01132
16


# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

# SEGURIDAD EN INTERNET HERRAMIENTAS Y SOLUCIONES

# T E S I S

QUE PARA OBTENER EL TÍTULO DE:

## INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

LUIS OSCAR BARRAGÁN VÁZQUEZ

LAURA PALMIERI PINEDO

LUDYVINA SÁNCHEZ ROSAS

NICOLÁS VELÁZQUEZ ALVARADO

DIRECTOR DE TESIS:
M. I. JORGE VALERIANO ASSEM


México D.F. 2003

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

**UNAM – Dirección General de Bibliotecas**
**Tesis Digitales**
**Restricciones de uso**

**DERECHOS RESERVADOS ©**
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.
NOMBRE: Laura Palmieri Pinedo
FECHA: 27 - Junio 2003
FIRMA: Laura Palmieri Pinedo

*DEDICACIÓN Y AGRADECIMIENTO:*

*A DIOS*
*Padre Celestial gracias por todas las bendiciones recibidas y por haberme permitido llegar hasta este punto de la vida.*

*A MI MADRE*
*GEORGINA VÁZQUEZ GONZALEZ*
*Por que me diste la vida, y me enseñaste con tu ejemplo a perseverar, porque me apoyas y quieres.*
*Madre te quiero y dedico esta Tesis con todo mi amor.*

*A MI PADRE*
*LUIS BARRAGÁN VILLAVICENCIO*
*Quien me ha enseñado a valorar la vida y verla desde un punto de vista distinto.*
*Por ser un gran Padre y poner en mi una semilla de bondad y amor.*
*Te dedico esta Tesis ya que con tus comentarios me motivaste a terminar mi Carrera.*

*A MIS HERMANOS*
*CLAUDIA, ISAAC Y MA. TERESA*
*Les agradezco por su amor, confianza y respeto por que siempre logramos mantenernos unidos y eso me motiva a seguir adelante.*
*Les dedico la presente como una forma de cariño.*

*A MI ESPOSA*
*BLANCA GEORGINA DURAN ALVARADO*
*Quien desde que nos casamos me apoyo e impulso para no desanimarme, agradezco su comprensión, paciencia, dedicación y esfuerzo.*
*Te dedico la Tesis con todo mi amor y como un logro de ambos.*

*A MIS HIJOS*
*DAFNE Y OSCAR*
*Les doy las gracias por la compresión que me han tenido, porque son una motivación para mi progreso, porque me quieren y apoyan.*
*Los quiero y dedico mi trabajo ya que cualquier esfuerzo que realice será poco, con todo mi cariño y amor.*

*LUIS OSCAR BARARAGAN VAZQUEZ*

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.
NOMBRE: Nicolás Vázquez Alvarado
FECHA: 27/Junio/2003
FIRMA:

TESIS CON
FALLA DE ORIGEN

Agradezco a Dios por el ángel
de la guarda que siempre me acompaña...
y a ti Marco, por ser ese ángel.

Gracias a mi madre y abuela por
el esfuerzo, cariño y voluntad.

A mi hermana, por quererme y apoyarme
en los momentos difíciles.

A mi amada Universidad por la oportunidad
de formarme como un ser independiente.

Laura Palmieri

TESIS CON
FALLA DE ORIGEN

C

**A mis padres (Pascual y Sofía):**
Porque siempre recibí lo mejor de ellos
y siempre guiaron mi vida.
Porque gracias a ellos soy una persona
feliz.

**A Pepe:**
Porque siempre ha estado a mi lado
apoyándome, amándome e impulsándome,
llenándome siempre de amor y
comprensión.

**A Dios:**
Porque siempre me ha permitido
lograr lo que he querido (y a veces más).
Por permitirme vivir y gozar de la vida.

**A la familia Soriano Avila:**
Por haberme permitido ser parte de ellos
y brindarme su apoyo y cariño.

**A Alstom T&D:**
Por las facilidades brindadas para
la realización de esta tesis.

A los que de una u otra manera hicieron
posible que este proyecto llegara a término.

**¡¡ GRACIAS !!**

**Ludyvina Sánchez Rosas**

TESIS CON
FALLA DE ORIGEN

*La muerte no es verdadera cuando se ha realizado correctamente la obra de la vida. A la memoria de mi padre, el maestro Juan Salvador.*

*Nicolás*

E

# TEMARIO


**INTRODUCCIÓN** ..... i

**CAPÍTULO 1. CONCEPTOS FUNDAMENTALES Y ARQUITECTURAS BÁSICAS** ..... 1
1. Definición de Red ..... 1
2. Componentes de las Redes ..... 1
3. Objetivos de las Redes de Computadoras ..... 7
4. Clasificación de las Redes de Computadoras ..... 8
5. Modelo OSI ..... 15
6. Modelo Internet ..... 17
7. Clases de Redes según su IP ..... 28
8. Técnicas de Conmutación ..... 30
9. Enrutamiento ..... 35

**CAPÍTULO 2. INTERNET** ..... 39
1. Historia de Internet ..... 39
2. Definición de Internet ..... 41
3. Servicios que ofrece Internet ..... 42
4. Tendencias de Internet ..... 52
5. Vulnerabilidades en Internet ..... 59

**CAPÍTULO 3. REDES Y SISTEMAS OPERATIVOS SEGUROS** ..... 63
1. Amenazas a la Seguridad ..... 63
2. Seguridad Externa ..... 72
3. Seguridad Interna ..... 83
4. Plan de Seguridad ..... 95
5. Evaluación de Sistemas Seguros ..... 105

**CAPÍTULO 4. SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES** ..... 123
1. Políticas de Seguridad entre una Red Privada e Internet ..... 124
2. Servicios de Protección al Proceso de Datos y su Transferencia ..... 140
3. Mecanismos para proveer Servicios de Protección ..... 144
4. Cultura de Seguridad ..... 149

**CAPÍTULO 5. PROPUESTA DEL TEMA DE SEGURIDAD EN REDES PARA LA ASIGNATURA DE REDES DE COMPUTADORAS** ..... 155
1. Incorporar el tema de "Seguridad en Redes", en la materia de Redes de Computadoras ..... 163
2. Incorporar la asignatura de "Seguridad en Internet, herramientas y soluciones", con carácter optativo ..... 168
3. Incorporar la asignatura de "Seguridad en Internet, herramientas y soluciones", con carácter obligatorio ..... 171

**CONCLUSIONES** ..... 181

**ANEXO 1. Criptografía** ..... 187
**ANEXO 2. Gestión de claves** ..... 191
**ANEXO 3. Netiquette** ..... 193

**BIBLIOGRAFÍA** ..... 195


F

# INTRODUCCIÓN

Todos los seres vivos tienen una forma específica de expresar sus emociones o sentimientos, el lenguaje es la manera en que el ser humano puede expresar lo que piensa o siente. Adicionalmente, la necesidad de trascender hizo que el hombre buscara formas gráficas para plasmar sus ideas y pensamientos, naciendo así la escritura.

Gracias a la escritura se han transmitido conocimientos de generación en generación, ha sido posible comunicarse sin depender de las distancias, conservar registros de dicha comunicación, así como formalizar actividades o acciones de toda índole. Al igual que la mayoría de áreas de conocimiento humano, la escritura es utilizada en forma especializada por las organizaciones militares y desarrollada altamente durante las actividades bélicas, ya sea para que los soldados reciban noticias de sus seres queridos o que los altos mandos requieran información sobre las condiciones y estrategias de batalla.

De lo anterior, es fácil desprender que, durante las guerras, surge la necesidad de proteger la información transmitida para garantizar su interpretación única y exclusivamente por el receptor en forma veraz, completa y oportuna. ¿Por qué? porque cuando el enemigo es capaz de interceptar la comunicación y conocer la estrategia de ataque de su adversario, está en condiciones de anticipar los hechos permitiéndose planear la huida, el contraataque, la defensa o el triunfo de la batalla. Por lo tanto, como la comunicación es vital, a toda la información enviada o recibida se le aplican procedimientos que generan una nueva escritura, a partir del mensaje original, con la intención de que únicamente el destinatario de un mensaje sea quien lo pueda leer. Con esta intención, las técnicas desarrolladas específicamente para cifrar información, conocidas como criptografía, se aplican en pro del secreto de información.

Por otra parte, la escritura se ha utilizado en diferentes actividades del hombre destacando su impacto dentro de la industria y la economía, importantes ramas del quehacer humano vinculadas estrechamente con su desarrollo y evolución. A través del tiempo, mediante la escritura se han formalizado o comprobado operaciones, transacciones, derechos y obligaciones entre personas u organizaciones, estableciendo formas e instancias para reconocer a cada uno de los participantes, sus facultades y la validez de los documentos. Con los avances tecnológicos y la evolución de los medios de comunicación, la representación gráfica y física de la información ha pasado a un nivel lógico, en donde las combinaciones de ceros y unos significan mucho más que un dato de computadora y de la misma forma, los documentos en papel disminuyen convirtiéndose en documentos electrónicos. Esta evolución en la representación, almacenamiento y difusión de la información tiene como consecuencia la necesidad de garantizar que, para un documento o comunicación en forma electrónica, tanto emisores como destinatarios o receptores son quienes dicen ser y por ende, tienen las facultades suscritas de participación; en este sentido, aparecen nuevas formas e instancias para certificación de los participantes, sus facultades y la validez de los documentos electrónicos.

Hoy por hoy, para las organizaciones públicas y privadas es indispensable poseer información veraz, completa y oportuna acerca del entorno nacional e internacional que, de igual forma que a las organizaciones militares, les permita tomar decisiones acerca del alcance o cobertura de sus operaciones o sobre las estrategias a corto, mediano y largo plazo. En este sentido, la información es considerada un activo fijo de cualquier organización que, como tal, debe protegerse y asegurarse pues las repercusiones de su pérdida o uso indebido pueden resultar cuantiosas. La información, en parte, es producto del funcionamiento de las organizaciones y la aplicación de resultados derivados de su análisis, constituye

una especie de realimentación a la organización para incrementar la eficiencia de las actividades diarias y hacerlas más eficaces.

Los sistemas computacionales han permitido almacenar y procesar grandes cantidades de información en menores tiempos y los sistemas de comunicación han agilizado su transmisión y publicación. La comunión de ambos conceptos, ha provocado que las redes de computadoras se conviertan en una herramienta indispensable para cualquier organización, orientando el uso y desarrollo de los sistemas distribuidos para facilitar el proceso e intercambio de información, la división de tareas y el aprovechamiento de los recursos compartidos.

La implantación de redes locales es una práctica común y de gran éxito en las que se enlazan las computadoras para comunicarse entre sí y compartir recursos dedicados o particulares de un equipo específico, todo dentro de las instalaciones de una organización, cuya extensión va desde una oficina hasta varios edificios contiguos o cercanos.

Para aquellas organizaciones que por su naturaleza se expanden como células ubicadas en diferentes territorios dentro de un país o en diferentes países, las redes locales sólo satisfacen requerimientos particulares a cada célula, pero las necesidades de información entre células sólo pueden cubrirse construyendo redes de área amplia privadas o haciendo uso de redes de área amplia de tipo público, todo dependerá de la capacidad económica e intereses de la organización. Lo cierto es que, para la mayoría de las organizaciones, resulta muy conveniente contratar un servicio de conexión remota mediante redes públicas que aventurarse a implantar un sistema de este tipo.

Adicionalmente, los avances tecnológicos y descubrimientos de nuevos materiales, han permitido desarrollar medios de transmisión de datos y conexión altamente eficientes y veloces; no obstante, en este sentido, la diferencia entre redes de un tipo u otro aún es notoria, siendo indispensable construir redes locales de alta velocidad interconectadas mediante redes de área amplia, privadas o públicas, cuyos tiempos de respuesta son varios cientos de veces más altos.

Después de la Segunda Guerra Mundial la incertidumbre sobre posibles ataques nucleares, despertó la preocupación de las fuerzas militares de los Estados Unidos de Norteamérica que, con la intención de mantener comunicación permanente en caso de un ataque de esa magnitud, integró una comisión para crear un sistema capaz de enviar y recibir información, aún cuando los medios de transmisión fuesen destruidos. Muchos de los investigadores que se unieron a este proyecto de enlace permanente, lo hicieron con la intención de compartir información científica en forma dinámica.

Con el tiempo, surgieron sistemas que permitían el envío de información punto a punto; esto es, dos equipos enlazados a través de algún medio de comunicación, inician una sesión específica de transmisión de información, la cual debe mantenerse viva para hacer posible el intercambio de datos y se concluye para dar por finalizada la comunicación. Más adelante, el avance tecnológico permitió la existencia de redes privadas con la capacidad de abarcar áreas geográficas extensas; sin embargo, para intercambiar información entre ellas, varias de esas redes establecieron conexiones con la red pública llamada Arpanet, teniendo que adaptarse y cumplir con las restricciones tecnológicas de enlace que ésta les imponía.

La cumbre del proyecto de comunicación permanente, iniciado después de la Segunda Guerra Mundial, se alcanza con la implantación del protocolo TCP, permitiendo la creación de un medio eficiente de comunicación dedicado, específicamente, a asegurar la transmisión de datos. Con las facilidades provistas por TCP, nace una red pública capaz de permitir la conexión múltiple de redes sin importar su arquitectura tecnológica y se le denomina Internet, una verdadera red de redes.

Durante su evolución, Internet ha superado las expectativas de crecimiento planteadas durante su creación, actualmente hay millones de usuarios diarios conectados a esta red; las conexiones se realizan desde equipos monousuario o a través de redes privadas; las distancias se han acortado y la información

fluye a caudales agilizando las actividades económicas, sociales y culturales esperando que, en los años próximos, más personas en todo el mundo utilicen los servicios de Internet, realizando actividades de compra, venta y pago de servicios, educación, comunicación y diversión.

Es cierto, las ventajas ofrecidas por Internet no se han alcanzado con ningún otro medio de comunicación, pero es necesario crear conciencia de que es un medio público de transmisión y por lo tanto es vulnerable. En los últimos años, se han ventilado innumerables casos relativos a actos realizados a través de Internet, con los que se ha expuesto claramente el nivel de seguridad que ofrece. Internet ha sufrido ataques de personas que desean demostrar sus conocimientos al ingresar y en ocasiones dañar sistemas protegidos a los que no tenían acceso, también se le ha utilizado para realizar actos ilícitos como alteración y robo de información, pornografía, prostitución y terrorismo; y aunque en algunos países se ha normado su uso, aún falta mucho por hacer, no es fácil legislar las actividades que se realizan a través de una red que opera a nivel mundial y a la que se conectan millones de individuos o grupos con creencias, ideas, costumbres, educación y ética diferentes.

La seguridad en Internet es relevante y un tema que se debe abordar con seriedad, haciendo las siguientes consideraciones:

- En el pasado, Internet surgió como una necesidad para mantener comunicación permanente aún cuando se destruyeran los medios de transmisión.

- En el presente, Internet es un medio a través del cual se puede encontrar desde la letra de una canción o una receta de cocina hasta realizarse operaciones bancarias millonarias y actúa como un motor de cambios sociales, culturales, políticos y económicos.

- En el futuro, Internet o los sistemas sucesores serán parte de la vida cotidiana y seguramente contarán con la capacidad suficiente para mantener registros detallados de cada individuo, permitir el control a distancia del hogar y la oficina, hacer efectiva la presencia virtual, disponer de satisfactores a demanda y en general, comunicar y localizar a quien sea en donde sea.

Consideramos que el esquema descrito en forma por demás breve, es lo suficientemente contundente para visualizar las amenazas o ataques a los que estamos expuestos y como la magnitud del riesgo está directamente vinculada al nivel de importancia de la información que viaja en una red. La única forma de disminuir la posibilidad de que ocurra un evento no deseado, cuando enviamos o recibimos información a través de una red, es que los sistemas de seguridad evolucionen simultáneamente con la entidad, tecnología o sistema que se desea proteger.

El presente trabajo de tesis, es una propuesta para abordar la seguridad en Internet, de las fases que se deben cubrir para implantar un sistema integral de seguridad y de las áreas de conocimiento o temas que se deben abarcar en la materia de redes de computadoras. A tal fin, la estructura de este documento se desarrolla de la siguiente forma:

- **Conceptos Fundamentales y Arquitecturas Básicas.**

  Es la compilación de conocimientos mínimos indispensables que se deben tener sobre redes de computadoras, describiendo los aspectos técnicos de construcción y distribución así como los relativos a comunicación y control.

- **Internet.**

  Breve reseña del origen y evolución de Internet acompañada de la definición, conceptos y tendencias de la red pública más grande del mundo, incluyendo la descripción de los servicios que proporciona, concluyendo con la identificación de riesgos adquiridos con el uso de esta red.

- **Redes y Sistemas Operativos Seguros.**

  Complemento a la identificación de riesgos, estableciendo características y técnicas que se deben observar para implantar servicios de comunicación y recursos compartidos seguros, abarcando la infraestructura de cómputo, telecomunicaciones y aplicaciones informáticas.

- **Seguridad en Internet, Herramientas y Soluciones.**

  Identificación de la necesidad y beneficios de la convivencia entre redes privadas y redes públicas, determinando la vulnerabilidad y clasificación de riesgos de dicha convivencia. Descripción de la infraestructura disponible para proteger una red privada y de los mecanismos físicos y lógicos existentes para asegurar la comunicación, concluyendo con una propuesta de cultura y esquema integral de seguridad.

- **Propuesta del Tema de Seguridad para la Asignatura de Redes de Computadoras.**

  Parte final del trabajo de análisis e investigación relativo a la seguridad en Internet, cuyo resultado es la identificación de los diferentes aspectos a estudiar en relación con el tema de redes de computadoras y la importancia de complementarlos con todo lo relativo a seguridad, abarcando la protección de los servicios de comunicación y recursos compartidos así como el aseguramiento de la información, su transmisión y recepción.

  Con base en lo anterior y en virtud de la relevancia del tema de seguridad, se elabora esta propuesta de modificación al temario de la asignatura de Redes de Computadoras, cuya intención principal es la de incrementar los alcances que esta materia tiene e impactar en las posibilidades que la carrera de Ingeniería en Computación brinda a sus profesionales.

  Para alcanzar el objetivo deseado, se llevó a cabo la revisión de los planes de estudio de diferentes Universidades de los Estados Unidos de Norteamérica, Canadá y del continente Europeo destacando que la seguridad es atendida mediante estudios de especialización posteriores a los de licenciatura y donde cada licenciatura está orientada a un área específica de la computación.

  Ahora bien, si la carrera de Ingeniería en Computación impartida en la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, se caracteriza por formar profesionales con las aptitudes para desarrollarse en cualquiera de las ramas de la computación, también debiese ser apto para intervenir en lo concerniente a redes y sistemas operativos seguros.

La estructura de este trabajo pretende mantener una secuencia lógica de conocimientos, iniciando con aspectos generales y concluyendo en temas específicos, sin dejar de considerar la necesidad imperiosa y beneficios de generar una cultura de seguridad.

# PAGINACIÓN DISCONTINUA

# CAPÍTULO 1
# CONCEPTOS FUNDAMENTALES Y ARQUITECTURAS BÁSICAS

Desde la creación de la computadora el hombre poco a poco se ha dado cuenta de las ventajas que ésta le ha proporcionado, ha visto como sus necesidades han sido satisfechas, sin embargo, el hombre en su afán de crecer día a día, ha ido desarrollado nuevas tecnologías tanto para el manejo de información, como para las comunicaciones, ha logrado incrementar la velocidad de las computadoras y minimizado en forma considerable el tamaño de todos sus componentes, logrando así, tener un mayor número de recursos a su disposición, dando un mejor uso a todos ellos y pudiendo compartirlos, no importando las distancias, naciendo un concepto nuevo dentro de la informática: las redes de computadoras, cuya definición, elementos que la componen, descripción, y clasificación se verán a continuación.

## 1. DEFINICIÓN DE RED

Existen diversas definiciones de lo que es una red, en este trabajo se considerará que una red **es un conjunto de computadoras y dispositivos asociados, conectados y comunicados entre sí para facilitar los servicios de transferencia de información y distribución de recursos compartidos entre usuarios, que incluso pudieran estar situados en puntos geográficamente distantes.**

## 2. COMPONENTES DE LAS REDES

Para instalar cualquier red de computadoras se requiere de hardware y software, esto es un conjunto de elementos interrelacionados, tales como: computadoras, servidores, tarjetas de red, medios de transmisión, concentradores o equipo de conectividad, software de aplicación y sistema operativo de red.

### Computadoras

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente realizando sus propios procesos, asimismo, las computadoras se convierten en estaciones de trabajo en red con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo puede compartir sus propios recursos con otras computadoras, ésta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun u otras marcas.

