarga en ciertos sectores de la red.
La relación costo-beneficio efectuada por la consulta a expertos demostró que por el momento no se requería de alarmas para la detección de intrusos, quizá en un futuro si se implementen.	Implementación de alarmas	No se implementó.	No hay resultados.

Tabla 4-5 COMPARACIÓN ENTRE LA METODOLOGÍA DE SEGURIDAD SUGERIDA Y LA METODOLOGÍA REALIZADA EN EL ININ.

ANÁLISIS	PASOS PROPUESTOS	PASOS REALES	RESULTADOS
CONTEMPLAR ASPECTOS			
En el estudio de la utilización del medio Internet para transferencia de información se detectó que se requiere del envió de voz, datos e imágenes, por lo que se propone a éstos usuarios utilicen métodos como la criptografía para proteger la integridad y autenticación de su información.	Utilización del método criptográfico.	Son contados los usuarios que han utilizado de criptografía, para la transferencia de su información.	Desconozco la optimidad de la utilización de éste método
Es primordial crear conciencia en quienes manejan información en la red, de lo eficaz que resultaría el seguir los lineamientos del sistema de seguridad, para obtener mayores y mejores resultados.	Registro de violaciones en la red.	1) Se diseñaron políticas de utilización de ciertos equipos. 2) Se limitaron las áreas de usuario. 3) Se establecieron sanciones a quienes incurran en violaciones.	1) Hay mas conciencia de lo que significa la integridad y perdida de información. 2) Hay mas gente involucrada en llevar acabo los métodos necesarios para salvaguardar la información.

Tabla 4-5 COMPARACIÓN ENTRE LA METODOLOGÍA DE SEGURIDAD SUGERIDA Y LA METODOLOGÍA REALIZADA EN EL ININ.

4.5 ASPECTOS IMPORTANTES EN LA METODOLOGÍA SUGERIDA

Para que la metodologia implementada tenga éxito se necesita de:

a) CONCIENCIA: Es necesario que cada miembro que integra al ININ y que esta involucrado en el sistema de la red, sepa valorar la información que maneja, para que tome con responsabilidad, las medidas que la parte administrativa proponga y que por su parte también contribuya a que la información cuente con los debidos métodos de seguridad.

b) CAPACITACIÓN: Se debe capacitar a todo el personal involucrado directa o indirectamente con la red, a que conozcan tanto su estructura fisica como lógica, que conozcan mas de los recursos que se ponen a su disposición mediante la red, así como también que conozcan de los métodos de seguridad y de las normas que se establezcan para el manejo de la red, todo esto con el fin de evitar que los propios usuarios sean quienes provoquen fallas en la red, o en alguna parte del sistema de seguridad.

c) REALIZAR UN ESTUDIO COSTO - BENEFICIO: Es necesario conocer hasta que punto es benéfico para la empresa invertir en un proyecto de seguridad, y si este es optimo, antes de tomar cualquier decisión, para evitar que futuras modificaciones repercutan en inversiones a largo plazo, actualizaciones drásticas o bien el sistema no se adapte en su totalidad a las necesidades de la red.

d) REALIZAR UN ANÁLISIS DE LAS POSIBLES FALLAS EN EL SISTEMA DE LA RED: Siempre ofrecerá una mejor garantía de detección de puntos críticos en una red, si primero estudiamos parte por parte cuales son aquellos sitios de primordial restricción para implementar seguridad, ya que con ello tendremos la certeza de que estaremos atacando los puntos débiles y no únicamente tratando de adivinar cuales son los posibles medios de infiltración de hackers en la red.

e) CONSULTORÍA EXTERNA: Siempre es necesario acudir con los expertos para tomar puntos de vista, o asesorías en cuanto a alguna situación problemática que de manera interna quede fuera del alcance de los involucrados resolver, esto reducirá costos y tiempo en espera y ayudará a quienes les interese a conocer y a aprender mas de las posibles fallas en un sistema de seguridad o de la red. Incluso antes de aprobar la implementación de cualquier proyecto de seguridad es preferible consultar con expertos que tan beneficioso y perjudicial puede ser llevar a cabo dichas propuestas.