### Servidores

Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten, algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos

distribuido, servidor de archivos dedicado y no dedicado, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

**Tarjeta de Red**

Para comunicarse con el resto de la red, cada computadora debe tener instalada una NIC (*Network Interface Card,* Tarjeta de Interfaz de Red), se les llama también adaptadores de red o sólo tarjetas de red, en la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo, las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en mini computadoras y mainframes, a menudo se usan cajas externas para Mac's y para algunas computadoras portátiles, la tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entenderla y así poder reenviarla.

**Medio de Transmisión**

La red debe tener un medio de transmisión que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un medio de transmisión disponible, la decisión sería sencilla, lo cierto es que hay muchos tipos de medio de transmisión, cada uno con sus propias ventajas y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial. Los medios de transmisión más comunes se listan a continuación:

- **Cable par trenzado:** El cable consta de 4 pares de hilos de cobre aislados dentro de un forro de plástico. Cada par está torcido con números diferentes de vueltas por pulgada con el fin de ayudar a eliminar la interferencia entre pares adyacentes y otros dispositivos eléctricos. Entre más apretado sea el torcido, es más alto el rango de transmisión que soporta y por supuesto, más el costo por metro. (Fig. 1.1).

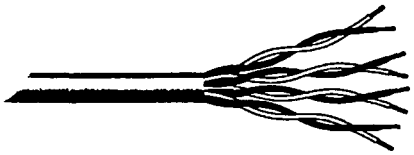

Fig. 1.1 Par trenzado

Existen 5 niveles o categorías de cable par trenzado, cada uno con diferentes aplicaciones:

| Nivel | Uso |
|---|---|
| 1 | Sólo voz (cable telefónico) |
| 2 | Datos a 4 Mbps (Local Talk) |
| 3 | Datos a 10 Mbps (Ethernet) |
| 4 | Datos a 20 Mbps (16 Mbps en Token Ring) |
| 5 | Datos a 100 Mbps (Fast Ethernet) |

Tabla 1.1 Categorías cable par trenzado



TESIS CON
FALLA DE ORIGEN

- **Cable coaxial:** Es tan fácil de instalar y mantener como el cable de par trenzado. Se trata de un cable de dos polos aislados entre sí. Uno de ellos es un hilo grueso que va en el centro, generalmente de cobre, cubierto con un material aislante. (Fig. 1.2).

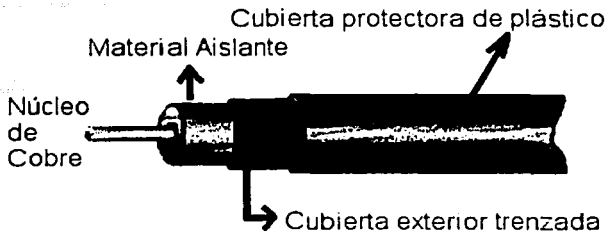


Fig. 1.2 Cable coaxial

- **Cable de fibra óptica:** Se refiere al medio y la tecnología asociada para transmisión de información con base en pulsos luminosos a través de una fibra o cable de vidrio o plástico. Este tipo de cable puede llevar mucha más información que un cable de cobre convencional y en general no está sujeto a interferencias electromagnéticas. (Fig. 1.3).

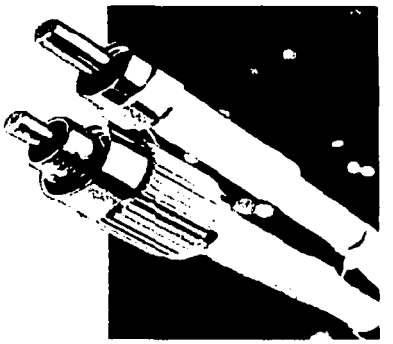

Fig. 1.3 Fibra óptica

- **Microondas, Radio Frecuencia y Ondas Satelitales:** Todas ellas medios de transmisión inalámbrica, estos son de los medios mas caros, pero en la actualidad ya son comunes por las facilidades que nos representan.

TESIS CON
FALLA DE ORIGEN

**Topología de red**

Se refiere a la forma o configuración de una red. Las topologías pueden ser físicas o lógicas.

- **La topología física** es la distribución o posición en que se encuentran conectadas las computadoras, unas con otras, la configuración de cables y demás periféricos, también se refiere a la distancia que existe entre ellas.

- **La topología lógica** es el método que se usa para comunicarse con las demás, la ruta que toman los datos de la red entre las diferentes computadoras, la tecnología de transmisión de datos que se emplea.

**Protocolos**

Es el conjunto de reglas que regulan la comunicación entre los nodos de una red. Estas reglas incluyen normas que regulan las siguientes características de una red: método de acceso, topologías físicas permitidas, tipos de cable y velocidad de transmisión de datos. Los protocolos más usados son: Ethernet, LocalTalk, Token Ring, FDDI y ATM.

**Equipo de conectividad**

Un dispositivo de red puede emitir y recibir señales de todos los demás dispositivos de la red, otra posibilidad es que cada dispositivo esté conectado a un concentrador, un equipo especializado que transmite de forma selectiva la información desde un dispositivo hasta uno o varios destinos en la red. Las redes emplean protocolos, o reglas, para intercambiar información a través de una única conexión compartida, estos protocolos impiden una colisión de datos provocada por la transmisión simultánea entre dos o más computadoras. Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito específico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivo para aumentar la flexibilidad y el valor. Dentro de los equipos de conectividad se mencionan:

- **Hubs o concentradores:** Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella. (Fig. 1.4).

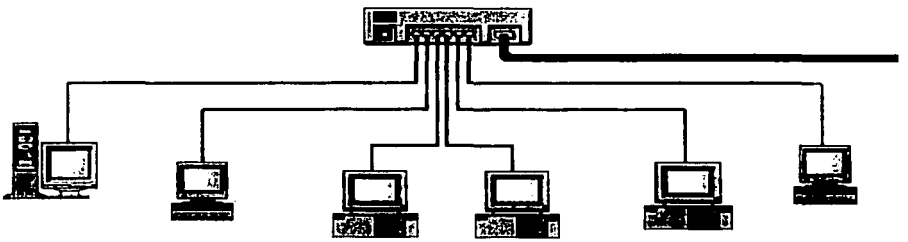

Fig. 1.4 Hubs o concentradores



TESIS CON
FALLA DE ORIGEN

- **Repetidores**: Un repetidor es un dispositivo que permite regenerar o replicar una señal con el fin de extender la longitud de la red. Los repetidores analógicos frecuentemente solo pueden amplificar la señal mientras que los digitales pueden reconstruir la señal. En una red de datos, un repetidor puede transmitir mensajes entre subredes que usan diferentes protocolos o tipos de cable.

- **Puentes**: Un puente es un dispositivo que conecta dos redes locales o dos segmentos separados de la misma red y que usan el mismo protocolo, para crear lo que aparenta ser una sola red.

- **Ruteadores**: Es un dispositivo que combina las funciones de un switch además de realizar operaciones de ruteo; es decir, envía datos buscando una dirección física de dispositivo y además envía paquetes localizando la siguiente dirección de salto. (Fig. 1.5).

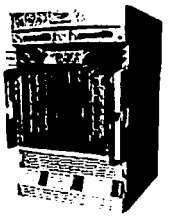

Fig. 1.5 Ruteador

- **Compuertas**: Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos, podría tenerse una red que consista en computadoras compatibles con IBM y otra con Macintosh.

**Sistema operativo de red**

Seleccionar un sistema operativo es la tarea más delicada en el proceso de instalación de una red, asimismo, las interconexiones que se planean a futuro y los tipos de aplicaciones que se desean instalar en el sistema, son de suma importancia. Dentro de los sistemas operativos de red los más usados son: NETWARE de NOVELL, WINDOWS NT ADVANCED SERVER de MICROSOFT y LAN SERVER de IBM, además de UNIX, LINUX, etcétera.

Este sistema operativo deberá administrar y coordinar todas las operaciones de dicha red, los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades, algunos sistemas operativos se comportan excelentemente en redes pequeñas, así como otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

Los servicios que los NOS (*Network Operating System*, Sistemas Operativos de Redes) realizan son:

**Soporte para archivos**: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.



TESIS CON
FALLA DE ORIGEN

**Comunicaciones**: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.

**Servicios para el soporte de equipo**: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etcétera.

De manera general, los componentes anteriores se engloban en las siguientes categorías: **software de aplicaciones, software de red y hardware de red.** (Tabla 1.2).

| | |
|---|---|
| **Software de aplicaciones** | Está formado por programas de cómputo que se comunican con los usuarios de la red y permiten compartir información (archivos, gráficos o videos) y recursos (impresoras o unidades de disco). |
| **Software de Red** | Son programas de cómputo que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente. |
| **Hardware de Red** | Está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de las computadoras. |

Tabla 1.2 Componentes generales de una red.

## 3. OBJETIVOS DE LAS REDES DE COMPUTADORAS

Para este campo no hay muchas discrepancias en lo que se refiere a los objetivos de las redes de computadoras, sin embargo se mencionarán los que a propósito de este capítulo se consideran los más importantes: Compartir recursos, confiabilidad, ahorro económico y reducción de distancias.

### Compartir Recursos

Las redes en general, comparten recursos, y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

### Confiabilidad

Al contar con fuentes alternativas de suministro se proporciona una alta confiabilidad. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU *(Central Process Unit*, Unidad de Proceso Central) significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

### Ahorro Económico

Las computadoras personales (PC, *Personal Computer*) tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Esta ventaja ha sido bien aprovechada por muchos diseñadores de sistemas, ya que por lo general se construyen redes constituidas por poderosas computadoras personales. De esta forma, el poder tener recursos como computadoras, discos duros, CD ROM, impresoras, información y otros servicios compartidos, permite que las grandes inversiones que se hacían al inicio de la revolución informática se vean claramente reducidas, ya que actualmente no es necesario invertir mucho dinero para obtener un mayor costo beneficio.

### Reducción de Distancias

Las redes de computadoras se utilizan como medio de comunicación entre dos o más personas que se encuentran alejadas; a través de ellas, es relativamente fácil intercambiar información, conversar por medio del teclado en tiempo real, enviarse mensajes de correo, así como establecer videoconferencias. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora.

## 4. CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS

Las redes de computadoras tienen diferentes clasificaciones, en la siguiente tabla (Tabla 1.3) se listan las más significativas.

| Clasificación | Tipos |
|---|---|
| Por su topología física | Bus<br>Anillo<br>Estrella |
| Por su extensión | LAN<br>WAN<br>MAN<br>Intranet<br>Extranet<br>Internet |
| Por la forma de conexión | Ethernet<br>Token Ring<br>Otras tecnologías |

Tabla 1.3 Clasificación de redes

A continuación se describirán de manera más extensa cada una de las categorías anteriormente mencionadas:

### Por su Topología Física

**Estrella**

Es la topología de red más antigua que existe, se utiliza el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de una topología de red en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador, el cual controla el flujo de datos. En una topología estrella, todos y cada uno de los nodos de la red se conectan al concentrador (*hub*) (Fig.1.6), los datos en estas redes fluyen del emisor hasta el concentrador, este controlador realiza todas las funciones de red además de actuar como amplificador de los datos. Esta configuración se suele utilizar con cables de par trenzado aunque también es posible implementarla utilizando cable coaxial o fibra óptica. Tanto Ethernet como LocalTalk utilizan esta topología.

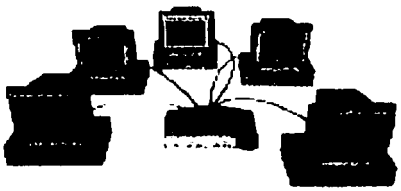

Fig. 1.6 Topología de Estrella



TESIS CON
FALLA DE ORIGEN

**Ventajas**

- Gran facilidad de instalación.
- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y reparación.

**Desventajas**

- Requiere más cable que otra topología.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos conectados a él.
- Es necesario adquirir concentradores.

**Bus**

En esta topología todos los nodos están conectados a la línea principal de comunicaciones, que consiste en un cable con un terminador en cada extremo (Fig. 1.7). Cada nodo está conectado a un segmento común de cable de red (*Back Bone*, columna vertebral) y cada uno supervisa la actividad de la línea, es decir, los mensajes son detectados por todos los nodos, aunque aceptados sólo por el nodo o los nodos hacia los que van dirigidos. Para evitar las colisiones que se producen cuando dos o más nodos intentan utilizar la línea al mismo tiempo, las redes en bus suelen utilizar detección de colisiones, o paso de señales, para regular el tráfico.

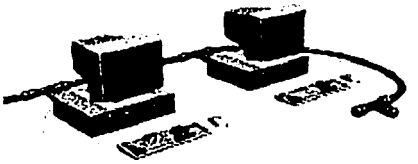

Fig. 1.7 Topología de Bus

**Ventajas**

- Es fácil conectar nuevos nodos a la red.
- Requiere menos cable que una topología estrella.

**Desventajas**

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requieren terminadores.
- Es difícil detectar el origen de un problema cuando toda la red "cae".
- No se debe utilizar como única solución en un gran edificio.

**Anillo**

Los dispositivos (nodos) están conectados en un circuito cerrado formando un Anillo o círculo lógico (Fig. 1.8). Los mensajes pasan de un nodo a otro en una sola dirección, factor que permite tener un control de recepción de mensajes. A medida que un mensaje viaja a través del anillo, cada nodo examina la dirección de destino adjunta al mensaje. Si la dirección coincide con la del nodo, éste



TESIS CON
FALLA DE ORIGEN

acepta el mensaje. En caso contrario regenerará la señal y pasará el mensaje al siguiente nodo dentro del bucle. Puede incluirse en su diseño una forma de puentear cualquier nodo defectuoso o vacante.

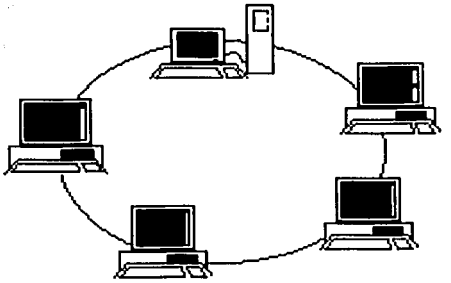

Fig. 1.8 Topología de Anillo

**Ventajas**

- Los cuellos de botella son poco frecuentes.
- Sólo existe un sentido en la transmisión.
- Cada nodo regenera la señal, lo que permite cubrir distancias superiores a las redes en estrella o redes en bus.

**Desventajas**

- Si falla un enlace compromete la integridad y funcionalidad de toda la red.
- Dado que es un bucle cerrado, es difícil agregar nuevos nodos.
- El rendimiento decae cuando aumenta el número de estaciones.

**Por su Extensión**

**LAN** (*Local Area Network*, Red de Área Local)

Es la red de comunicación utilizada por una sola organización, empresa, universidad, etcétera, es una combinación de hardware y medios de trasmisión relativamente pequeños. Por lo regular no rebasan una decena de kilómetros y comúnmente utilizan un sólo medio de transmisión, en términos generales, una LAN queda comprendida dentro de un edificio, permite a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, etcétera

Una configuración típica en una LAN, es tener un servidor de archivos en la que se almacena todo el software de control de la red, así como el software que se comparte con las demás computadoras de la red. Las computadoras que no son servidores de archivos reciben el nombre de estaciones de trabajo, éstas suelen ser menos potentes y tienen un software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.



TESIS CON
FALLA DE ORIGEN

Las redes LAN prestan servicios de comunicación de datos a grandes velocidades (dependiendo del material utilizado como enlace), a causa de la poca distancia, las redes LAN tienen tasas muy bajas de error en sus transmisiones.

Características preponderantes:

- Los canales son propios de los usuarios o empresas.
- Los enlaces son líneas de alta velocidad.
- Las estaciones se encuentran cerca entre sí.
- Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- La arquitectura permite compartir recursos.

**MAN** (*Metropolitan Area Network*, Red de Área Metropolitana)

Es un tipo de red que interconecta a los usuarios con los recursos de cómputo en un área geográfica más grande que la que puede cubrir una LAN pero más pequeña que el área cubierta por una WAN. El término se aplica a la interconexión de redes en una ciudad para formar una red más grande, es decir, se interconectan varias redes locales mediante puentes; su tamaño puede variar hasta los 100 kilómetros y están conformadas por diferentes medios de trasmisión, hardware y software (Fig.1.9).

Una MAN puede manejar datos y voz, e incluso podría estar relacionada con una red de televisión por cable local, una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales, como no tiene que conmutar, el diseño se simplifica. La razón principal para distinguir la MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este se llama DQDB (*Distributed Queue Dual Bus*, Bus Dual de Cola Distribuida). El DQDB consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras, cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior, el trafico hacia la izquierda usa el bus inferior. Un aspecto clave de la MAN es que hay un medio de difusión al cual se conectan todas las computadoras, esto simplifica mucho el diseño comparado con otros tipos de redes.


Fig. 1.9 Red de Área Metropolitana (MAN)

TESIS CON
FALLA DE ORIGEN

**WAN** (*Wide Area Network*, Red de Área Amplia)

Este tipo de red se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas computadoras se llaman hosts. Los hosts están conectados por una subred de comunicación, el trabajo de una subred es conducir mensajes de un host a otro (Fig. 1.10). La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación, las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra, los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. El término que se usará para las computadoras de conmutación, es ruteadores. El intercambio de información es más lento comparado con las redes de área local. Es común que una red WAN tenga como nodos a redes LAN, además los protocolos que utiliza una red de área amplia para transmitir datos entre dos de sus nodos son complejos de operar y la probabilidad de que una transmisión sea errónea crece en proporción con el tamaño de la red. Una WAN incluye toda las redes que son más grandes que la MAN. Una WAN por definición es una red que abarca todo el planeta. Internet es un ejemplo de este tipo de red.

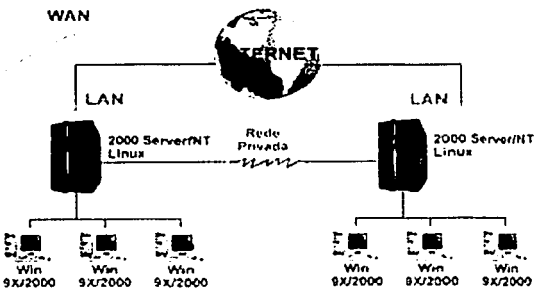


Fig. 1.10 Red de Área Amplia

**Intranet**

Una Intranet es un ambiente de computación heterogéneo que conecta diferentes plataformas de hardware, ambientes de sistema operativo e interfaces de usuario con el fin de permitir comunicación continua, colaboración, transacciones e innovación. Una Intranet es una red privada dentro de una organización, es decir, sólo los miembros de la compañía pueden tener acceso a ella, es una red propia que ha sido creada para satisfacer las necesidades específicas de una compañía u organización, la cual sigue debidamente los protocolos ya establecidos de Internet, muy en específico el TCP/IP.



TESIS CON
FALLA DE ORIGEN

Puede darse el caso de que sea una red aislada, es decir, que no se encuentre conectada a Internet, ésta alberga información que sólo puede utilizar quien esté definido como usuario válido de la Intranet. Esta definición es muy similar a lo que entendemos por LAN o WAN, tan sólo sustituyendo el concepto "Sitio Web" por el de "Servidor".

La diferencia entre las otras redes y ésta radica en el uso de una interfaz común, que es independiente de la computadora desde la cual el usuario se conecta al servidor. La interfaz será la misma y el usuario podrá obtener o ingresar información del mismo modo, de hecho, esta interfaz es un software de interpretación desarrollado para cada sistema operativo y que trae al usuario la información organizada utilizando un lenguaje estandarizado como HTML, Java o Actives. La comunicación entre los equipos, independiente de la plataforma utilizada, se realiza sobre un protocolo de comunicaciones estándar como TCP/IP u otro diferente, siempre que todos los equipos que se comuniquen a la Intranet utilicen el mismo protocolo.

**Extranet**

Es una red privada que usa el protocolo Internet y el sistema público de telecomunicaciones para compartir de forma segura parte de la información de la compañía u operaciones con proveedores, vendedores, socios y otros negocios. Puede ser vista como parte de la intranet de una compañía que es parcialmente accesible a usuarios externos. Una extranet provee varios niveles de acceso a usuarios externos; sólo se puede acceder a una extranet si se tiene un nombre de usuario y contraseña válidos, de esta manera la identidad del usuario determina a que partes de la extranet tiene acceso.

**Internet**

El Internet también conocido como la Red, es la red de computadoras más grande del mundo. Esta red de redes mundial provee correo electrónico, noticias, acceso a control remoto, transferencia de archivos y otros servicios a nivel mundial. El Internet está basado en el IP (*Internet Protocol*, Protocolo de Internet) el cual es una comunicación global estándar. El Internet es la conexión de múltiples redes. (Ver **Capítulo II. INTERNET**).

La figura 1.11 muestra un modelo general de relación entre Intranet, Extranet e Internet.