f) PLAN DE IMPLANTACIÓN: Es bueno implementar una a una las decisiones estratégicas, y analizar que tan benéfico o perjudicial resulta el implementar cada una de dichas medidas, puesto que si todas se implementarán de manera simultánea y alguna de ellas no es tan benéfica como se espera, ésta puede repercutir en todas las demás y no se visualiza si el sistema de seguridad funciona correctamente y de acuerdo a lo que se propuso o no.

g) PLAN DE MEJORA CONTINUA: Todo proyecto que se implemente debe pensarse a cierto plazo, sin embargo y sobre todo en cuanto a computación se refiere existen avances, por lo que, en ciertos momentos puede que sólo se requiera de la actualización de algunos de los medios que se utilizaron para el sistema de seguridad, y en otros casos algunos de los medios que se utilizaron hayan quedado obsoletos y sea necesario volver a reestructurar el sistema de seguridad. Aunque lo que se desea es que la mejora sea parcial no total, pues esto último daria a entender una mala toma de decisiones y por lo tanto una mala inversión en el anterior sistema de seguridad.

CONCLUSIONES

1. Definitivamente contar con un proceso metódico para la implementación de seguridad en cualquier red es una verdadera necesidad, pues cada etapa permitirá definir un proceso gradual de desarrollo, y de una mejor visualización de aspectos que probablemente antes no habían sido contemplados.

2. Debemos evitar gastos y esfuerzos inútiles en medidas inadecuadas e inactuales, por ello propongo que en todo proyecto primero se debe tener una evaluación de todos los aspectos que requieren de servicios de seguridad y discernir las medidas que se emplearán de acuerdo a las necesidades de los distintos sitios, para que nuestra implementación tenga éxito, debe ser a la medida de la situación.

3. Identificar la vulnerabilidad a una amenaza es tal vez la parte clave dentro del análisis de riesgos pues permite elegir posteriormente un mecanismo que ayude a disminuir la probabilidad de que ocurra dicha amenaza.

4. Existen diversas directrices, y métodos para mantener la seguridad informática, sin embargo, es importante cubrir aspectos de seguridad, sin sobreproteger la información a tal grado que después nos resulte imposible el acceso a dicha información en la red.

5. Antes de implementar cualquier medida se debe contemplar que hay avances en la tecnología, lo cual puede resultar una desventaja si empleamos métodos o implementamos medidas que pueden quedar obsoletas, por ello es primordial que nuestro proyecto cubra las necesidades de seguridad a largo plazo y tener presente que tanto los hackers como la tecnología avanzan y que de no observar esto, podemos a corto plazo quedar vulnerables ante probables intentos de robo o manipulación de información.

6. Para que el proyecto de seguridad tenga una exitosa terminación es necesario tener un objetivo claro y consiente de lo que se persigue, y que tanto del personal que tiene el acceso a la red, como la parte administrativa tomen conciencia que la seguridad dependerá de que contribuyan en las medidas que se tomen.

Se observó que en el momento de la toma de decisión para la implementación de la metodología, hubo que consultarse a expertos para realizar estudios costo - beneficio, y algunos de los pasos propuestos fueron descartados, otros demostraron no arrojarían los resultados esperados y en la mayoría de los aspectos propuestos los resultados fueron benéficos, todo esto lo podemos observar en la tabla 4-5. Por lo que la metodología de seguridad idónea para implementarse en el ININ consiste de los siguientes pasos:

1. Realizar una buena configuración de la red.
2. Colocar los servidores en áreas protegidas, así como también proteger al sistema de interconectividad.
3. Asignación de perfiles de usuario.
4. Control operacional de los equipos que conforman la red.
5. Funciones de uso de recursos.
6. Funciones de uso de rendimiento.
7. Funciones de acceso a servidores.
8. Detección de fallas tanto en hardware como en software en la red.
9. Mecanismos para la detección de intrusos. (observación todavía sigue como propuesta la utilización de firewalls para la detección de hackers informáticos a nivel Internet, no se puede proponer aún como válido la utilización de éste método para la red del ININ).
10. Utilizar contraseñas para todas las áreas de usuario en los servidores.
11. Utilización del método criptográfico (se desconocen aún los resultados).
12. Registro de violaciones en la red.