Fig. 1.11 Alcances de Intranet, Extranet e Internet



TESIS CON
FALLA DE ORIGEN

## Por la forma de Conectarse

### Redes Ethernet

Ethernet, al que también se conoce como IEEE 802.3, es el estándar más popular para las LAN que se usa actualmente, el estándar 802.3 emplea una topología lógica de bus y una topología física de estrella o de bus. Ethernet permite datos a través de la red a una velocidad de 10 Mbps.

Ethernet usa un método de transmisión de datos conocido como CSMA/CD (*Carrier Sense with Multiple Access with Collision Detection*, Acceso Múltiple con Detección de Portadora y Detección de Colisiones). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transfiriendo información, de no ser así, el nodo transferirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información, en caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío, así, la falla de un sólo nodo no hace que falle la red completa. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podrá llegar al punto de saturación, sin embargo, con una red diseñada adecuadamente, la saturación rara vez es preocupante. Existen tres estándares de Ethernet: 10BASE5, 10BASE2, y 10BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red.

### Redes Token Ring

Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes, con una velocidad de operación de 4 Mbps ó 16 Mbps, Token Ring emplea una topología lógica de anillo y una topología física de estrellao anillo. La tarjeta de red de cada computadora se conecta a un cable que a su vez, se enchufa a un hub central llamado MAU (*Multi-station Access Unit,* Unidad de Acceso a Multiestaciones).

Token Ring se basa en un esquema de paso de señales (*Token passing*), es decir, que pasa un Token (señal) a todas las computadoras de la red. La computadora que esté en posesión del Token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el Token pasa a la siguiente computadora del anillo. Si la siguiente computadora tiene que enviar información, acepta el Token y procede a enviarla, en caso contrario, el Token pasa a la siguiente computadora del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red Token Ring examina y luego retransmite cada Token, un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. Token Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional, sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente que CSMA/CD.

### Otras tecnologías

Existen varias tecnologías que satisfacen las necesidades de las redes actuales, incluyendo a Fast Ethernet, FDDI (*Fiber Distributed Data Interface,* Interfaz de Distribución de Datos por Fibra), Frame Relay (Retransmisión de Tramas) y ATM (*Asynchronous Mode Transfer,* Modo de Transferencia Asíncrona).

**Fast Ethernet:** Llamado también 100BASEX, es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps, un incremento 10 veces mayor que el Ethernet estándar de 10 Mbps.

**FDDI:** Es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI (*American National Standards Institute*, Instituto Nacional Americano de Estándares) para FDDI especifica una velocidad de 100 Mbps. Dado que el cable de fibra óptica no es susceptible a la

interferencia eléctrica o tan susceptible a la degradación de la señal de red como sucede con los cables de red estándar, FDDI permite el empleo de cables mucho más largos que otros estándares de red.

**Frame Relay:** Es un servicio orientado a la conexión, para mover datos de un nodo a otro a una velocidad razonable y bajo costo. El Frame Relay puede verse como una línea virtual rentada. El usuario renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas o frames (es decir, paquetes) de hasta 1600 bytes entre ellos. Además de competir con las líneas rentadas, el Frame Relay compite con los circuitos virtuales permanentes de X.25.

**ATM:** Es un conjunto de estándares internacionales para la transferencia de datos, voz y video por medio de una red a muy altas velocidades. Puesto que opera a velocidades que van desde 1.5 Mbps hasta 1.5 Gbps, ATM incorpora parte de los estándares Ethernet, Token Ring y FDDI para la transferencia de datos.

## 5. MODELO OSI (*Open Systems Interconection*, Interconexión de Sistemas Abiertos)

En 1984, la ISO (*International Standard Organization,* Organización Internacional de Estándares) desarrolló un modelo llamado OSI, el cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el más conocido y el más usado para describir los entornos de red.

El modelo de referencia OSI es la arquitectura de red actual más prominente, su objetivo es desarrollar estándares para la interconexión de sistemas abiertos. El término OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. OSI es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas (Tabla 1.4). Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. Algunas de las funciones de cada capa o nivel se describen a continuación:

| Nivel | Nombre | Función |
|---|---|---|
| 7 | Aplicación | Provee servicios generales relacionados con aplicaciones (Transferencia de archivos) |
| 6 | Presentación | Formato de Datos |
| 5 | Sesión | Coordina la interacción en la sesión (diálogo) de los usuarios |
| 4 | Transporte | Provee una transmisión de datos confiable punto a punto |
| 3 | Red | Enruta unidades de información |
| 2 | Enlace de Datos | Provee intercambio de datos entre dispositivos en el mismo medio |
| 1 | Físico | Transmite un flujo de bits a través del medio físico |

Tabla 1.4 Capas del Modelo OSI

TESIS CON
FALLA DE ORIGEN

A continuación se explicarán las funciones de cada una de las capas del modelo OSI.

| **Nivel de Aplicación** |
|---|
| En este nivel, se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las cuales gestionan: |
| **Transferencia de archivos (FTP)** |
| **Intercambio de mensajes (correo electrónico)** |

| **Nivel de Presentación** |
|---|
| En este nivel, se realizan las siguientes funciones: |
| **Se da formato a la información para visualizarla o imprimirla** |
| **Se interpretan los códigos que estén en los datos (conversión de código)** |
| **Se gestiona la encriptación de datos** |
| **Se realiza la compresión de datos** |

| **Nivel de Sesión** |
|---|
| Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos. Algunas de las funciones que realiza son las siguientes: |
| **Establecimiento de la conexión de sesión** |
| **Intercambio de datos** |
| **Liberación de la conexión de sesión** |
| **Sincronización de la sesión** |
| **Administración de la sesión** |

| **Nivel de Transporte** |
|---|
| Esta capa asegura que se reciban todos los datos y en el orden adecuado. Realiza un control de extremo a extremo. Algunas de las funciones realizadas son: |
| **Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red** |
| **Multiplexaje** |
| **Regula el control de flujo del tráfico de extremo a extremo** |
| **Reconoce los paquetes duplicados** |

| **Nivel de Red** |
|---|
| Esta capa permite la interconexión de sistemas, mediante la comunicación entre niveles de enlace. Algunas de las funciones realizadas son: |
| **Determina el establecimiento de la ruta** |
| **Mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento** |
| **Realiza control de congestión** |



TESIS CON
FALLA DE ORIGEN

| Nivel de Enlace de Datos |
|---|
| Esta capa garantiza la transmisión entre los extremos de una comunicación, ya que el medio físico puede presentar problemas de ruido e interferencia. Algunas de las funciones realizadas son: |
| **Detección y control de errores (mediante el empleo del CRC)** |
| **Control de secuencia** |
| **Control de flujo** |
| **Control de enlace lógico** |
| **Control de acceso al medio** |
| **Sincronización de la trama** |

| Nivel Físico |
|---|
| Esta capa define las características de la red: Mecánicas, Eléctricas, Funcionales y de Procedimiento para la activación, mantenimiento y desactivación de los sistemas físicos que conectan los sistemas. |
| **Define las características eléctricas (niveles de tensión)** |
| **Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico)** |
| **Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter** |

## 6. MODELO INTERNET

El modelo Internet utiliza el esquema de comunicación cliente/servidor, en el que un equipo solicita información (cliente) y el otro la entrega (servidor); sin embargo, el rol que un equipo puede desempeñar no es estático, ya que en un instante puede actuar como cliente y momentos más tarde como servidor.

### 6.1 Arquitectura TCP/IP (*Transfer Control Protocol / Internet Protocol*, Protocolo de Control de Transferencia / Protocolo Internet)

Aunque el modelo de referencia OSI sea universalmente reconocido, el modelo abierto de Internet estándar desde el punto de vista histórico y técnico es el TCP/IP. El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadoras, desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

El modelo TCP/IP está basado en el tipo de red conmutación de paquetes *(packet-switched)*, y tiene cuatro capas: Aplicación, Transporte, Red y Enlace (Tabla 1.5). Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI, aunque no se corresponden, por lo que no deben confundirse.

| Nivel | Nombre | Función |
|---|---|---|
| 4 | Aplicación | Acceso del usuario a las aplicaciones |
| 3 | Transporte | Comunicación de extremo a extremo |
| 2 | Red | Gestión y direccionamiento de las comunicaciones |
| 1 | Enlace | Flujo de datos e interfaz con el medio físico |

Tabla 1.5 Capas del Modelo Internet



TESIS CON
FALLA DE ORIGEN

### Capa de aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación, y simplemente crearon una capa de aplicación que manejara protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa.

### Capa de transporte

Permite que capas pares en los hosts fuente y destino puedan conversar. La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza los servicios de la capa de red para proveer un servicio eficiente y confiable a los procesos de la capa de aplicación. El hardware y el software dentro de la capa de transporte se denominan entidades de transporte, y pueden estar en el kernel, en un proceso de usuario o en una tarjeta. En esta capa se produce la segmentación de los datos producidos en la capa de aplicación en unidades de menor tamaño, denominadas paquetes o datagramas. Un datagrama es un conjunto de datos que se envía como un mensaje independiente. La capa de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. Simplemente considera que la comunicación entre ambos extremos está ya establecida y la utiliza.

### Capa de red

El propósito de la capa de red es enviar paquetes desde cualquier red y que éstos lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino. Para poder enrutar los datagramas de la capa de Transporte, éstos se encapsulan en unidades independientes, en las que se incorporan diferentes datos necesarios para el envío, como dirección de origen del datagrama, dirección de destino, longitud del mismo, etcétera.

En una comunicación con arquitectura TCP/IP ambos host pueden introducir paquetes en la red, viajando, independientemente de cual sea su destino. Por ello, no hay ninguna garantía de entrega de los paquetes ni de orden en los mismos.

### Capa de enlace

También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete para realizar realmente un enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI. Uno de los principales elementos que maneja esta capa es el de las direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red, y que son el medio principal de localización de un host dentro de una red, cada tarjeta tiene un número identificador, los 3 primeros bytes son asignados por el fabricante de la misma, mientras que los otros 3 se asignan de forma especial, cuando un host debe enviar un paquete a otro de su red busca a éste mediante su número de tarjeta de red (dirección física).

### 6.2 Comparación OSI-TCP/IP

Si comparamos el modelo OSI y el modelo TCP/IP, se observarán ciertas similitudes y diferencias, que por facilidad se han englobado en la siguiente tabla (Tabla 1.6).

<table>
<tr><th colspan="2">Modelo TCP/IP</th><th colspan="2">Modelo OSI</th></tr>
<tr><td>Aplicación</td><td rowspan="4">Protocolos</td><td>Aplicación</td><td rowspan="4">Capas del Hosts</td></tr>
<tr><td rowspan="2">No hay capas especificadas</td><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td>Transporte</td></tr>
<tr><td>Red</td><td rowspan="3">Redes</td><td>Red</td><td rowspan="3">Capas de Medios</td></tr>
<tr><td rowspan="2">Enlace</td><td>Enlace</td></tr>
<tr><td>Física</td></tr>
</table>

Tabla 1.6 Comparación de los Modelos OSI-TCP/IP

**Similitudes:**

- Ambos se dividen en capas o niveles.
- Ambos tienen capa de aplicación, aunque incluyen servicios muy distintos.
- Para el intercambio de información utilizan conmutación de paquetes.

**Diferencias**

- OSI distingue de forma clara los servicios, las interfaces y los protocolos, TCP/IP no.
- OSI fue definido antes de implementar sus protocolos, por lo que algunas funcionalidades fallan o no existen. En cambio, TCP/IP se creó a partir de la definición de sus protocolos, por lo que se amolda a ellos perfectamente.
- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, no se crean redes a partir de protocolos específicos relacionados con OSI, aunque todo el mundo utiliza el modelo OSI como guía.



TESIS CON
FALLA DE ORIGEN

## 6.3 Protocolos TCP/IP

El diagrama que aparece en la Fig. 1.12, se denomina gráfico de protocolo. Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP.

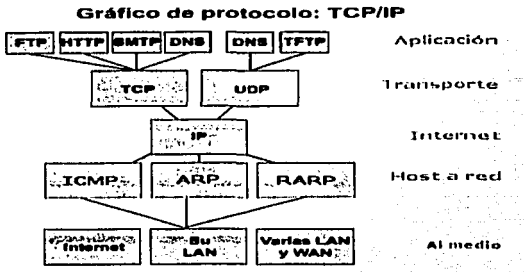


Fig. 1.12 Gráfico de protocolo

TCP/IP está conformado por una familia de protocolos, actualmente existen alrededor de 6,000 aplicaciones; es difícil definir cada una de ellas por motivos de extensión, pero se tratarán las más comunes por cada una de las capas de este modelo.

### Capa de Aplicación

Aparecen distintas tareas de red que probablemente no conozca, pero como usuario de Internet, probablemente use todos los días. Estas aplicaciones se ven controladas por los siguientes protocolos:

**FTP** (*File Transfer Protocol*, Protocolo de Transferencia de Archivos): Este protocolo permite el acceso al sistema de directorios de una computadora remota y el envío y la descarga de archivos. Como medida de seguridad, el acceso a dichos directorios está protegido por un sistema de control de acceso de tipo usuario-password.

**TELNET** (*Remote Login*, Protocolo de servicio de conexión remota): Es un emulador de terminal que permite acceder a los recursos y ejecutar programas en una computadora remota, es decir, nos permite conectarnos a un equipo remoto y actuar sobre él como si estuviéramos físicamente conectados al mismo.

**HTTP** (*Hypertext Transfer Protocol*, Protocolo de Transferencia de Hipertexto): Proporciona el servicio de páginas web, mediante el cual podemos solicitar éstas a un servidor web y visualizarlas en los navegadores clientes.

**SMTP** (*Simple Mail Transport Protocol*, Protocolo de Transporte de Correo Simple): Proporciona el servicio de correo electrónico, permitiendo enviar mensajes a otros usuarios de la red. Estos mensajes se envían primero a unos servidores especiales, desde los cuales pueden ser descargados por el destinatario final.



TESIS CON
FALLA DE ORIGEN

**DNS** (*Domain Name Service*, Servicio de Nombre de Dominio): Proporciona el servicio de traducción de nombres de domino en direcciones IP reales.

**TFTP** (*Trival File Transport Protocol*, Protocolo de Transporte de Archivo Trivial): El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los diseñadores de software.

## Capa de Transporte

Las funciones principales de la capa de transporte son regular el flujo de información para garantizar la conectividad de extremo a extremo entre aplicaciones de host de manera confiable y precisa. El control de extremo a extremo, que suministran las ventanas deslizantes, y la confiabilidad proporcionada por el uso de números de secuencia y acuses de recibo son las funciones principales. En el nivel de transporte aparecen dos protocolos principales:

**TCP** : Ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. Para ello, en el host fuente, parte el flujo de bits en mensajes discretos y los envía, mientras que en el host destino los recibe y los monta de nuevo para crear el flujo original, manejando el control de flujo de la transmisión.

El formato de los paquetes TCP, es el siguiente:

**Puerto de origen y destino**. Identifican los puntos terminales de la conexión a través de un número único de puerto, es decir, las aplicaciones que envían y reciben la información.

**Números de secuencia**. Es la asignación numérica del paquete enviado.

**Número de asentamiento**. Es la asignación numérica del paquete recibido.

**Offset**. Contiene la longitud de la cabecera.

**Reservado**.

**Flags**. Se utiliza para enviar código entre dos computadoras, tiene una longitud de 6 bits y puede asignar los siguientes valores:

1. Urgente
2. Asentamiento
3. Impulso (*push*). Datos enviados por el usuario.
4. Restablecimiento (*reset*). Utilizado para finalizar la comunicación.
5. Sincronización (*synchronize*). Utilizado para establecer la comunicación.
6. Finalizado (*finish*). Utilizado para terminar una comunicación.

**Ventana**. Controla el tamaño de los paquetes de datos que se pueden enviar y realiza funciones relativas al control de flujo.

**Cheksum**. Contiene el código de redundancia para la cabecera y el paquete de datos.

**Puntero de urgencia**. Indica la localización dentro del paquete de datos considerados como urgentes.



TESIS CON
FALLA DE ORIGEN

**Opciones.** Si existe un manejo diferente de la información, la descripción se coloca en este campo.

**Relleno (padding).** Se utiliza para completar el campo de opciones hasta un múltiplo de 32 bits. Está compuesto por ceros.

Las conexiones TCP son punto a punto y full dúplex, caracterizándose éste último tipo porque en ellas se permite una transferencia concurrente en ambas direcciones, con lo que en realidad existen dos flujos independientemente que se muevan en direcciones opuestas y sin ninguna interacción aparente. Este hace que se reduzca eficazmente el tráfico en la red.

**UDP** (*User Datagram Protocol*, Protocolo de Datagrama de Usuario): Protocolo no confiable y no orientado a conexión para la entrega de mensajes discretos. En este caso los paquetes enviados mediante el protocolo IP reciben el nombre específico de datagramas, éstos se envían sin realizar una conexión definida entre los host, ni mantener un control de los paquetes enviados y recibidos. Los datagramas se enrutan de manera independiente, por lo que deben llevar la dirección completa de destino.

Los campos que conforman el datagrama son:

- Puerto de origen
- Puerto de destino
- Longitud
- Checksum
- Datos

## Capa de Red

En el modelo TCP/IP existe solamente un protocolo, el IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada, IP sirve como protocolo universal que permite que cualquier computadora en cualquier parte del mundo pueda comunicarse en cualquier momento, y es la base fundamental de Internet.

El protocolo **IP** define las unidades de transferencia de datos, denominadas paquetes o datagramas, y se encarga de su transferencia desde el host origen al host destino, se implementa por software. El papel de la capa IP es averiguar como enrutar paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP, para hacerlo posible, cada interfaz en la red necesita una dirección IP, la dirección IP identifica un host de forma única, el host no pueden tener una misma dirección IP pública, pero si pueden tener la misma IP si pertenecen a dos redes privadas diferentes.

El protocolo **IP** no está orientado a conexión y no es confiable, ya que manda paquetes (datagramas) sin contar con mecanismos de verificación de entrega y sin comprobación de errores. Afortunadamente, el protocolo superior, TCP, se encarga de corregir estas debilidades, en cuanto al ruteo o direccionamiento de los datagramas, se puede realizar paso a paso por todos los nodos o mediante tablas de rutas estáticas o dinámicas.

Este protocolo es usado por los de la capa de transporte para encaminar los datos a su destino, siendo ésta su última misión, por lo que no se preocupa de la integridad de la información que contienen los paquetes. Para poder direccionar los datagramas, IP introduce una nueva cabecera formada por 160 bits, y que contiene diferentes datos necesarios para poder enrutar los paquetes, como la longitud de la cabecera, la longitud total del datagrama, un número de identificación, tipo de



TESIS CON
FALLA DE ORIGEN

protocolo al que pertenece el datagrama, campo de comprobación (checksum), dirección de origen, dirección de destino, etcétera. A pesar de ser el protocolo IP el único encargado del direccionamiento a nivel general, a nivel interno existe otro protocolo ampliamente usado, el RIP *(Routed Information Protocol,* Protocolo de Información de Ruteo), conocido también por el programa que lo implementa, el Route Daemon. Es consecuencia directa de la implementación del ruteo en redes locales, y divide las máquinas participantes en el proceso de ruteo en activas y pasivas. Los ruteadores activos anuncian sus rutas a los otros difundiendo un mensaje cada 30 segundos, mensaje que contiene información tomada de la base de datos de ruteo actualizada. Las máquinas pasivas listan y actualizan sus rutas con base en estos mensajes.

**Formato de los datagramas IP**

Tiene una longitud mínima de 20 bytes, consta de una cabecera de 20 bytes fijos y una parte para los datos de longitud variable. Los campos de que consta la cabecera son:

**Versión.** Indica la versión del protocolo de cada datagrama.

**Opciones.** Es utilizado con fines de seguridad, enrutamiento, fuente informe de errores, depuración y sellado de tiempo entre otros.

**Tipo de servicio.** Indica el tipo de servicio que desea obtener de una subred.

**Longitud total.** Longitud total del datagrama IP.

**Identificación.** Con este dato, el servidor destinatario identifica a quien pertenece el datagrama recibido.

**Flags.** No se utiliza.

**Fragmento de offset.** Indica el lugar del datagrama actual al cual pertenece este fragmento.

**TTL.** Es un contador que se utiliza para limitar el tiempo que los paquetes pueden itinerar por la red sin llegar a su destino. Cuando llega a cero, el paquete es destruido.

**Protocolo.** Indica el proceso de transporte al que pertenece el datagrama, las opciones más habituales son TCP y UDP.

**Checksum de cabecera.** Código de redundancia de la cabecera.

**Dirección de origen y destino.** Contienen las direcciones IP del servidor de origen y destino.

**Opciones.** Se definen variaciones para el tráfico de información.

**Padding.** En caso de que el campo opciones sea utilizado, se completa con ceros hasta llegar a múltiplos de 32 para conseguir un formato uniforme.