En base a la experiencia adquirida se comenta que:

LAS METODOLOGÍAS SE ADAPTAN NO SE COPIAN, UNA METODOLOGÍA COPIADA ESTA CONDENADA AL FRACASO.

GLOSARIO

APLICACIÓN: Es aquella que lleva a cabo el trabajo solicitado por el usuario.

BRIDGE (PUENTE): Es un sistema formado por software y hardware que permite conectar dos redes LAN entre si. Se puede colocar en el servidor de archivos de comunicaciones.

CONCENTRADOR (HUB): Son equipos que permiten compartir el uso de una línea entre varias computadoras. Todas las computadoras conectadas a los concentradores pueden usar la línea, pero no de forma simultánea, ni utilizando distintos protocolos, ni distintas velocidades de transmisión.

CPU: Unidad Central de Proceso, que contiene a la Unidad Aritmética y Lógica, a la Unidad de Control y a la Unidad de Memoria que contiene tanto a la Memoria ROM como a la Memoria RAM.

DNS (DOMAIN NAME SYSTEM): Es el sistema de nombre de Dominio, un esquema para la traducción de direcciones internas de Internet en cadenas de caracteres y palabras con significado de nombres de usuario y lugares de conexión.

ESTACIÓN DE TRABAJO: Mientras un equipo PC no se conecta a la red se denomina Computadora Personal; y en cuanto utiliza la red se convierte en estación de trabajo.

FIBRA OPTICA: Esta formado por un núcleo de material transparente muy fino, rodeado de otro material con distinto índice de refracción. De esta forma las señales luminosas que viajan por el núcleo son reflejadas por la capa externa, llegando al extremo del cable.

FTP (FILE TRANSFER PROTOCOL): El protocolo de transferencia de archivos es una aplicación de Internet que permite transferir archivos de una computadora a otra.

GATEWAY: Es un sistema formado por hardware y software que permite las comunicaciones entre una red LAN y una gran computadora (mainframe). Se suelen colocar en el servidor de comunicaciones.

HACKERS : Es el término coloquial con el que se conoce a los piratas informáticos, que burlan la seguridad de las redes y se introducen en ellas, sin el debido permiso, con el único fin de husmear en su interior o hacer pequeñas travesuras.

HIPERTEXTO: Es un método de presentación de información mediante el cual al seleccionar cualquier palabra presente en el texto se puede ampliar la información sobre la misma; es decir, cualquier palabra, objeto de duda se encuentra enlazada con otro documento que pueden ser tanto textos como gráficos o sonido. Estos textos se encuentran en el WWW (World Wide Web). De Internet.

INTERFAZ: Es el cable que une a la computadora con el módem.

INTERNET: Es una red intermediaria que conecta redes en red.

MAIL (CORREO ELECTRÓNICO): Es una aplicación que permite enviar mensajes a otros usuarios de la red sobre los que este instalado. En Internet el correo electrónico permite que todos los usuarios conectados a ella puedan intercambiarse mensajes.

MAINFRAME: Son equipos caros y reservados. Estos equipos ocupaban edificios no estaban diseñados para dar respuesta directa (on-line) a las ordenes de un usuario, usaban el método de procesamiento por lote, usaban tarjetas perforadas que contenian datos y programas introducian las tarjetas al ordenador y al dia siguiente enviaban a los usuarios los resultados impresos.