**Datos.** La información que transporta el paquete.

Como TCP/IP no especifica claramente un protocolo de nivel de enlace de datos, era necesario un mecanismo para traducir las direcciones IP a direcciones que entendieran el software de capa de enlace de datos por sobre el que corre TCP/IP y para controlar posibles errores al nivel de subred. Por eso se introdujeron protocolos específicos, entre los que destacan:

**ICMP** (*Internet Control Messages Protocol*, Protocolo de Mensajes de Control de Internet): Es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta, etcétera, es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

**ARP** (*Address Resolution Protocol*, Protocolo de Resolución de Direcciones): Una vez que un paquete llega a una red local mediante el ruteo IP, la entrega al host destino se debe realizar forzosamente mediante la dirección MAC (*Medium Access Control*, Control de Acceso al Medio), número de la tarjeta de red, por lo que hace falta algún mecanismo capaz de transformar la dirección IP que figura como destino en el paquete de la dirección MAC equivalente, es decir, se obtiene la relación dirección lógica-dirección física. Esto sucede así porque las direcciones Ethernet y las direcciones IP son dos números distintos que no guardan ninguna relación entre ellos.

De esta labor se encarga el protocolo ARP, comparar en las LAN direcciones IP con direcciones Ethernet (de 48 bits) de forma dinámica, evitando así el uso de tablas de conversión. Mediante este protocolo una máquina determinada (generalmente un ruteador de entrada a la red o un swicht) puede hacer un broadcast mandando un mensaje, denominado petición ARP, a todas las demás máquinas de su red para preguntar que dirección local pertenece a alguna dirección IP, obteniendo respuesta por la máquina buscada mediante un mensaje de respuesta ARP, en el que le envía su dirección Ethernet. Una vez que la máquina que solicita tiene este dato envía los paquetes al host destino usando la dirección física obtenida.

**RARP** (*ARP Reply*, ARP por Réplica): Permite que una máquina que acaba de arrancar, sin disco duro, pueda encontrar su dirección IP desde un servidor, para ello utiliza el direccionamiento físico de red, proporcionando la dirección hardware física (MAC) de la máquina de destino para identificar de manera única el procesador, transmitiendo por difusión la solicitud RARP. Una vez que la máquina obtiene su dirección IP la guarda en memoria, y no vuelve e usar RARP hasta que no se inicia de nuevo.

### 6.4 Direcciones IP

El papel de la capa IP es averiguar como encaminar paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP. Para hacerlo posible, cada interfaz en la red necesita una dirección IP, que identifica, de forma única, a la computadora y a la red a la cual pertenece, ya que el sistema de direcciones IP es un sistema jerárquico. Se trata de una dirección única a nivel mundial y la concede INTERNIC (*Internet Network Information Center*, Centro de Información de la Red Internet).



TESIS CON
FALLA DE ORIGEN

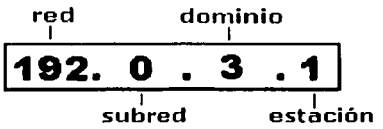


Fig. 1.13 Definición de octetos para direcciones IP

Consiste en 32 bits que normalmente se expresan en forma decimal, en cuatro grupos de tres dígitos separados por puntos, cada número estará entre cero y 255, cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111), los escribimos en la forma decimal para hacerlos más comprensibles, pero hay que tener bien claro que la red entiende sólo direcciones binarias. No todas las direcciones IP son válidas, no podemos asignar a un host una IP aislada, pues no existen IP aisladas, si no que forman parte siempre de alguna red. Todos los hosts conectados a una misma red poseen direcciones IP con los primeros bits iguales (bits de red), mientras que los restantes son los que identifican a cada host concreto dentro de esa red.

Para redes que no van a estar nunca conectadas con otras, se pueden asignar las direcciones IP que se desee, aunque de forma general, dos nodos conectados a una misma red no pueden tener la misma dirección IP. A partir de una dirección IP una red puede determinar si los datos deben ser enviados a través de un ruteador o gateway hacia el exterior de la red, si los bytes correspondientes a la red de la dirección IP son los mismos que los de la dirección actual, los datos no se pasarán al ruteador; si son diferentes si pasarán, para que los direccione hacia el exterior de la red. En este caso, el ruteador tendrá que determinar el camino idóneo con base en la dirección IP de los paquetes y una tabla interna que contiene la información de enrutamiento.

Desde el punto de vista de su accesibilidad podemos clasificar las direcciones IP en:

**Direcciones IP públicas**

Aquellas que son visibles por todos los hosts conectados a Internet. Para que una máquina sea visible desde Internet debe tener asignada obligatoriamente una dirección IP pública, y no puede haber dos host con la misma dirección.

**Direcciones IP privadas**

Aquellas que son visibles únicamente por los hosts de su propia red o de otra red privada interconectada por medio de ruteadores. Los hosts con direcciones IP privadas no son visibles desde Internet, por lo que si quieren salir a ésta, deben hacerlo a través de un ruteador o un proxy que tenga asignada una IP pública. Las direcciones IP privadas se utilizan en redes privadas para interconectar las computadoras de las áreas de trabajo.

Desde el punto de vista de su perdurabilidad podemos clasificar las direcciones IP en:

**Direcciones IP estáticas**

Aquellas asignadas de forma fija o permanente a un host determinado, por lo que cuando una máquina con este tipo de IP se conecte a la red lo hará siempre con la misma dirección IP. Normalmente son usados por servidores web, ruteadores o máquinas que deban estar conectadas a la red de forma permanente, y en el caso de direcciones IP públicas estáticas hay que contratarlas, generalmente a un ISP (*Internet Service Provider*, Proveedor de Servicios de Internet). Las conexiones a Internet mediante ADSL son de este tipo.

**Direcciones IP dinámicas**

Aquellas que son asignadas de forma dinámica a los hosts que desean conectarse a Internet y no tienen una IP fija. Un ejemplo típico de este tipo de direcciones IP es el de una conexión a Internet mediante módem. El ISP dispone de un conjunto de direcciones IP para asignar a sus clientes, de forma que cuando uno de ellos se conecta mediante modem se le asigna una de estas IP, que es válida durante el tiempo que dura la conexión. Cada vez que el usuario se conecte lo hará con una dirección IP distinta.

**Nombre de Dominio**

Como una dirección IP escrita en cualesquiera de estos formatos es difícil de recordar, se optó por poder asignar un nombre de dominio a cada dirección IP, nombre que fuera más fácil de recordar. Este es el motivo por el que nos referimos a la dirección de Yahoo como yahoo.com, y no como 64.58.76.225, que es su dirección IP expresada en forma decimal.

Pero entonces, ¿cómo sabe la computadora a qué IP nos referimos para mandarle los paquetes?, a través del DNS (*Domain Name System*, Sistema de Nombres de Dominio), que consiste en una serie de tablas en las que se registra la relación IP-nombre de dominio, inicialmente estas tablas se guardaban en un único computadora central, en un archivo llamado "host.txt", que contenía una tabla de nombres de estructura plana, por lo que cuando otro host cualquiera necesitaba resolver una dirección IP en el nombre de dominio asociado necesitaba consultar a ésta computadora central. Pero a medida que las direcciones IP y sus nombres asociados fueron creciendo el archivo "host.txt" se fue haciendo demasiado grande y complejo, el mantenimiento del mismo se hizo muy complicado y el tráfico hacia ese computadora llegó a saturar la red. Por estos motivos se hizo necesario idear e implementar un nuevo sistema de resolución de nombres de dominio que distribuyese el trabajo entre varios servidores especiales, denominados servidores DNS, que forman una estructura jerárquica.

Para su funcionamiento, el sistema DNS utiliza tres componentes principales:

**Clientes DNS** (*resolvers*): Son host particulares, estaciones de trabajo o servidores que envían peticiones de resolución de nombres a un servidor DNS.

**Servidores DNS** (*name servers*): Son servidores especiales que contestan a las peticiones de los clientes, consultando para ello sus bases de datos de resolución. En caso de no disponer de la equivalencia solicitada por el cliente pueden reenviar la petición a otro servidor DNS.

**Espacio de nombres de dominio** (*domain name space*): Son bases de datos distribuidas entre distintos servidores.

El espacio de nombres de dominio está estructurado jerárquicamente, en forma de árbol, clasificando los distintos dominios en niveles. El punto más alto de la jerarquía lo ocupa el denominado dominio raíz. De él parten los dominios de primer nivel, y de cada uno de éstos parten dominios de segundo nivel, y así sucesivamente. Cada uno de los dominios puede contener tanto host particulares como más subdominios.

Cuando la capa IP de un host concreto necesita saber la dirección IP de una serie de paquetes a partir de los nombres de dominio se establece una conexión UDP (*User Datagram Protocol*, Protocolo de Datagramas de Usuario) con el servidor DNS adecuado, que le da la equivalencia necesaria.



TESIS CON
FALLA DE ORIGEN

Actualmente cada servidor DNS gestiona y actualiza los nombres de host de un dominio o subconjunto de nodos de Internet que son administrados por un organismo, empresa o institución. De esta forma, cuando se conecta un nuevo nodo a Internet, su nombre de host es dado de alta en el servidor DNS del dominio al que corresponda. Los dominios de un nodo van separados por puntos y organizados de forma jerárquica, empezando por el dominio de mayor nivel.

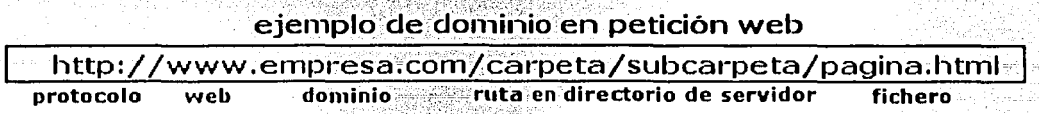


Fig. 1.14 Ejemplo de dominio en petición web

**Tipos de servidores DNS**

En función del ámbito de dominios que abarca y de su posición en la jerarquía, los servidores DNS se clasifican en las siguientes categorías:

**Servidores DNS primarios** (*Primary Name Servers*): Éstos almacenan la información de dominios en una base de datos local, siendo los responsables de mantener la información de los dominios actualizada, por lo que cualquier cambio en los datos o cualquier alta o baja de dominio debe ser comunicada a estos servidores.

**Servidores DNS secundarios** (*Secundary Name Servers*): Se encuentran por debajo de los anteriores en la jerarquía, por lo que deben obtener de ellos los datos correspondientes a su zona de acción, mediante un proceso de copia denominado "transferencia de zona". Estos servidores actúan además como sistemas de seguridad, al mantener la información de forma redundante, con lo que si un servidor DNS tiene problemas, la información se puede recuperar desde otro. Además, evitan la sobrecarga del servidor principal, distribuyendo el trabajo entre distintos servidores situados estratégicamente, con lo que se gana velocidad en las resoluciones.

**Servidores DNS maestros** (*Master Name Servers*): Son los que transfieren las zonas desde los servidores primarios a los servidores secundarios. Puede ser a la vez un servidor primario o secundario de esa zona. Cuando un servidor secundario arranca busca un servidor maestro y le solicita la transferencia de zona, que éste habrá obtenido previamente del servidor primario correspondiente. Con ello se consigue evitar que los servidores secundarios sobrecarguen al servidor primario con transferencias de zona.

**Servidores DNS locales** (*Caching-Only Servers*): Servidores que no tienen autoridad sobre ningún dominio, limitándose tan solo a contactar con otros servidores DNS para resolver peticiones de sus clientes a partir de los datos de direcciones almacenados en su memoria caché. Cuando un cliente solicita a uno de estos servidores la resolución de un nombre de dominio lo primero que hace es consultar su memoria caché. Si encuentra la dirección IP asociada se la devuelve al cliente, y en caso de no encontrarla consulta a otros servidores hasta que la consigue, enviándosela al cliente y anotándola en su caché para próximas peticiones de otros clientes.

**Resolución de nombres de dominio**

Se conoce con el nombre de resolución de nombres de dominio el proceso de traducción de un nombre de dominio a su correspondiente dirección IP.

Cuando un cliente DNS (nuestra máquina) debe obtener la IP asociada a un nombre de dominio concreto debe formular una pregunta formal al servidor DNS correspondiente, pudiendo efectuarse la misma de tres formas diferentes:

**Preguntas DNS recursivas:** Éstas son en las que el servidor DNS debe intentar por todos los medios posibles obtener la resolución pedida, aunque para ello tenga que preguntar a otros servidores DNS. Este tipo de preguntas es el que suelen hacer los host al servidor DNS local de su proveedor de Internet.

**Preguntas DNS iterativas:** Son aquellas en las que el servidor devolverá al cliente la resolución pedida en caso de conocerla, y en caso contrario le devolverá la dirección IP de otro servidor DNS que sea capaz de resolver el nombre solicitado. Un ejemplo de este tipo de preguntas es el que hace el servidor DNS local de nuestro proveedor de Internet a otros servidores DNS de rango superior cuando no encuentra en su memoria caché la dirección IP asociada al nombre de dominio por el que preguntamos.

**Preguntas DNS inversas:** Son un tipo especial de preguntas, en las cuales conocemos la IP destino y deseamos obtener el nombre de dominio asociado. En estos casos, y para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial denominado in-addr.arpa. Cuando un cliente DNS desea conocer el nombre de dominio asociado a una IP dada se formula una pregunta inversa, en la que se invierten los 4 bytes de la dirección IP debido a que los nombres de dominio son más genéricos por la derecha, al contrario de lo que ocurre con las direcciones IP.

## 7. CLASES DE REDES SEGÚN SU IP

A la hora de asignar direcciones IP a una red se considera el tamaño y las necesidades de ésta, por lo que se distinguen 3 tipos principales de redes (y de direcciones IP):

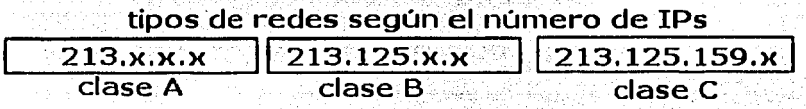


Fig. 1.15 Tipos de redes según el número de IPs

**Redes de clase A:** Son aquellas redes que precisan un gran número de direcciones IP, debido al número de host que comprenden. A este tipo de redes se les asigna un rango de direcciones IP identificado por el primer grupo de 3 dígitos (primer octeto de la IP), de tal forma que disponen de los otros 3 grupos siguientes para asignar direcciones a sus host. Su primer byte tiene un valor comprendido entre 1 y 126.

| Clase A |
| --- |
| 1-126 |

El número de direcciones resultante es muy elevado, más de 16 millones, por lo que las redes de clase A pueden ser asignadas a organismos que requieran conectar más de 64,516 equipos a Internet.

**Redes de clase B:** Son redes que precisan un número de direcciones IP intermedio para conectar todos sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los dos primeros grupos de 3 dígitos (primer y segundo octetos de la IP), de tal forma que disponen de los otros 2 grupos siguientes para asignar direcciones a sus host.

Sus dos primeros bytes deben estar entre 128.1 y 191.254, por lo que el número de direcciones resultante es de 64,516.

| Clase B |
| --- |
| 128-191 |

Las redes de clase B corresponden a organismos que requieran conectar más de 256 equipos a Internet y hasta 64,516 equipos.

**Redes de clase C:** Son redes que precisan un número de direcciones IP pequeño para conectar sus host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los tres primeros grupos de 3 dígitos (primero, segundo y tercer octetos de la IP), de tal forma que disponen de un sólo grupo para asignar direcciones a sus host.

Sus 3 primeros bytes deben estar comprendidos entre 192.1.1 y 223.254.254.

| Clase C |
| --- |
| 192-223 |

El número de direcciones resultante es de 256 para cada una de las redes.

En la Tabla 1.7 se resumen los posibles tipos de redes.

| Clase | primer byte decimal | Número de redes | número de host |
| --- | --- | --- | --- |
| A | 1 – 126 | 126 | 16,387,064 |
| B | 128 – 191 | 16,256 | 64,516 |
| C | 192 – 223 | 2.,064,512 | 254 |

Tabla 1.7 Tipos de Redes

En la tabla anterior se observa que hay ciertos números de red que no se usan, esto es así porque están reservados para usos concretos, de esta forma, las redes cuyo primer byte es superior a 223



TESIS CON
FALLA DE ORIGEN

corresponden a clases especiales, la tipo D y la tipo E, que aún no están definidas, mientras que las que empiezan con el byte 127 (note que falta en la tabla) se usan para propósitos especiales.

También hay que destacar que los valores extremos en cualquiera de los bytes, 0 y 255, no se pueden asignar a ningún host ni red. El número 0 se denomina dirección de red, está reservado como dirección de la propia red, y el 255 se reserva para la función broadcast en las redes Ethernet, mediante la cual, un mensaje es enviado a todas las máquinas de la red, sin salir de ella. La dirección de broadcast (*broadcast address*) hace referencia a todos los host de la misma red.

No todas las direcciones IP posibles son aptas para su uso común. En primer lugar, existen una serie de direcciones reservadas para su uso en redes privadas (aquellas cuyos host no van a ser visibles desde Internet), que sirven para implementar la pila de protocolos TCP/IP a las mismas. Existe un rango de direcciones reservadas según la clase de red.

| Direcciones Especiales |
| --- |
| 127, 224-255 |

### 7.1 Máscara de red

Cuando dos o más redes diferentes se encuentran conectadas entre sí por medio de un ruteador, éste debe disponer de algún medio para diferenciar los paquetes que van dirigidos a los host de cada una de las redes. Es aquí donde entra en juego el concepto de máscara de red, que puede definirse como una dirección IP especial que permite efectuar este enrutamiento interno de paquetes.

Dada una dirección IP de red cualquiera, la máscara de red asociada es aquella que en binario tiene todos los bits que definen la red puestos a 1 (255 en decimal), y los bits correspondientes a los host puestos a 0 (0 en decimal).

Así, las máscaras de red de los diferentes tipos de redes son:

Red Clase A. Máscara de red = 255.0.0.0
Red Clase B. Máscara de red = 255.255.0.0
Red Clase C. Máscara de red = 255.255.255.0

La máscara de red posee la importante propiedad de que cuando se combina con la dirección IP de un host se obtiene la dirección propia de la red. Cuando al ruteador que conecta varias redes le llega un paquete saca de él la dirección IP del host destino y realiza una operación AND lógica entre esta IP y las diferentes máscaras de red que une, comprobando si el resultado coincide con alguna de las direcciones propias de red. Este proceso de identificación de la red destino de un paquete y el host al que va dirigido el paquete, se denomina enrutamiento.

## 8. TÉCNICAS DE CONMUTACIÓN

Cuando los datos hay que enviarlos a largas distancias e incluso a no tan largas, generalmente deben pasar por varios nodos intermedios, estos nodos son los encargados de encauzar los datos para que lleguen a su destino. Este es el problema al que los diseñadores y administradores de redes tienen que enfrentarse, la selección de una ruta óptima entre dos nodos en una red. La conmutación es una técnica de comunicación que facilita la transmisión punto a punto entre fuente y destino en una red informática. A



TESIS CON
FALLA DE ORIGEN

continuación trataremos las técnicas más conocidas: Conmutación de circuitos y conmutación de paquetes.

### 8.1 Conmutación de circuitos

En conmutación de circuitos, los nodos intermedios no tratan los datos de ninguna forma, sólo se encargan de encaminarlos a su destino. En redes conmutadas, los datos que entren a la red, provenientes de alguna de las estaciones, son conmutados de nodo en nodo hasta que lleguen a su destino. Existen nodos sólo conectados a otros nodos y su única misión es conmutar los datos internamente a la red. También hay nodos conectados a estaciones y a otros nodos, por lo que deben de añadir a su función como nodo, la aceptación y emisión de datos de las estaciones que se conectan. Los enlaces entre nodos están multiplexados en el tiempo o por división de frecuencias. Generalmente hay más de un camino entre dos estaciones, para así poder desviar los datos por el camino menos colapsado. Para cada conexión entre dos estaciones, los nodos intermedios dedican un canal lógico a dicha conexión. Para establecer el contacto y el paso de la información de estación a estación a través de los nodos intermedios, se requieren de estos pasos:

| | |
|---|---|
| **Establecimiento del circuito** | El emisor solicita a un cierto nodo el establecimiento de conexión hacia una estación receptora, la cual dedica uno de sus canales lógicos a la estación emisora y se encarga de encontrar los nodos intermedios para llegar a la estación receptora, para lo cual, considera ciertos criterios de enrutamiento. |
| **Transferencia de datos** | Una vez establecido el circuito exclusivo para esta transmisión (cada nodo reserva un canal para esta transmisión), la estación transmite desde el emisor hasta el receptor conmutando sin demoras de nodo en nodo. |
| **Desconexión del circuito** | Una vez terminada la transferencia, el emisor o el receptor indican a su nodo más inmediato que ha finalizado la conexión, y este nodo informa al siguiente de este hecho y luego libera el canal dedicado. Así de nodo en nodo hasta que todos han liberado el canal dedicado. |

Tabla 1.8 Método de conmutación de circuitos

Debido a que cada nodo conmutador debe saber organizar el tráfico y las conmutaciones, éstos deben tener la suficiente "inteligencia" como para realizar su labor eficientemente. La conmutación de circuitos suele ser bastante ineficiente ya que los canales están reservados aunque no circulen datos a través de ellos. Para tráfico de voz, en que suelen circular datos (voz) continuamente, puede ser un método bastante eficaz ya que el único retardo es el establecimiento de la conexión, y luego no hay retardos de nodo en nodo.