MULTIPLEXOR: Son equipos que permiten tener más de una comunicación simultánea por una sola línea. Cada una de las comunicaciones opera como si tuviera la línea de forma exclusiva, pudiendo utilizar diferentes velocidades y protocolos en cada una de ellas.

MÓDEM: Es un equipo que convierte las señales digitales de la computadora a las analógicas de la línea (modulación) las envía a otra computadora y cuando recibe este, las vuelve a convertir de analógicas a digitales (demodulación).

NFS (NETWORK FILE SYSTEM): El sistema de archivo de red es un protocolo que permite que una computadora pueda acceder a los archivos de otra computadora como si fuesen propios. El protocolo NFS esta incorporado dentro del propio sistema operativo, y con el se evitan las extrañas sintaxis que a menudo deben utilizar los usuarios para acceder a archivos de otras computadoras dentro de una red.

NORMA IEEE 802.3: Se encuentra basada en los primeros niveles del modelo OSI. Dividiendo el nivel de enlace de datos en dos subniveles: uno de control de enlace lógico (Logic Link Control LLC) y otro de control de acceso al medio

(Media Access Control MAC), el LLC se ocupa de la colisión de detección de datos.

PAQUETE DE DATOS: Contiene cuatro partes:

1. Cabecera - Contiene un identificativo del bloque de comienzo, el identificativo de destino del paquete y el identificativo del origen del mismo, y la información referente al protocolo que se utiliza.

2. Información - Contiene el texto o la parte que se va a transmitir.

3. Control de errores - Contiene la información necesaria para que el sistema pueda verificar si los datos del paquete se han recibido correctamente.

4. Bloque final - Contiene la información que indica que el paquete ha finalizado.

PROTOCOLO: Son reglas que garantizan la compatibilidad del software y el hardware de redes suministradas por distintos proveedores.

PUNTO A PUNTO: Es un protocolo utilizado para acceder a Internet mediante una línea telefónica y un módem.

SERVIDOR: Es una computadora que tiene como objetivo primordial interconectar computadoras para compartir recursos, aplicaciones e información.

S. O. DE RED: El sistema operativo de red sirve para la realización de procedimientos de control y seguridad de red.

TOPOLOGÍA: Son la unión física de conexión entre los dispositivos de red.

TRANSMISIÓN: Es el proceso de transporte de la información codificada de un punto a otro. En estas se acepta la información, se convierte a un formato que sea fiable y rápido de transmitir, se transmite a determinado lugar y una vez recibido se vuelve a convertir para entenderse.

UNIX: Es un sistema operativo de red que ofrece servicios de multitarea y multiusuario.

BIBLIOGRAFÍA

A FONDO: REDES DE ÁREA LOCAL
STAN SCHATT
ED. ANZOS, 1987
Pág. 294

INTERNET FIREWALLS AND NETWORK SECURITY
KARANJIT SIYAN, PH. D.
ED. NEW RIDERS PUBLISHING INDIANAPOLIS INDIANA
Pág. 407

REDES DE ORDENADORES
ANDREW S. TANENBAUM
ED. PRENTICE HALL, 1991.
Pág. 759

REDES LOCALES Y TCP/IP
JOSÉ LUIS RAYA CABRERA
CRISTINA RAYA PÉREZ
ED. ALFAOMEGA, 1997
Pág. 185

TODO SOBRE INTERNET
ED. MARCOMBO, 1996
Pág. 407

SEMINARIO BÁSICO DE REDES LOCALES QUE IMPARTE SOPORTE TECNOLÓGICO EN APLICACIONES Y FUNCIONES DE INFORMÁTICA S.A. DE C.V.
TECNOLOGICO DE TOLUCA, OCTUBRE DE 1996.

SEMINARIO DE SEGURIDAD DE INFORMACIÓN EN REDES QUE IMPARTE DGSCA.
UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO, FACULTAD DE INGENIERÍA, NOVIEMBRE DE 1996.

INTERNET:
http://www.inin.mx