La conmutación de circuitos, a pesar de sus deficiencias, es el sistema más utilizado para conectar sistemas informáticos entre sí a largas distancias, debido a la profusión e interconexión que existe (debido al auge del teléfono) y a que una vez establecido el circuito, la red se comporta como si fuera una conexión directa entre las dos estaciones, ahorrando bastante lógica de control.

### 8.2 Conmutación de paquetes

Debido al auge de las transmisiones de datos, la conmutación de circuitos es un sistema muy ineficiente ya que mantiene las líneas mucho tiempo ocupadas, aún cuando no hay información circulando por ellas, además, la conmutación de circuitos requiere que los dos sistemas conectados trabajen a la misma velocidad, cosa que no suele ocurrir hoy en día debido a la gran variedad de sistemas que se comunican. En conmutación de paquetes, los datos se transmiten en paquetes cortos, para transmitir grupos de datos más grandes, el emisor divide estos grupos en paquetes más pequeños y les adiciona una serie de bits de control. En cada nodo, el paquete se recibe, se almacena durante un cierto tiempo y se transmite hacia el emisor o hacia un nodo intermedio.

### 8.3 Ventajas de la Conmutación de Paquetes frente a la de Circuitos

- La eficiencia de la línea es mayor, ya que cada enlace se comparte entre varios paquetes que estarán en cola para ser enviados en cuanto sea posible. En conmutación de circuitos, la línea se utiliza exclusivamente para una conexión, aunque no haya datos a enviar.
- Se permiten conexiones entre estaciones de velocidades diferentes, esto es posible ya que los paquetes se irán guardando en cada nodo conforme lleguen (en una cola) y se irán enviando a su destino.
- No se bloquean llamadas, ya que todas las conexiones se aceptan, aunque si hay muchas, se producen retardos en la transmisión.
- Se pueden usar prioridades, un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos, aquellos más prioritarios según ciertos criterios de prioridad. Cuando un emisor necesita enviar un grupo de datos mayor que el tamaño fijado para un paquete, éste lo divide en paquetes y los envía uno a uno al receptor.

### 8.4 Tipos de Retardo

- Retardo de propagación, tiempo despreciable de propagación de la señal de un nodo a otro nodo.
- Tiempo de transmisión, tiempo que tarda el emisor en emitir los datos.
- Retardo de nodo, tiempo que emplea el nodo desde que recibe los datos hasta que los emite (gestión de colas).

## 8.5 Técnicas básicas para el envío de Paquetes

### Técnica de datagramas

Cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control (número de paquete, nombre, dirección destino, etcétera) y lo envía hacia su destino.

Puede ocurrir que por haber tomado caminos diferentes, un paquete con número llegue a su destino antes que el otro. También puede ocurrir que se pierda un paquete. Todo esto no lo sabe ni puede controlar el emisor, por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido (para su posible reclamación al emisor), y para esto, debe tener el software necesario. En la figura 1.16 se muestra de manera gráfica el flujo de un datagrama.

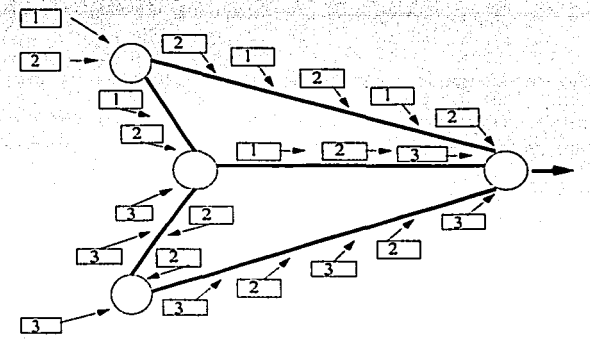

Fig. 1.16 Envío de paquete utilizando datagramas

### Técnica de circuitos virtuales

Antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de Petición de Llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes. Este camino virtual será numerado o nombrado inicialmente en el emisor y será el paquete inicial de Petición de Llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número. De esta forma, el enrutamiento sólo se hace una vez (para la Petición de Llamada). El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez. En la figura 1.17 se muestra el flujo que sigue la información en un circuito virtual.

TESIS CON
FALLA DE ORIGEN

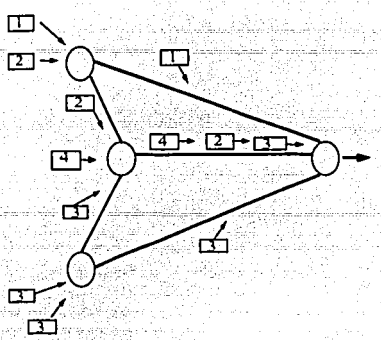

Fig. 1.17 Envío de paquete utilizando circuitos virtuales

**Ventajas de los Circuitos Virtuales frente a los Datagramas**

- El enrutamiento en cada nodo sólo se hace una vez para todo el grupo de paquetes. Por lo que los paquetes llegan antes a su destino.
- Todos los paquetes llegan en el mismo orden del de partida ya que siguen el mismo camino.
- En cada nodo se realiza la detección de errores, por lo que si un paquete llega erróneo a un nodo, éste lo solicita otra vez al nodo anterior antes de seguir transmitiendo los siguientes.

**Desventajas de los Circuitos Virtuales frente a los Datagramas**

- En datagramas no hay que establecer llamada (para pocos paquetes, es más rápida la técnica de datagramas).
- Los datagramas son más flexibles, es decir que si hay congestión en la red una vez que ya ha partido algún paquete, los siguientes pueden tomar caminos diferentes, lo que en circuitos virtuales no es posible.
- El envío mediante datagramas es más seguro ya que si un nodo falla, sólo un paquete se perderá (en circuitos virtuales se perderán todos).

### 8.6 Comparación entre Conmutación de Circuitos, Conmutación de Paquetes y Datagramas

En conmutación de circuitos hay un retardo inicial hasta establecer la conexión (en cada nodo se produce un retardo). Tras el establecimiento de la conexión, existe el retardo del tiempo de transmisión y el retardo de propagación. Pero toda la información va a la vez en un bloque sin más retardos adicionales.

En conmutación de paquetes mediante circuitos virtuales, existe el mismo retardo inicial que en conmutación de circuitos. Pero además, en cada nodo, cada paquete sufre un retardo hasta que le llega su turno de envío de entre la cola de paquetes a emitir por el nodo. A todo esto, habría que sumar el retardo de transmisión y el retardo de propagación.

En datagramas, se ahorra el tiempo de establecimiento de conexión, pero no los demás retardos que hay en circuitos virtuales. Pero existe el retardo de enrutamiento en cada nodo y para cada paquete. Por tanto, para grupos grandes de datos, los circuitos virtuales son más eficaces que los datagramas, aunque para grupos pequeños sean menos eficaces que los datagramas.

Existen dos niveles en donde se pueden utilizar técnicas de datagramas y de circuitos virtuales. En un nivel interno (entre estación y nodo), se llaman operación de datagrama interno y operación de circuito virtual interno. Pero cuando se sale de este ámbito controlable por la estación emisora, la propia red decide la utilización de servicios de datagrama externo o servicio de circuito virtual externo para sus comunicaciones (ocultos al usuario o emisor).

Para los servicio externos hay una serie de consideraciones a seguir:

Si se utilizan operaciones de datagrama interno y servicios de datagrama externo, al haber errores, no hay pérdidas de tiempo en establecer nuevas conexiones ni se necesitan muchos espacios de almacenamiento.

Si se utilizan operaciones de circuitos virtuales internos y servicios de circuitos virtuales externos, se mejoran las prestaciones para transmisiones de grandes grupos de información y de acceso a terminales remotos.

## 9. ENRUTAMIENTO

Se conoce con el nombre de enrutamiento (*routing*) el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada. Durante el viaje entre ambos host, los paquetes han de atravesar un número indefinido de host o dispositivos de red intermedios, debiendo existir algún mecanismo capaz de direccionar los paquetes correctamente de uno a otro hasta alcanzar el destino final. Este mecanismo de ruteo es responsabilidad del protocolo IP, y lo hace de tal forma que los protocolos de las capas superiores, como TCP y UDP, no tienen constancia alguna del mismo, limitándose a preocuparse de sus respectivas tareas.

Cuando un host debe enviar datos a otro, lo primero que hace es comprobar si éste se encuentra en su misma red examinando la dirección IP del host destino. Si la parte de red de dicha dirección coincide con la de su propia red (o subred), los datagramas son enviados directamente mediante la dirección de la tarjeta NIC del host destino, conocida como dirección física. En caso de que no conozca la misma, se envía un mensaje de petición ARP, que será respondido por el host destino enviando su dirección física. Este proceso recibe el nombre de ruteo directo.

En caso de que el remitente compruebe que el destinatario no se encuentra en su propia red local, los datagramas son enviados a un dispositivo especial, denominado ruteador o gateway, que es el que se va a encargar de buscar la ruta de direccionamiento que se deben dar a los datagramas para que alcancen su destino correcto. El proceso entonces es conocido con el nombre de ruteo indirecto, y es el común en comunicaciones por Internet.

Un ruteador es un dispositivo conectado a dos o más redes, perteneciendo a todas ellas a la vez, por lo que tendrá una dirección física y una dirección IP diferente en cada una de las mismas.

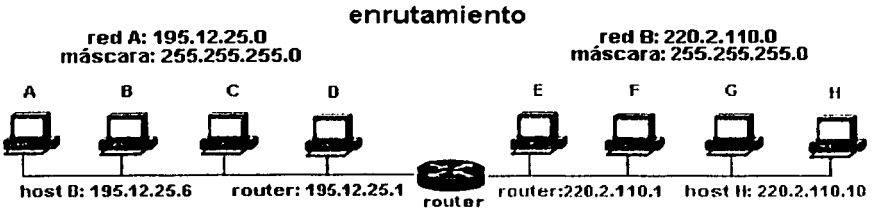


Fig. 1.18 Modelo de enrutamiento

**Características**

La función de enrutamiento tiene los siguientes requisitos:

Exactitud: es la fidelidad en la entrega de información.

Sencillez: es la capacidad de encontrar el camino más corto y menos transitable para que viaje un paquete de información.

Robustez: es la capacidad para redirigir el tráfico a zonas seguras cuando hay fallos.

Estabilidad: es posible que si un sistema es muy robusto, se convierta en inestable al reaccionar demasiado bruscamente ante situaciones concretas.

Imparcialidad: es la capacidad para tratar de forma similar a las comunicaciones sin importar la distancia entre los nodos. Existen sistemas que premian, las conexiones cercanas frente a las más lejanas, con lo que la comunicación entre estaciones alejadas se dificulta.

Optimización: es posible que la robustez y la imparcialidad reporten un costo adicional de cálculo en cada nodo, lo que implica que ya no es el sistema más óptimo.

Eficiencia: es la capacidad para entregar correctamente la información de un nodo a otro.

**Lugar e instante de decisión**

El instante en que se decide hacia donde se enviará un paquete en un nodo es muy importante:

En datagramas, esto se produce una vez por paquete.

En circuitos virtuales se produce una vez por petición de llamada.

Existen tres lugares en los que se puede decidir desde donde enviar un paquete:

En el propio nodo (enrutamiento distribuido).

En un nodo señalado para esta tarea (enrutamiento centralizado). Este enrutamiento tiene el inconveniente de que si este nodo se estropea, el enrutamiento de todos los nodos que dependen de él es imposible, y todos los nodos serán inservibles.

En la propia estación de origen.



TESIS CON
FALLA DE ORIGEN

## 9.1 Estrategias de enrutamiento

**Enrutamiento estático**: Cada nodo enrutará sus datos a otro nodo adyacente y no cambiará dicho enrutamiento nunca (mientras dure la topología de la red). Existe un nodo de control que mantiene la información centralizada. Como cada nodo enrutará sus datos sólo a un nodo adyacente para cada nodo destino posible, sólo es necesario almacenar estos contactos entre nodos adyacentes y no todos los caminos entre todos los nodos de la red. En el nodo central se almacenan todas las tablas de enrutamiento, pero en cada nodo sólo hay que almacenar las filas que conectan ese nodo con el siguiente para conseguir el enrutamiento a cada nodo posible destino de la red. Este sistema es muy eficiente y sencillo pero poco tolerante a fallos en nodos adyacentes, ya que sólo puede enrutar a uno.

**Inundaciones**: Consiste en que cada nodo envía una copia del paquete a todos sus vecinos y éstos lo reenvían a todos sus vecinos excepto al nodo del cuál lo habían recibido. De esta forma se asegura que el paquete llegará a su destino en el mínimo tiempo posible. Para evitar que a un nodo llegue un paquete repetido, el nodo debe guardar una información que le haga descartar un paquete ya recibido. Esta técnica, al ser muy robusta y de costo mínimo, se puede usar para mensajes de alta prioridad o muy importante. El problema es la gran cantidad de tráfico que se genera en la red.

**Enrutamiento aleatorio**: Se elige aleatoriamente el nodo al cual se va a reenviar el paquete. De esta forma, se puede asegurar que el paquete llegará al destino pero en un mayor tiempo que con la técnica de inundaciones, pero el tránsito en la red es mucho menor.

**Enrutamiento adaptable**: Consiste en que la red va cambiando su sistema de enrutamiento conforme se cambian las condiciones de tráfico de la red. Para conseguir esto, los nodos deben de intercambiar información sobre congestión de tráfico y otros datos. En estas técnicas de intercambio de información entre nodos, pueden hacerse intercambios entre nodos adyacentes, todos los nodos, o incluso que haya un nodo central que coordine todas las informaciones.

**Desventajas**

- El costo de procesamiento en cada nodo aumenta.
- Al intercambiar información de nodo en nodo, aumenta el tráfico.
- Es una técnica muy inestable.

**Ventajas**

- El usuario cree que aumentan las prestaciones.
- Se puede ayudar en el control de la congestión.

TESIS CON
FALLA DE ORIGEN

# CAPÍTULO 2
# INTERNET

## 1. HISTORIA DE INTERNET

La historia del nacimiento de Internet está llena de sucesos importantes, algunos de los cuales se podrían pasar por alto cuando se revisan de manera textual, por esta razón se prefirió hacer un cronograma (Tabla 2.1), que presenta dichos sucesos de manera ordenada y resumida, con el fin de que el lector conozca en forma clara los sucesos que dieron vida a lo que hoy se conoce como Internet .

| Año | Acontecimiento | Descripción |
|---|---|---|
| 1960 | Surge la idea | El surgimiento fue motivado cuando la guerra fría era más latente y, como consecuencia de solucionar, un problema estratégico en los Estados Unidos, sus centros de comunicaciones podrían ser atacados, por lo que nace la idea de diseñar un sistema no centralizado. |
| 1968 | Nace la primera Red de Computadoras | En las Universidades del Sureste de los Estados Unidos una agencia llamada Arpanet (*Advanced Research Projects Agency Network*, Red de la agencia de proyectos de Investigación Avanzada), realiza un proyecto que consistía básicamente en la unión entre sí de cuatro computadoras enormes mediante líneas de transmisión. Este proyecto fue financiado por Darpa (*Defense of Advanced Research Projects Agency*, Agencia de proyectos de Investigación Avanzada para la defensa). |
| 1972 | La red crece a 37 nodos | Los principales Centros de Investigación, Universidades y Centros Militares estaban unidos entre sí, esta red era utilizada solo por expertos dado que no era nada amistosa, sino todo lo contrario, muy complicada de usar. |
| 1973 | Incorporación de Protocolos | Aquí se integraron los Protocolos, conjuntos de normas que marco las pautas y privilegios entre las computadoras; el más conocido, TCP/IP (*Transfer Control Protocol / Internet Protocol*, Protocolo de Control de Transferencia / Protocolo de Internet), sistema que establece las bases de la mayor parte del Internet. El TCP se encarga de fragmentar la información en pequeños paquetes para después volverlos a juntar en un destino final. El IP tiene como función el verificar que estos paquetes vayan dirigidos correctamente hacia un mismo destino. |



TESIS CON
FALLA DE ORIGEN

| Año | Acontecimiento | Descripción |
|---|---|---|
| 1983 | TCP / IP queda establecido | Este conjunto de normas denominado arquitectura de protocolos, establecido por Vinton Cerf, informático estadounidense que formaba parte de un proyecto dirigido por Robert Kahn y patrocinado por ARPA; fue universalmente adoptado. |
| 1983 | Separación de Arpanet | En este año se produce la separación de ARPANET y así la red pudo seguir creciendo sin la supervisión del mando militar americano. |
| 1989 | Desaparece Arpanet | |
| 1989 | Nace el sistema "Archie" | Esta aplicación de Internet, cuya función era la de recompilar, listar y distribuir la información dentro de Internet de manera automatizada, periódicamente se conectaba a todos los servidores de FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos) conocidos y obtenía un listado de los archivos disponibles, sin embargo, aún así se requerían ciertos conocimientos técnicos para manejar esta herramienta. |
| 1989 | Se crea el HTTP | En este año el acontecimiento más importante para el desarrollo de Internet surge cuando el informático británico Timothy Berners-Lee que trabajaba para el Consejo Europeo de Investigación Nuclear (*CERN*), crea el HTTP (*Hipertext Transfer Protocol*, Protocolo de Transferencia de Hipertexto), protocolo usado para la transferencia de documentos WWW y HTML (*Hipertext Markup Language*, Lenguaje de Marcado de Hipertexto), lenguaje en donde se forman la mayoría de las páginas que se visualizan en Internet. |
| 1991 | Se da lugar a la WWW (*World Wide Web, Red Mundial Amplia*). | Debido al Lenguaje HTTP que admite elementos de hipertexto y multimedia, se da lugar a WWW. Este sistema, se basa en conectar unos textos con otros a base de incluir enlaces en ellos (hipertexto), y fue costoso de desarrollar. |
| 1991 | Se desarrolla la primera interfaz intuitiva para Internet el Gopher. | Durante 1991, en un intento por fomentar el uso de la informática y telecomunicaciones para los estudiantes, la Universidad de Minesota, implementó Gopher, que proporcionaba a los alumnos directorios completos de información de su interés, consistía en un sistema de menús para acceder a los archivos y tuvo un gran éxito, en pocos años había más de 10.000 en el mundo, todos interconectados. La utilidad de este aumentó con un programa que recorría los diferentes Gophers (servicio FTP) del mundo recopilando enlaces y construyendo un índice, este programa se le denomino Verónica, también conocido como programa araña. |
| 1992 | Surge Delphi | Primera empresa privada en ofrecer acceso a Internet. |

| Año | Acontecimiento | Descripción |
|---|---|---|
| 1993 | **Se crea el primer Browser o Navegador** | Este programa, minimizó costos, sirvió para visualizar documentos WWW y para navegar por Internet. Los navegadores o browser son aplicaciones de hipertexto que facilitan la navegación por los servidores de Internet y los mas avanzados, cuentan con multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, Newsgroup y E-mail. |
| 1995 | **Desaparece la limitación de uso a Internet** | Cualquier pretensión de limitación al uso comercial de Internet desapareció definitivamente, AOL (*America on Line*), Prodigy y Compuserve entraron en la Red y la Internet comercial inició su camino. |

Tabla 2.1 Historia de Internet

## 2. DEFINICIÓN DE INTERNET

El Internet, algunas veces simplemente llamado "La red, WWW, Web, W3 ó World Wide Web" es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, acceder información de otra computadora e inclusive tener comunicación directa con otros usuarios en otras computadoras.

Es una red informática, donde un conjunto de computadoras están conectadas entre sí, proporcionándose facilidades e intercambiando información entre usuarios situados en puntos geográficamente distantes (ver Fig. 2.1). El rápido crecimiento del Internet ha conseguido que la red haya tomado el nombre de "*La red de redes*", debido a que las computadoras de todo el mundo están conectadas.

Hoy en día, el Internet es un medio de comunicación público, cooperativo y autosuficiente en términos económicos, accesible a cientos de millones de personas en el mundo entero. Físicamente, el Internet usa parte del total de recursos actualmente existentes en las redes de telecomunicaciones.

La principal diferencia entre Internet y cualquier otra red informática, reside en que ésta no pertenece a ningún país, ni organismo oficial, ni a ninguna empresa determinada, es decir, se trata de una red libre ya que cualquier persona puede acceder a ella desde cualquier punto del planeta, de la misma forma que no existe ningún tipo de restricción para toda la información que circula por la misma.

Sin embargo, existen organismos internacionales repartidos por todo el mundo y organizados de forma jerárquica, sin ningún afán de lucro, encargados de regular el crecimiento de Internet y garantizar su buen funcionamiento.

TESIS CON
FALLA DE ORIGEN

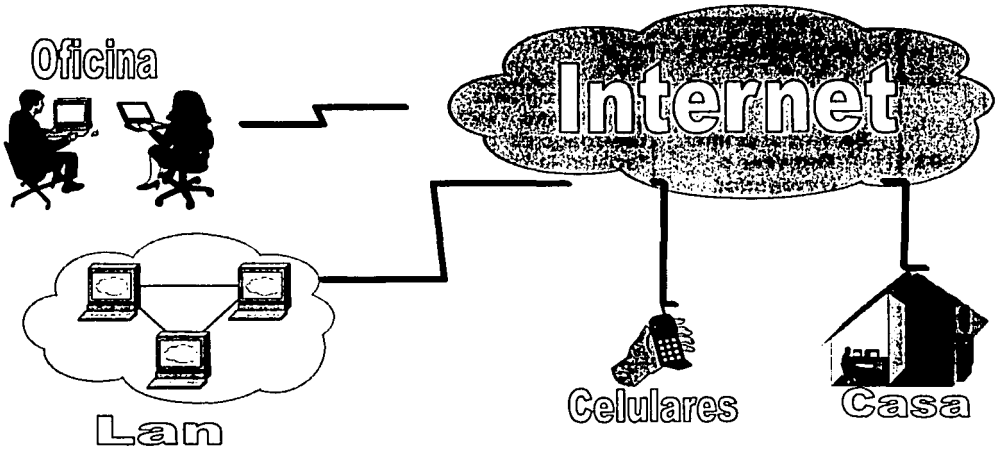


Fig. 2.1 Modelo de Conexión a Internet

## 3. SERVICIOS QUE OFRECE INTERNET

Probablemente la característica más llamativa de Internet, es que se puede tener acceso a cualquier parte del mundo por el precio de una llamada, es decir, la distancia no es proporcional al costo de la comunicación establecida, debido a que cada tramo de red gestiona sus propios gastos y no son repercutidos directamente al usuario.

Para muchos usuarios del Internet, el correo electrónico (*e-mail*) ha reemplazado prácticamente al servicio postal, el correo es la aplicación de mayor uso en la red, también se pueden realizar conversaciones "en vivo" con otros usuarios usando IRC (*Internet Relay Chat*, Conversación retardada de Internet), realizar compra-venta de cualquier tipo de producto, tener acceso a información en bibliotecas virtuales, leer noticias del mundo, buscar información de temas específicos, lograr conexiones con otros equipos por medio de FTP, y más recientemente, el software y hardware para telefonía en Internet, que permite conversaciones de voz en línea y finalmente las videoconferencias en tiempo real que auque el costo es elevado y se requiere de muchos recursos para lograrla, está iniciando un largo camino por recorrer en el mundo de Internet.

Todos los equipos que están conectados a Internet deben emplear el mismo lenguaje para comunicarse, los lenguajes de comunicación entre computadoras se llaman protocolos, el lenguaje de Internet es el denominado TCP/IP y está formado por dos protocolos o niveles de comunicación:

- El IP que es el encargado por una parte de establecer la manera en que las computadoras se identifican, y por otro lado es el encargado de establecer el direccionamiento de la información que llega de una computadora a otra a través de la Red.



TESIS CON
FALLA DE ORIGEN

- El TCP que es el encargado de garantizar que la comunicación entre dos computadoras sea fiable y que llegue sin ningún problema a su destino.

A continuación describiremos los servicios que podremos encontrar en Internet:

- **Archie:** Sistema para recoger, indexar y servir información dentro de Internet automáticamente. Las versiones iniciales proporcionaban un directorio indexado de nombres de archivos de todos los archivos de FTP anónimos de Internet. Las versiones posteriores permiten otros tipos de obtención de información.

- **Audio Conferencias:** Es un servicio interactivo, esta aplicación implica el intercambio de señales de voz entre un grupo de personas. Por lo que la red tendrá que proporcionar conectividad a todos los participantes.

- **Buscadores:** Se utilizan para localizar una determinada página cuya dirección URL (*Uniform Resource Locator,* Localizador de Recursos Uniformes), se desconoce. De los buscadores más conocidos mencionaremos: Netscape, Google, Altavista, México Web, Yahoo, Licos, Infoseek, Exite, Magallan, Opentext, estos trabajan básicamente como si fuera un diccionario virtual, y los métodos de búsqueda que utilizan pueden variar entre cada uno de ellos pero en general son: *Por palabras, Temas, Direcciones IP, Nombres de Sitios Web, Nombres de Empresas*. Los buscadores se pueden clasificar mediante diferentes criterios: *Estructura, Forma de Indexar, Metodología para nuevos enlaces.*

| Criterio | Tipo de Búsqueda | Descripción |
|---|---|---|
| **Por su Estructura** | **Índice temático** | Permiten buscar por temas y subtemas, hasta llegar a la categoría a la que pertenece la web que se busca. Son especialmente útiles cuando lo que se busca no es algo específico. |
| | **Motor de búsqueda** | No clasifican por temas. Suelen estar combinados con los índices temáticos en el mismo web para dar mayor potencia y flexibilidad al usuario. |
| **Por como Indexan** | **Descriptivos** | Sólo permiten encontrar palabras contenidas en ciertas partes de las páginas de web: título, dirección, descripción. |
| | **Full text** | Permiten encontrar cualquier palabra contenida en cualquier parte de las páginas de web. |

| Criterio | Tipo de Búsqueda | Descripción |
|---|---|---|
| Por inclusión de enlaces | No intrusivos | Sólo se pueden encontrar en ellos aquellas páginas que han sido dadas de alta por alguien en el propio buscador. |
| | Intrusivos | Permiten localizar páginas aunque nadie las haya dado de alta, ya que disponen de programas araña (o robots) que recorren la Web indexando todas las páginas que encuentran. Se puede pedir al programa que acuda a un determinado web para acelerar su indexación. También se puede impedir que el programa araña indexe una página. |

Tabla 2.2 Clasificación de los buscadores

Cada buscador tiene sus propias reglas para las búsquedas avanzadas, generalmente todos cumplen con reglas básicas.

Algunos buscadores permiten refinar la búsqueda para ir limitando las páginas requeridas, algunos también permiten hacer preguntas en lenguaje natural. Es importante realizar las búsquedas de forma que los buscadores devuelvan el menor número posible de páginas, es decir, afinar los datos lo más posible.

Desde el punto de vista del creador de webs, una herramienta muy útil para que los buscadores indexen correctamente las páginas son las etiquetas Meta (son etiquetas en la página para encontrar la descripción y palabras claves que se le asocian), que van en la sección Head (encabezado) de las páginas HTML.

- **Chat**: Palabra que en inglés significa conversar, es en realidad eso, una conversación en línea en la que pueden participar a la vez un número muy alto de usuarios. Básicamente se puede comparar al servicio News aunque su diferencia, la instantaneidad de la comunicación, es su mayor atractivo. Esto es lo que hace que el chat sea un servicio actualmente en auge dentro de la Red.

- **Comunicación en Tiempo Real**: Son servicios que en un futuro mejorarán las comunicaciones entre la empresa y su entorno, esto redundará en una reducción de los costos de las comunicaciones empresariales y particulares.

- **Conferencias Audiovisuales**: Es la transmisión de información a través de audio y video. Este servicio es de los más exigentes ya que aquí se necesitan obtener respuestas en tiempo real.

- **Dinero Electrónico y Sucursales Bancarias Virtuales:** Aunque ya es posible comprar, hacer pedidos y pagar por productos en la Web, la parte del pago no es completamente segura, hay varias firmas comerciales trabajando duramente para desarrollar sistemas de pago seguros en Internet, por ejemplo CyberCash Inc., Checkfree Corporation, DigiCash que desarrollan y ponen en el mercado productos y servicios que permiten realizar transacciones seguras usando tarjetas de crédito, de débito, cheques, dinero electrónico y efectivo. En el momento en que deseemos realizar un pago, usaremos este tipo de servicios. Pronto podremos comprar y pagar servicios (como suscripciones y recibir un periódico en conexión o quizás incluso comprar un coche) sin separarnos de nuestra computadora personal.

La aparición del dinero electrónico crea nuevas necesidades a los consumidores; las cuales pueden ser utilizadas por las entidades bancarias (sucursales virtuales) para atraer nuevos clientes y ofrecer mayores posibilidades de atención.

A través de los sitios web de las entidades financieras es posible revisar saldos, realizar pagos de nóminas, tarjetas de crédito y de servicios públicos; hacer transferencias de fondos, abrir cuentas corrientes o de ahorros, solicitar préstamos, servicio de asesores virtuales, entre otros.

Sin embargo, a pesar de todos los servicios prestados la aceptación entre los clientes por la Web es aún baja debido a la falta de confianza a los sistemas electrónicos de seguridad y el temor a utilizar esta nueva tecnología, muchos de estos temores son infundados y la seguridad de las transacciones por medio de la Web es aceptable; ya que los bancos antes de liberar un producto tienen que cumplir con las disposiciones emitidas por la Superintendencia Bancaria y también es obligatorio efectuar pruebas de penetración al sistema y la evaluación de cada una de las escalas de seguridad; asimismo, existen ciertas medidas de seguridad que son implementadas en las transacciones bancarias, las cuales se listan y explican a continuación:

| Medidas | Descripción |
|---|---|
| **Firewall** | Es un filtro que evita el acceso no autorizado a la red de cada una de las instituciones financieras, y de las redes corporativas en general. |
| **Encriptación** | La conversión de información legible en ilegible. Los datos viajan de manera cifrada. |
| **Identificación** | Cada usuario posee un login (nombre de identificación) y una contraseña personal e intransferible. |
| **Autentificación** | La información es corroborada con la base de datos. Si corresponde a la del usuario se autoriza la transacción. |
| **Certificación** | La información confidencial que debe ingresar el usuario es certificada y cifrada. |
| **Antivirus** | Las plataformas deben poseer un software antivirus para la protección de los servidores y las estaciones de trabajo. |
| **Otros movimientos de Seguridad** | Movimientos entre cuentas previamente inscritas.<br>Bloqueos de claves después de 3 intentos fallidos.<br>Reconfirmación de la transacción realizada.<br>Registro de cada movimiento en bases de datos.<br>Emisión de un número de validación que el usuario puede imprimir y conservar como soporte de su transacción. |

Tabla 2.3 Medidas de seguridad en las transacciones financieras en Internet

- **Economía Cibernética:** El concepto "Economía Cibernética o de Internet" involucra a todas las compañías que generan toda o parte de sus ganancias directamente de la red mundial, o de productos y servicios relacionados con ella.

Según un estudio de la Universidad de Texas encargado por Cisco Systems, la economía de Internet ha crecido a niveles que alcanzan los 250 mil millones de dólares, al mismo tiempo, destaca el hecho de que la red es responsable de la generación de 3 millones de empleos.

El fenómeno de la red de redes sigue trascendiendo los límites de lo tecnológico y poco a poco se convierte en una comunidad que compra, vende, se comunica y se entretiene en Internet, y a pesar de no tener gobierno, crece en una proporción que sobrepasa los límites de lo imaginable y sorprende cada vez más a los analistas de mercados. Otro dato interesante es la creación de compañías, una de cada tres, del total de 5000 investigadas, no existía antes de 1996, nacieron gracias al potencial que ofrecía la red mundial de computadoras.

Gran parte del desempeño económico de los Estados Unidos en la década de los noventa se atribuye a la nueva economía generada o basada en el Internet, se estima que una buena parte del crecimiento per capita de Estados Unidos se debe al desarrollo de la economía digital. En este tránsito hacia la economía digital se benefician consumidores, empresarios e inversionistas. Para los consumidores, el acceso ilimitado y la absoluta transparencia en la información sobre el mercado y sus precios les permite acceder a una mejor oferta de bienes y servicios. Sin duda, el comercio electrónico presenta enormes oportunidades en el futuro para quienes lo aprovechen.

Pero para aprovechar las oportunidades y no quedar fuera de ellas se necesitan tecnología, velocidad e innovación. Toda transacción comercial en línea está protegida por una serie de procedimientos para impedir la manipulación de la información por parte de personas ajenas a la misma, para ello se han creado protocolos de seguridad, descritos a continuación en la tabla 2.4.

| Protocolo | Descripción |
|---|---|
| **SSL (*Secure Sockets Layer*, Capa de Conexión Segura)** | Diseñado por Netscape, (navegador creado por Netscape, es uno de los navegadores Internet más difundidos) es el protocolo de uso más generalizado en el mercado mundial, cifra o encripta la información suministrada por el comprador, brindando confidencialidad e integridad del mensaje y además posee sistemas para avalar la autenticidad del vendedor. |
| **SET (*Secure Electronic Transactions*, Transacción Electrónica Segura)** | Este protocolo también encripta o cifra la información necesaria, pero a diferencia del anterior requiere de una certificación digital de todas las personas o entidades que participan en la transacción (comprador, vendedor, banco, etcétera). Este protocolo es más seguro por tener mayores controles de identificación pero a su vez es menos práctico tanto a nivel técnico como operativo. |

Tabla 2.4 Protocolos de seguridad



TESIS CON
FALLA DE ORIGEN

- **Educación Virtual:** La educación "en línea" o en forma virtual ha generado diversidad de opiniones sobre las verdaderas posibilidades de Internet como medio educativo, sin embargo, la utilización de esta tecnología, permitirá a la enseñanza generar un cambio en los modelos educativos acordes a los tiempos modernos; por ejemplo un estudiante podría tomar cursos en los sitios que más le convenga y realizar de esta forma una carrera "a la carta", estando acorde con una nueva tendencia educativa.

  La utilización de Internet esta generando un espacio para que los docentes desplieguen toda su creatividad, pero hay que entender que ésta no es la única herramienta para modernizar la educación y que tampoco se debe convertir la tecnología en una mala imitación de la Pedagogía tradicional; en la cual se enseña por medio de libros, posteriormente se realiza un examen y se olvida de la parte de investigación, es decir, lo que ahora cuenta es la habilidad de aprender como aprender.

  Uno de los principales cuestionamientos en el sector educativo tiene que ver con la existencia de nuevas tecnologías (como realidad virtual, multimedia, inteligencia artificial, las comunicaciones e Internet, entre otras), cada vez más sofisticadas, que ponen a disposición de los estudiantes y profesores una gran cantidad de posibilidades para el aprendizaje.

- **E-Mail o Correo Electrónico:** Es un servicio muy popular y como su propio nombre indica se trata de un servicio de correo, pero en Internet, que nos permite comunicarnos con cierta rapidez y de una forma muy sencilla con otro usuario, siempre y cuando, éste disponga de otra dirección de e-mail.

  El usuario especifica el mensaje de texto junto con el nombre y/o dirección destino y lo envía a través del servidor de correo local que transmite el mensaje al servidor destino a través de una red de computadoras, el usuario destino recupera el mensaje a través de su servidor de correo, el e-mail no es un servicio en tiempo real, ya que tolera retardos, tampoco es un servicio orientado a conexión, ya que no necesita establecer una conexión de red para cada mensaje.

  Este servicio requiere de fiabilidad, a fin de tener una alta probabilidad de que el mensaje se reciba sin errores y en el sitio adecuado, el usuario puede solicitar una confirmación de la llegada del mensaje. Finalmente comentaremos que la seguridad y la privacidad pueden llegar a ser un problema de primeras magnitud.

  Una dirección de correo electrónico está compuesta de un **identificador de usuario** y de un **identificador de la computadora**, unidos por el carácter **@**.

  Ejemplo: nombre@compañía.com.mx

  En este caso nuestro servidor de correo sería compañía.

  Existen varios tipos de cuenta de acuerdo al grado de personalización, definidas en la siguiente tabla (Tabla 2.5).

TESIS CON
FALLA DE ORIGEN

| Tipo | Ejemplo de dirección de correo | Definición |
|---|---|---|
| **Gratuita** | oscar@hotmail.com | El servidor de correo permite personalizar la cuenta con el nombre del usuario (siempre que en este servidor no exista otro usuario con el mismo nombre, en cuyo caso debemos elegir otro), el grado de personalización es muy básico, este es un tipo de cuenta destinada a usuarios finales. |
| **Con Subdominio** | oscar@compañía.hotmail.com | En este caso el servidor además de nombre de usuario nos permite incluir un subdominio propio, aunque siempre aparezca vinculado al dominio del servidor. |
| **Con Dominio propio** | oscar@compañia.com | Al tratarse del dominio propio el grado de personalización es completo puesto que no se identifica con ningún servidor ajeno a la empresa. |

Tabla 2.5 Tipos de cuentas de correo electrónico

Los servidores se pueden identificar por uno o dos nombres, más el nombre de la organización (compañía) y el identificador del país, todos los países tiene su propio identificador, sin embargo existe una excepción, Estados Unidos no necesita colocar un identificador de país, a continuación describimos algunos:

| País | Identificador |
|---|---|
| México | .mx |
| España | .es |
| Reino Unido | .uk |
| Canadá | .ca |
| Alemania | .ge |
| Suiza | .ch |
| Francia | .fr |
| República Dominicana | .do |
| Argentina | .arg |
| Japón | .jp |

TESIS CON
FALLA DE ORIGEN

Existen otros identificadores que se utilizan para reconocer el tipo de las organizaciones y que se detalla a continuación:

| Organización | Identificador |
|---|---|
| De carácter comercial | .com |
| Que operan en las comunicaciones. | .net |
| Sin ánimo de lucro | .org |
| Gubernamental en México | .gob |
| Educativas | .edu |
| Centro militares | .mil |
| Gubernamentales en USA | .gov |
| Artistas | .art |

Existen varios programas que nos permiten gestionar nuestro correo electrónico, y sin duda alguna es el primer servicio que utilizan tanto particulares como cualquier organización cuando utilizan Internet, debido a que sustituye el correo tradicional, elimina muchas de las llamadas telefónicas, sobre todo las de larga distancia y nos permite utilizarlo como fax.

El mayor inconveniente de la utilización del correo electrónico es la falta de confidencialidad ya que un mensaje puede ser leído por personas que no nos interesa que tengan acceso al mismo. No obstante, en las últimas versiones de Windows tenemos nuevas opciones de accesibilidad pudiendo mandar la información con un sistema de encriptamiento o cifrado (Ver **Anexo 1. Criptografía**). Existe dentro de este servicio una aplicación muy útil llamada Lista de Distribución de Correo (*Mailing Lists*) estas son las direcciones electrónicas utilizadas para distribuir mensajes a un grupo de personas. Generalmente, una lista de distribución se utiliza para discutir acerca de un determinado tema. Una lista de distribución puede ser abierta o cerrada y puede tener o no un moderador. Si es abierta significa que cualquiera puede suscribirse a ella; si tiene un moderador los mensajes enviados a la lista por cualquier suscriptor pasan primero por aquel, que decidirá si distribuirlos o no a los demás suscriptores.

- **FTP** (*File Transfer Protocol,* Protocolo de Transferencia de Archivos), consiste en la transferencia de archivos de una computadora a otra en Internet, generalmente se utiliza para el intercambio de productos informáticos y programas.

  Las empresas de informática ponen cada vez más al alcance del usuario sus productos bajo este formato con el fin de que estos puedan bajarlos y de esta forma verlos sin necesidad de comprarlos, de esta manera los usuarios pueden verlos, probarlos y actualizar sus versiones, estos archivos se organizan en directorios y nos permiten trabajar con los directorios del servidor como si fueran propios.

  La mejor forma de localizar archivos en servidores FTP es utilizando un servicio de búsqueda, que nos permite localizar servidores FTP anónimos que constituyen uno de los principales medios de distribución de software e información en Internet, algunos de los archivos que podemos transferir son: sonido, texto, programas, video y datos.

  Existen también cuentas FTP con una clave para el usuario, estas por ejemplo pueden servir para: actualizar páginas web, facilitar el acceso de una manera sencilla y rápida a la red comercial de una empresa, catálogos, demos que por su formato no pueden ser enviadas por correo electrónico, facilita al usuario una clave de acceso FTP dando posibilidad una comunicación más ágil entre empresa y empleado.

- **Gopher**: Es un proyecto desarrollado por la Universidad de Minesota, básicamente es un servicio FTP con la ventaja de utilizar títulos descriptivos en el menú lo que confiere una mayor facilidad de manejo.

  Para obtener información situada en un servidor, se puede seleccionar un enlace cuya URL (*Uniform Resource Locator*, Localizador Uniforme de Recursos) se teclee en el campo de dirección de un navegador, los navegadores actuales permiten acceder a estos servidores de la misma manera en que se ingresa a las páginas web.

  A pesar de que las páginas Gopher tienen un formato muy básico, los listados del menú permiten mostrar páginas de contenido o sublistados de menú adicionales, sus menús aparecen en forma de listas de enlaces, cada uno de ellos precedido de un pequeño icono que indica el tipo de recurso que este representa, sus enlaces pueden llevar a: menús, archivos de texto, imágenes, índices, archivos de películas y binarios.

- **Grupos de Noticias** (*News*), se le aplica este término al sistema de listas de correo que mantiene la red Usenet. Los grupos de noticias envían información acerca de un tema específico, previamente solicitado por el usuario de Internet, donde a la vez otros usuarios interesados en el mismo tipo de noticias exponen sus opiniones y puntos de vista acerca de las mismas.

  Actualmente hay servidores gratuitos que interconectan a usuarios interesados en un mismo tema mediante e-mail, este servicio se puede comparar a un sitio de anuncios específicos para cada tema de discusión, donde todos y cada uno de los usuarios tienen acceso a las noticias relacionadas con este tema, así como a las opiniones de todos los demás usuarios.

  Es muy importante para acceder a este tipo de servicios guardar ciertas normas de educación en la Red, a estas normas se las denomina Netiquette (Ver **Anexo 3. Netiquette**), puesto que las News son un espacio libre para expresar opiniones personales acerca de diferentes temas.

  Recordemos que Internet actúa como un lenguaje, y para expresarnos en la Red debemos conocer la forma correcta de hacerlo.

- **HTML**:(*Hipertext Markup Lenguaje,* Lenguaje de Marcado de Hipertexto), los documentos de web son creados empleando un lenguaje llamado HTML, el cual consta de códigos, llamados marcas o etiquetas que sirven para formatear los elementos gráficos y los enlaces, al seleccionar un enlace se abrirán en el navegador documentos situados en un servidor, los documentos pueden contener texto, imágenes, sonidos, películas, o una combinación de estos elementos.

- **Hipermedia**: Son medios de enlace a otros medios a través de texto, imágenes y videos que están vinculados a otros sitios (hipertexto, hiperimágenes e hipervideos, respectivamente).

- **Internet Phone:** Es un servicio de comunicación entre dos usuarios conectados a Internet con el cual, pueden hablarse y escucharse; es necesario tener instalado un equipo multimedia en la computadora (tarjeta de sonido, micrófono y bocinas).

- **Internet Voice Mail** (Correo de voz): Es un correo electrónico en el cual el destinatario oye el mensaje en lugar de leerlo, este servicio no es interactivo, es una aplicación que puede tenerse dentro del propio correo electrónico.

- **IRC** (*Internet Relay Chat*, Difusión de Comunicación por Internet), los servidores de IRC están estructurados en redes que agrupan a los participantes de cada chat en diferentes canales, siendo cada canal una conversación sobre un tema específico o en un idioma determinado.

- **Oficina Virtual:** El uso masivo de la red mundial de computadoras ha impulsado a varias instituciones y sus redes de servicios a mirar hacia afuera, y no limitar sus ventajas a los usuarios internos.

  Después de comprobar y aprovechar las bondades de este servicio, la mayoría de universidades y empresas grandes o pequeñas, ofrecen ahora a sus estudiantes, empleados o clientes acceso a sus redes, y por supuesto a sus bancos de información (listados de existencias, clientes, itinerarios de vuelos, horarios y disponibilidad de clases).

  Así, desde la oficina virtual, en casa o algún lugar del mundo, desde una red externa o incluso en una ubicación diferente de la misma organización, los usuarios acceden a servicios e información dentro de las redes de la empresa o universidad.

- **Realidad Virtual:** Concepto con el que se conoce a una serie de tecnologías que pretenden reproducir la realidad mediante la utilización de computadoras y dispositivos externos, generalmente, una computadora genera una imagen falsa que el usuario contempla a través de un casco equipado con un visor especial, de manera que tiene la impresión de estar presente en la escena reproducida por la computadora.

  En su grado más alto de sofisticación, los equipos de realidad virtual se completan con guantes y trajes equipados con sensores, que permiten "percibir" los "estímulos" y "sensaciones" generadas por la computadora, en definitiva, el usuario percibe como real algo que no lo es.

  Esta tecnología se ha aplicado más al mundo de los videojuegos, existen ya aplicaciones en medicina, que han permitido importantes avances en la simulación de intervenciones quirúrgicas.

  La proliferación de "mundos" de realidad virtual (o tridimensionales) que se pueden visitar y explorar usando cascos y visores especiales, ya está en marcha, usan algo llamado VRML (*Reality Virtual Model Language*, Lenguaje de Modelado de Realidad Virtual), un tipo de tecnología completamente novedoso y excitante diseñada en tercera dimensión (3D).

- **Talk** (conversación, charla) Protocolo que permite a dos personas conectadas a computadoras situadas en dos lugares distintos comunicarse por escrito entre sí en tiempo real. Es una conversación interactiva usando el teclado.

- **Telnet** (Conexión Remota Interactiva): La Red nos ofrece la posibilidad de utilizar, mediante nuestro acceso, otras computadoras situadas en cualquier parte del mundo, al igual que el FTP necesitamos el software necesario y un protocolo específico para este servicio llamado Telnet.

  Para el uso de este servicio, se utiliza la URL: Telnet <dirección IP>.

Mediante este sistema podemos utilizar otra computadora de una manera remota, como si este estuviera en nuestra propia mesa, los requisitos para acceder a este servicio son muy sencillos, saber el nombre y/o la dirección del servidor remoto y estar habilitado para poder utilizarlo mediante un identificador de usuario (*Userid*) y un password o clave de acceso.

- **URL** (*Uniform Resource Locator,* Localizador Uniforme de Recursos): Es un sistema unificado de identificación de recursos de la red, las direcciones están compuestas de un protocolo y dirección local del documento dentro del servidor, estas direcciones permiten que se identifique a objetos como FTP, WWW y Gopher.

- **Video bajo demanda**: Es un servicio interactivo y su objetivo es proporcionar acceso a una biblioteca de videos, es decir una especie de videoclub situado en algún lugar remoto junto con algunos procedimientos de control, reproducción, grabación, avance cuadro x cuadro, retroceso, congelación de imagen y pausa.

  El usuario entra al servicio a través de un menú de selección, donde hace el pago del servicio y es entonces cuando se empieza a transmitir el video a través de la red hasta el usuario, esta aplicación no es tiempo real ya que tolera retrasos, la cuestión relacionada con la seguridad y la privacidad afectan principalmente a la fase inicial en la que se realiza la selección y el pago.

- **Videoconferencias**: Es un servicio que integra al mismo tiempo imagen y sonido, es Internet phone más la imagen de los dos participantes en la conferencia, se necesita, además del kit básico multimedia, una tarjeta de captura de video así como una cámara digital.

- **WAIS** (*Wide Area Information Server,* Servidores de Información de Área Amplia): Básicamente es un buscador, añadiendo una ventaja fundamental, busca por palabras, no por títulos como un buscador normal con lo cual permite encontrar documentos en los que se trata de un tema determinado sin necesidad de que este aparezca como título de la URL localizada, es un servicio de información distribuida que permite hacer preguntas en lenguaje simple.

## 4. TENDENCIAS DE INTERNET

Cada vez son menos los escépticos que pensaban que Internet sería una moda pasajera, es suficiente echar un vistazo a nuestro alrededor y comprobar como las noticias de Internet en los periódicos, la radio, la televisión, son cada vez más extensas, todo el mundo habla de Internet, y cabe preguntarse ¿nos encontramos realmente ante las puertas de una revolución mundial?.

Internet ha cambiado desde su existencia, no se puede decir que Internet ha acabado su proceso evolutivo, está cambiando para proveer nuevos servicios como, audio y video, esta evolución nos traerá nuevas aplicaciones, telefonía Internet y, televisión por Internet, está cambiando hacia una nueva generación de tecnologías de red con distintas características y requisitos: desde ancho de banda doméstico hasta satelital y, por último esta buscando nuevos modos de acceso y nuevas formas de servicio que darán lugar a nuevas aplicaciones, que, a su vez, harán evolucionar a la propia red.

La cuestión más importante sobre el futuro de Internet no es como cambiará la tecnología, sino como se controlará esa evolución. Será difícil encontrar la forma de esta estructura dado el gran número de intereses que concurren en la red.

Las redes de banda ancha que se están creando, así como el espectacular desarrollo de la telefonía móvil (actualmente en tercera generación) permitirán aplicaciones como telemedicina, videoconferencia de alta calidad y todo tipo de servicios en cualquier parte del mundo gracias a la telefonía sin hilos.

El fruto de la tecnología móvil en Internet es el desarrollo de páginas WML (*Wireless Markup Language,* Lenguaje de Creación Inalámbrica), permite la visualización de páginas web en dispositivos inalámbricos que incluyan la tecnología WAP (*Wireless Application Protocol,* Protocolo de Aplicaciones Inalámbricas), es un estándar que define la forma de acceso a datos a través del teléfono móvil.

La prueba definitiva de que Internet es el futuro, lo veremos reflejado en algunas de las tendencias que mencionaremos a continuación: Internet2, Economía Cibernética, Educación Virtual, JINI, Lenguaje XML, Periódicos en Internet, Sucursales Bancarias y WIS (*Web Information System*, Sistema de Información Web).

### 4.1 Internet 2

La Red Internet 2 (I2) espera ser 100 veces más rápida que la Internet actual y es desarrollada por un consorcio conformado por unas 300 universidades y unas 100 empresas, entre las que se encuentran Qwest Technologies, Cisco Systems, Nortel Networks, 3Com, AT&T, IBM, Microsoft, Sprint, MCI; y muchos organismos estatales.

Internet 2 está reservada para aplicaciones que requieren de una transmisión de datos casi instantánea, como por ejemplo: telemedicina, capacitación a distancia, manipulación simultánea de modelos computacionales, visualizaciones en tiempo real de cálculos efectuados en supercomputadoras remotas, video bidireccional, teleconferencias, y procesamiento de imágenes satelitales.

Esto significa, que usuarios ubicados en diferentes lugares del mundo, podrán ver las imágenes de video en alta definición de un telescopio y observar todos simultáneamente el cosmos en tiempo real. Pero seguramente esto sería poco si tenemos en cuenta que con esta tecnología se pueden crear laboratorios virtuales, desarrollar experimentos, compartir recursos científicos y médicos, como fotografías de células, tomografías, radiografías, todo en cuestión de segundos.

Internet 2 trabajará con una versión diferente del Internet IPv6 (*Internet Protocol versión 6,* Protocolo de Internet versión 6), actualmente el que estamos usando en la web es el IPv4(*Internet Protocol versión 4*, Protocolo de Internet versión 4). La nueva versión, lanzada en mayo del 2000, es más flexible, manejará anchos de banda más grandes, e incrementará su confiabilidad y su seguridad.

Quienes usen una Palm se verán grandemente beneficiados, ya que la nueva versión 6 estará orientada al mercado de Internet móvil. Al diseñar el protocolo IPv6 se tuvo en cuenta la posibilidad de poder asignar direcciones a todos los habitantes del mundo y de ofrecer múltiples servicios a cada uno de los usuarios de la red teniendo una proyección estimada al año 2020.

Los principales objetivos de Internet 2 son:

- La creación y el sostenimiento de una red con tecnología de liderazgo con la capacidad de cubrir las necesidades de la comunidad de investigación.
- Dirigir los esfuerzos del desarrollo de la red para permitir la creación de una nueva generación de aplicaciones que exploten al máximo las capacidades de las redes de gran ancho de banda.
- Trabajar para transferir rápidamente los nuevos servicios de red y aplicaciones a todos los niveles de educación y a la comunidad de Internet en general.

**Internet 2 en México**

En México, Internet 2 es un proyecto nacional iniciado en abril de 1999, se firma oficialmente con la creación de la Corporación Universitaria para el Desarrollo de Internet (CUDI), que enlaza universidades y centros educativos y tecnológicos.

En esta corporación se planean, diseñan los mecanismos que regirán a la Internet 2 mexicana, de acuerdo a las necesidades y situación económica del país. Actualmente, CUDI cuenta con una red ATM de alta velocidad operando a los 155 Mbps, conectando las principales ciudades de México, Monterrey, Tijuana, Guadalajara y el DF.

**Ventajas que ofrece Internet 2**

- **Gran ancho de banda.** Una de las características fundamentales de Internet 2 es el manejo de un gran ancho de banda. En la actualidad, dependiendo de los recursos disponibles, se tienen velocidades del orden de los cientos de megabits por segundo, pero la tendencia es alcanzar rangos de gigabits por segundo según la demanda.

- **Calidad de los servicios** (*Quality of Service*). En la Internet, todos los paquetes de información tienen la misma prioridad, de tal forma que si se envía video por la red, a la vez que se transfiere un archivo de datos, ambas operaciones compiten por el mismo canal, por lo que probablemente los cuadros de video no lleguen a su destino en forma continua, es decir, se tendrá un congelamiento o al menos un deterioro en la calidad de la imagen. En cambio, en Internet 2, se puede dar prioridad al video, de tal forma que se garantice que todos los cuadros lleguen a tiempo y, sólo en los espacios que el video deje libre, se irán transmitiendo los paquetes del archivo de datos. Esta característica permite también mantener en un nivel adecuado el retardo de la información. Siendo importante sobre todo para sistemas de control de dispositivos a distancia.

- **Transmisión multipunto** (*Multicast*). Otra solución que ofrece Internet 2 es que en Internet normal, cuando se desea transmitir información a un conjunto de usuarios (por ejemplo: en la transmisión de un evento en vivo), se envían los mismos paquetes de la señal de video a cada uno de los usuarios, multiplicando el tráfico en la red; en Internet 2 se está experimentando una tecnología conocida como multicasting, mediante la cual se envía, una sola vez, cada paquete con la información necesaria para que llegue a todos los usuarios que deben recibirlo.

- **Retardo reducido y uniforme** (*Low Latency/Low Jitter*). En aplicaciones sensibles al retardo de la información, es vital reducirlo al mínimo posible. En Internet 2, con la combinación de un gran ancho de banda, la priorización de los servicios y técnicas avanzadas de enrutamiento se logran retardos realmente muy pequeños en el orden de los milisegundos extremo a extremo. Esto permite desarrollar sistemas de control a distancia de equipos muy sofisticados, en los cuales el retardo de la información de control podría resultar fatal.

- **Mayor seguridad, privacidad y confiabilidad**. Otro aspecto importante que se está experimentando en Internet 2 consiste en la mejora de la seguridad y privacía de la red, utilizando protocolos que permitan autenticar plenamente el origen de los datos y que asegure la integridad y confidencialidad de los mismos.

De esta forma, en México se están realizando esfuerzos por proveer este tipo de servicios a instituciones educativas, impulsando la investigación, participación y el intercambio de conocimiento entre las distintas universidades del país y el mundo. La figura 2.2 muestra un modelo general para Internet 2.

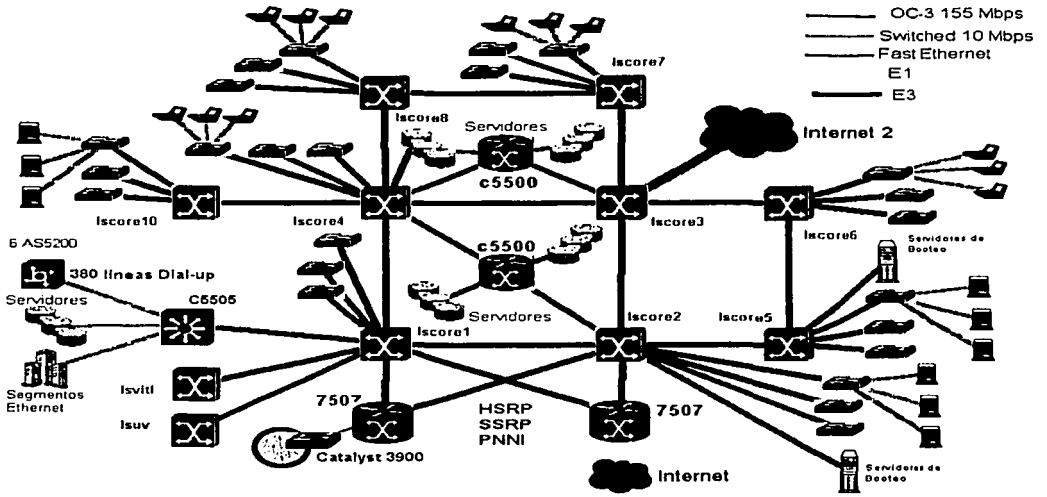


Fig. 2.2 Modelo de Internet 2

### 4.2 Economía Cibernética

El desarrollo de la actividad económica basada en Internet ha sobrepasado todas las expectativas, tal como lo reporta el Departamento de Comercio de los Estados Unidos en su documento *The emerging digital economy II* (La economía digital emergente II), los cálculos iniciales se quedaron muy cortos. En efecto, al comienzo de 1998 se estimaba que para el año 2000 las transacciones por Internet alcanzarían los 7000 millones de dólares en Estados Unidos. Sin embargo, al finalizar 1998 ya se había excedido de esta cifra.



TESIS CON
FALLA DE ORIGEN

En las transacciones de negocio a negocio, se anticipó que para el año 2002 el tamaño sería de 300 000 millones de dólares en Estados Unidos, ahora, Forrester Research estima que en el año 2003 ascenderán a 1.3 billones de dólares.

Es impresionante el movimiento hacia Internet de los negocios, que está acompañado de un crecimiento igualmente importante en la cantidad de usuarios de la red mundial. Se calcula que el número de usuarios de Internet en el mundo hoy día es de 513 millones y que para el año 2005, se espera que este número de usuarios llegue a los mil millones.

### 4.3 Educación Virtual

Actualmente se estima que un 55% de las escuelas y universidades norteamericanas tienen programas de educación virtual, además, que hay aproximadamente 1 millón de estudiantes en programas virtuales y 13 millones en programas tradicionales. El Gartner Group estima que en el año 2002 más del 80% de las escuelas y universidades de Estados Unidos estarán usando metodologías y tecnologías de educación a distancia en por lo menos un programa académico tradicional.

### 4.4 JINI (*Java Intelligent Network Infrastructure*, Infraestructura Inteligente de Red Java)

Es un sistema de programación distribuida, totalmente basado en Java, cuyo objetivo es unificar hardware y software para que dentro de una red sean vistos como un solo elemento.

Entre muchos usos, abre la posibilidad de crear viviendas inteligentes donde todos los dispositivos, desde una cafetera hasta un televisor, estén conectados a un servidor, el cual a su vez se halle conectado a Internet. Así, los residentes podrían controlar o programar cualquier artefacto de su casa de manera remota.

Pero Jini va mucho más allá y quiere abarcar los nuevos dispositivos que permiten conectarse a la Web o a una extranet de forma inalámbrica, lo que está transformando las telecomunicaciones y los negocios electrónicos.

### 4.5 Lenguaje XML (*Extensible Markup Language*, Lenguaje de Marcado Extendido)

Un estándar de desarrollo que amplía las posibilidades y mejora las características para la creación de servicios y aplicaciones de Internet.

El uso de esta herramienta permitirá a los usuarios personalizar su experiencia en línea e incrementar los niveles de seguridad y productividad de sus sistemas.

El esquema XML será la piedra angular en la nueva arquitectura del comercio electrónico que actualmente se está construyendo para llevar a cabo el intercambio de documentos entre diferentes plataformas IT; aún si son incompatibles. Consta de las siguientes partes:

- La primer parte describe un lenguaje utilizado para describir la estructura de alto nivel de un documento XML.
- La segunda parte describe la lista de tipos de datos permitidos por el lenguaje XML.

Mediante el uso del esquema XML se podrá detectar si los archivos recibidos tienen información faltante, información con formatos incorrectos (por ejemplo las fechas con dos dígitos para representar los años, o campos numéricos con caracteres alfanuméricos) o información errónea.

El rango de características es muy completo e incluye una gran selección de tipos básicos de información; tales como enteros, números de punto flotante, códigos, horas y fechas; también incluye formas de limitar valores según los rangos de información válida o según listas de valores válidos.

### 4.6 Periódicos en Internet

Durante la reunión de la Asociación Mundial de Periódicos, realizada en junio del 2000, quedó claro que los diarios electrónicos no deben ser un valor agregado sino empresas independientes. Poco a poco, las versiones electrónicas de los periódicos tradicionales están dejando de ser tan solo una parte del negocio de la información y han comenzado a competir como un medio más.

### 4.7 Sucursales Bancarias en Internet

El futuro de las sucursales bancarias virtuales parece asegurado: Un estudio de la empresa de análisis de mercados Jupiter Communications dice que 18.1 millones de hogares de Estados Unidos usarán frecuentemente estos servicios, para el año 2002. Estas proyecciones y las significativas ventajas de sus servicios han servido para impulsar una nueva clase de negocios: bancos de Internet, entidades que sin necesidad de infraestructura física, cumplen a la perfección con todos los servicios de sus homólogos reales.

### 4.8 WIS (*Web Information System,* Sistema de Información de la Web)

Los nuevos sistemas de información de las organizaciones denominados WIS, operan en múltiples sitios geográficos interconectados entre sí por Internet o Intranet. La información y los servicios de procesamiento están repartidos en dichos sitios, y deben cooperar entre sí para responder a las necesidades de los usuarios externos e internos.

Existe gran variedad de esquemas y herramientas para desarrollar aplicaciones en Internet o Intranet, dando lugar a diferentes arquitecturas de sistemas WIS. Es difícil comparar y seleccionar la mejor arquitectura que nos garantice la construcción de sistemas WIS robustos, escalables, seguros, eficientes e interoperables debido a la constante evolución de los esquemas y herramientas existentes.

Sin embargo, se pueden enunciar algunas pautas a seguir cuando se quieran elegir herramientas de desarrollo de sistemas WIS (intranets o extranets):

- La programación con CGI's (Protocolo o interfaz de intercambio de información que se realiza entre el navegador y un servidor WWW), que accedan bases de datos es sencilla y en general suficiente para los sistemas intranets que tienen como finalidad la publicación de información al interior de una organización y/o la conformación de una comunidad virtual de los empleados. Sin embargo, es un esquema de muy bajo rendimiento que es inadecuado para desarrollar aplicaciones intranets de misión crítica.

- La programación de scripts mezclados con hojas HTML permite desarrollar sistemas intranets con mejor rendimiento que el que ofrecen los CGI's. Sin embargo, para su operación se requiere contar con navegadores o servidores Web específicos y su mantenimiento puede resultar difícil. Por esta razón este esquema de programación, al igual que los CGI's, puede utilizarse para desarrollar sistemas intranets de publicación o de comunidad virtual pero resulta inadecuado para los sistemas de misión crítica.

Las plataformas Java y CORBA (especificación de mensajes basada en objetos desarrollado por *Object Management Group*) permiten desarrollar sistemas intranets que integren aplicaciones de misión crítica de la organización, o sistemas extranets que vinculen a la organización con sus proveedores y sus clientes. En una mayor o menor medida estas tres plataformas (y sobre toda su combinación) permiten construir sistemas WIS robustos, escalables, seguros, eficientes e interoperables.

### 4.9 Crecimiento

Para el año 2001, el mercado global de comercio electrónico alcanzó 1.2 billones de dólares. Para el año 2003, las ventas a través de la red serán de 8000 millones de dólares.

En el 2003 habrá 26.3 millones de usuarios de Internet en América Latina. En el año 2005, 700 millones, del total de mil millones de usuarios de Internet, estará fuera de Estados Unidos.

### 4.10 El Tamaño de Internet

Se ha determinado que 1.5 millones de páginas Web nacen cada día.

El Web duplica su tamaño cada 8 meses.

Existen, aproximadamente 70 millones de páginas Web.

El 90 % de todo el tráfico del Internet circula por 350,000 servidores distintos.

El 50% de todo el tráfico de Internet circula solo en 900 páginas Web, las más importantes están disponibles actualmente.

Para comparar el alcance que tiene Internet, se presenta a continuación una tabla comparativa (Tabla 2.6) del número de usuarios con los que cuenta, sabiendo que la tendencia es un crecimiento a nivel global.

| Región | Número de usuarios |
|---|---|
| Todo el Mundo | 513.43 millones |
| África | 4.15 millones |
| Asia y Pacifico | 143.99 millones |
| Europa | 154.63 millones |
| Medio Este | 4.65 millones |
| Canadá y EE.UU. | 180.68 millones |
| América Latina | 25.33 millones |

Tabla 2.6 Número de personas que actualmente utilizan Internet



TESIS CON
FALLA DE ORIGEN

# 5. VULNERABILIDADES EN INTERNET

Las vulnerabilidades asociadas con Internet ponen en peligro a los gobiernos, fuerzas armadas, comercios y usuarios individuales, Internet es un mundo complejo y dinámico de redes conectadas entre sí, que carecen de límites claros y control central.

Debido a que originalmente no fue organizada tomando en cuenta la seguridad, es difícil asegurar la integridad, disponibilidad y privacidad de la información. Sin embargo, es importante establecer medidas de control ya que Internet ha reemplazado a otras formas de comunicación electrónica, creciendo a una tasa asombrosa.

En consecuencia con el crecimiento de Internet, las herramientas de los intrusos se vuelven cada vez más refinadas y también son más fáciles de usar y están ampliamente disponibles. Sin embargo, es posible tomar medidas para reducir el riesgo de que haya violaciones de seguridad a las empresas que tratan de establecer una posición en el mercado electrónico.

Las vulnerabilidades que existen en Internet son muchas y muy variadas, de forma general pueden ser englobadas en tres grandes grupos: Correo Electrónico, Internas y Virus.

## 5.1 Vulnerabilidad del Correo Electrónico

Las vulnerabilidades del correo electrónico se exponen cuando se utiliza este servicio que ofrece Internet, a través de ellas, la seguridad se ve sobrepasada ya que este medio es muy importante y bastante usado para poder comunicarnos, enviarnos mensajes, adjuntar archivos, enviar direcciones de correo, recibir ligas de páginas de Internet, etcétera.

Al recibir en nuestro equipo todo este tipo de beneficios también recibimos y abrimos canales para que nuestra seguridad sea violada a través de la vulnerabilidad del correo electrónico, mencionaremos algunas de ellas:

### 5.1.1 Archivos adjuntos con contenido malicioso

Esta vulnerabilidad se da a través de los archivos adjuntos de correo y el inicio de esto es debido a la confianza que nosotros depositamos en amigos y conocidos quienes nos envían correos, nosotros no sabemos si el correo fue enviado o si se auto envío después de haber tomado la libreta de direcciones de la víctima. Este tipo de archivos adjunto utiliza nombres atractivos e inclusive cambia el nombre de las extensiones para ser ejecutados por los usuarios.

A menudo se intenta penetrar las redes enviando un archivo adjunto que parece una película Flash, la que mientras visualiza una animación atractiva, ejecuta comandos en segundo plano que roban las contraseñas y dan a quienes enviaron el correo el acceso a la red.

Este método permite ocultar la actual extensión del archivo, es decir, ocultan el hecho de que el archivo inofensivo es realmente un peligroso archivo. Los archivos adjuntos en correos todavía son, probablemente, el número uno de las amenazas.

### 5.1.2 Por recibir correo con formato HTML

Se trata de código insertado en los e-mails con formato HTML, que se encarga de descargar, diminutas imágenes invisibles de un pixel (unidad más pequeña que puede conformar una imagen), también puede implementarse a través de algún pequeño código en JavaScript, esta información puede ser rastreada, de modo que las compañías que las insertan puedan ser informadas de la frecuencia con la que se leen sus anuncios. Además, un mensaje con formato HTML es capaz de ejecutar nuestro browser, y de ese modo el remitente puede colocar en nuestra PC los clásicos cookies (o galletas), que como resultado permitirán al remitente recoger cierta información, como la dirección IP que tenemos en ese momento, el tipo de navegador que usamos, y los sitios Web que visitamos.

### 5.1.3 Mal manejo de las cabeceras MIME (*Multipurpose Internet Mail Extensions*)

Esta vulnerabilidad puede ser explotada por un usuario con malas intenciones que envía un correo electrónico de HTML preparado con un ejecutable o descarga, y un usuario abre el correo electrónico o visita el sitio Web, entonces Internet Explorer ejecutará el archivo automáticamente en el equipo del usuario. Si esto ocurre, el ejecutable puede realizar alguna acción, como añadir, cambiar, o borrar datos, comunicarse con sitios Web, o formatear el disco duro.

## 5.2 Vulnerabilidades Internas

Este tipo de vulnerabilidad no es notado por el usuario, simplemente se ejecuta en segundo plano o cuando bajamos alguna aplicación de Internet.

### 5.2.1 Al bajar Música

Cuando bajamos música y tenemos instalado Windows Media Player y Movie Maker, se abre un camino para el ingreso de virus, cuando se ingresa a un sitio, y automáticamente se escucha un tema musical asociado, podría estar ejecutándose un virus en el sistema. Los archivos que lo hacen posible son conocidos como .ASX (*Active Stream Redirector*), que son accesos directos de audio o video del Media Player. Los archivos .ASX puedan llegar a ejecutar algún código oculto. Y este código puede instalar y ejecutar cualquier otro programa, por ejemplo un virus o un troyano. Inclusive se puede usar para enviar correo, o para acceder a otras computadoras conectadas en red. Nada impide que alguien pueda usarlo para enviarle un troyano, mientras se escucha un tema musical, tal vez un virus acaba de instalarse en el sistema.

### 5.2.2 Falsificación de zonas seguras

La falsificación de zonas de seguridad, se realiza mediante una página construida con etiquetas HTML o códigos Scripts especiales, que pueden hacer que el navegador cargue páginas WEB en el contexto de seguridad de Intranet o de sitios de confianza o en un segundo plano desactivar la configuración de seguridad de nuestro equipo.

### 5.2.3 Vulnerabilidad en las Cookies (Galletas)

Esta vulnerabilidad permite a un sitio malicioso acceder a cualquier cookie en la memoria del navegador o guardada en el disco. Las cookies, son utilizadas por diferentes sitios Web para guardar preferencias del usuario, llevar estadísticas, nombres de usuario y contraseñas. Son consideradas inocentes, puesto que sólo guardan texto y no ejecutan ningún tipo de código que pusiera en peligro la seguridad de nuestra computadora.

Son muy usadas en sitios de transacciones comerciales (desde carritos de compras a movimientos bancarios), para la autentificación del usuario. Sin embargo, esta vulnerabilidad, pone en peligro nuestra seguridad, ya que a partir de esta falla, un sitio cualquiera puede leer las cookies de otro sitio, adquiriendo así contraseñas e información confidencial.

### 5.2.4 Vulnerabilidad en Frames

En esta vulnerabilidad el atacante puede construir una web con distintos frames para leer información de otros sitios y podría leer los archivos del sistema de la víctima. La vulnerabilidad permite que desde un frame se puedan leer los datos contenidos en un segundo frame correspondiente a otro sitio o dominio. El ataque podría ser llevado a cabo desde una página web o un e-mail con formato HTML.

## 5.3 Vulnerabilidad a través de los Virus.

Esta vulnerabilidad es la más conocida por los usuarios ya que lo primero en que pensamos cuando tenemos un problema en nuestra computadora, es que un virus lo está causando, la gran propagación de los virus a través del correo electrónico, se debe a que es muy fácil engañar a la persona que lo recibe, haciéndole pensar que lo envía un conocido.

Estadísticamente, este hecho es el que más resultado le ha dado a los virus que emplean el correo electrónico para propagarse.

Los tipos de virus que pueden llegar a través de Internet, son:

### 5.3.1 Hoaxes (mistificación, broma o engaño)

Son mensajes con falsas advertencias de virus, o de cualquier otro tipo de alerta o de cadena (incluso solidaria, o que involucra a nuestra propia salud), o de algún tipo de denuncia, distribuida por correo electrónico. Su común denominador, es pedirle los distribuya "a la mayor cantidad posible de conocidos", jamás reenvíe un mensaje de este tipo que llegue a su correo.

Estas clases de alarma, suelen ser TOTALMENTE FALSAS, o basadas en hechos erróneos, pero lo que es peor activan un tipo de "contaminación" muy diferente, propagar cientos y hasta miles de mensajes de advertencia sobre los mismos. Y aún en el caso de denuncias basadas en hecho reales, esta forma de hacerlo desvirtúa totalmente su verdadero objetivo, que significa bromas o engaños los cuales hacen referencia a un programa rastreador de mensajes.

### 5.3.2 Gusanos

Uno de sus medios de transmisión es a través de correo electrónico (el mensaje de correo tiene un formato especial), como un archivo adjunto o incluido en el mensaje de correo. El gusano aprovecha algunas de las vulnerabilidades cuando un usuario se conecte a una página modificada por el gusano, resultará automáticamente infectado, cuando el mensaje llegue al usuario y éste lo abra o lo muestra en la vista previa, el cliente de correo (Outlook u Outlook Express) ejecuta automáticamente el archivo anexado y se produce la infección.

Además se envía a través de correo electrónico conectándose directamente a Internet a través de comandos SMTP. Para conseguir las direcciones e-mail de sus víctimas, hace login al sistema de correo a través de Simple MAPI y recorre mensajes en busca de direcciones de correo en su interior.

### 5.3.3 Caballos de Troya

Este tipo de virus les permite a los intrusos después de haberlo instalado en nuestra computadora, acceder a ella. Esto lo logran después de haber explotado un canal de vulnerabilidad libre en nuestra red o nuestro equipo, y posteriormente ellos logran entrar fácilmente y romper toda seguridad.

Así es posible concluir, que Internet se ha convertido en una herramienta cotidiana y a la que fácilmente se puede tener acceso, su uso se ha extendido a personas de todas las edades, culturas, niveles educacionales y creencias, Internet 2 revolucionará aún más, el uso de esta herramienta. Sin embargo, no hay que olvidar que Internet presenta vulnerabilidades que amenazan la seguridad e integridad por lo que se deben tomar medidas de prevención, detección o en el peor de los casos corrección para que las pérdidas sean controladas.

# CAPÍTULO 3
# REDES Y SISTEMAS OPERATIVOS SEGUROS

La seguridad de los equipos debe ser algo a considerar en cualquier red. Diariamente por cualquiera de ellas circulan todo tipo de datos, muchos que se podrían catalogar como *confidenciales* (nóminas, expedientes, presupuestos, etcétera) o al menos como *privados* (correo electrónico, proyectos de investigación, artículos a punto de ser publicados, etcétera). Independientemente de la etiqueta de los datos, parece claro que una falla en la seguridad de un equipo o de la propia red no beneficia a nadie, y mucho menos a la imagen de una organización. Y ya no se trata simplemente de una cuestión de imagen: según el Instituto de Seguridad de Computadoras *(Computer Security Institute)*, a raíz de un estudio de más de 250 empresas norteamericanas, en el que se ponía de manifiesto el costo que supone carecer de infraestructuras de seguridad en la empresa y en el que se ha hecho notar que la falta de medidas de seguridad en la Red ha hecho perder en el 2002, 455 millones de dólares a las empresas consultadas, cifra muy superior a los 265 millones que según el estudio se perdieron en el año 2000, cifra que cada año se incrementa en más del 35%; los delitos informáticos en general aumentan también de forma espectacular año tras año, alcanzando incluso cuotas del 800%.

A lo largo de este capítulo se intentará hacer un repaso de los puntos habituales referentes a seguridad en redes de computadoras (problemas, ataques, defensas, etcétera); de esta forma se ofrecerá una perspectiva general de la seguridad en entornos de red, el funcionamiento de sus mecanismos, y su correcta utilización. También se hablará, en menor medida, sobre temas menos técnicos pero que también afectan directamente a la seguridad informática, como puedan ser el problema del personal o la legislación vigente.

El objetivo final de este proyecto es marcar pautas para conseguir un nivel de seguridad aceptable en los sistemas conectados en cualquier red, entendiendo por "aceptable" un nivel de protección suficiente para que la mayoría de intrusos y situaciones que amenazan potencialmente a los sistemas de cómputo fracasen ante un ataque.

## 1. AMENAZAS A LA SEGURIDAD

Se puede entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica es muy difícil de conseguir, hablando particularmente de sistemas operativos o redes de computadoras, se suaviza la definición de seguridad y se procede a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él).

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: **confidencialidad, integridad y disponibilidad.**

- La **confidencialidad** nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.



TESIS CON
FALLA DE ORIGEN

- La **integridad** significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada.

- La **disponibilidad** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

Y generalmente tienen que existir los tres aspectos descritos para que haya seguridad, es decir, un sistema puede conseguir confidencialidad para un determinado archivo haciendo que ningún usuario pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Los tres elementos principales a proteger en cualquier sistema informático son el **software**, el **hardware** y los **datos.**

**Hardware** es el conjunto formado por todos los elementos físicos de un sistema informático, como CPU (*Control Process Unit,* Unidad de Procesamiento Central), terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes, etcétera) o tarjetas de red.

El **software** es el conjunto de programas lógicos que hacen que el hardware sea funcional, en él se engloban tanto sistemas operativos como aplicaciones.

Los **datos** son el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o información de una base de datos.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar. Sin embargo, cualquiera de los tres elementos descritos está expuesto a diferentes amenazas. Se entiende por amenaza una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjera una violación de la seguridad.

Existen cuatro formas de amenazas a la seguridad en un sistema de cómputo: **interrupción, intercepción, modificación y falsificación.**

**Interrupción.** Un objeto del sistema se pierde, se hace inutilizable o inaccesible (Fig. 3.1). Por ejemplo, la destrucción maliciosa de un dispositivo de hardware, el borrado de un programa o base de datos, o la falla del administrador de archivos del Sistema Operativo.

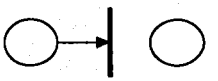

Fig. 3.1 Interrupción

TESIS CON
FALLA DE ORIGEN

**Intercepción.** Implica que una parte no autorizada consigue acceder a un determinado objeto del sistema (Fig. 3.2). La parte no autorizada puede ser una persona, un programa u otra computadora. Por ejemplo, la copia ilícita de programas o datos, el acceso a datos mediante una red, etcétera.

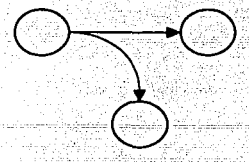

Fig. 3.2 Intercepción

**Modificación.** Se presenta cuando una parte no autorizada no sólo consigue acceder, sino que además daña algún objeto del sistema (Fig. 3.3). Por ejemplo, se pueden modificar valores en una base de datos, alterar un programa para que realice operaciones complementarias, o modificar los datos que se están transmitiendo.

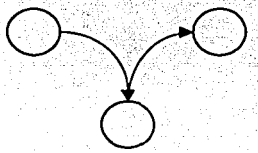

Fig. 3.3 Modificación

**Falsificación.** Se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "generado", es decir, una parte no autorizada puede generar objetos falsos en el sistema de cómputo (Fig. 3.4). Por ejemplo, el intruso puede añadir transacciones en una red, o añadir registros en una base de datos. Algunas de estas adiciones pueden ser detectadas como falsificaciones, pero si están muy bien realizadas, pueden no distinguirse de las reales.

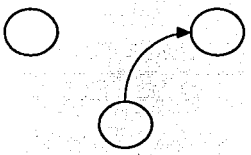

Fig. 3.4 Falsificación

En la gran mayoría de publicaciones relativas a la seguridad informática en general tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero es preferible hablar de "elementos" y no de personas ya que el sistema puede verse perjudicado por múltiples entidades aparte de humanos, como por ejemplo programas, catástrofes naturales, etcétera.



TESIS CON
FALLA DE ORIGEN

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema (Tabla 3.1) y que trata de proporcionar una idea acerca de qué o quién amenaza un sistema. A lo largo de este documento se ahondará en diferentes aspectos de los elementos presentados aquí.

| | | |
|---|---|---|
| **FACTORES HUMANOS** | Atacantes Pasivos<br><br>Atacantes Activos | Personal<br>Ex-empleados<br>Curiosos<br>Terroristas<br>Intrusos<br>Remunerados |
| **FACTORES LÓGICOS** | Software malicioso o incorrecto<br>Exploits<br>Herramientas de Seguridad<br>Puertas traseras<br>Bombas lógicas<br>Canales ocultos o encubiertos<br>Virus<br>Gusanos<br>Caballos de Troya<br>Programas conejo o bacterias<br>Técnicas Salami | |
| **FACTORES NATURALES** | Naturales: Temblores, Inundaciones, Tormentas eléctricas, otros | Artificiales: Actos terroristas, Electricidad, otros |

Tabla 3.1 Clasificación de Amenazas a los sistemas informáticos

Para ahondar en este tema, se resaltarán las características de cada una de las clasificaciones.

### 1.1 Factores Humanos

No podernos engañarnos, la mayoría de ataques a un sistema van a provenir en última instancia de personas que de manera ya sea intencionada o no intencionada, pueden causarnos enormes pérdidas.

Generalmente se trata de personas que intentan conseguir el máximo nivel de privilegio posible aprovechando errores del software. Pero con demasiada frecuencia se suele olvidar que los "piratas clásicos" no son los únicos que amenazan nuestros equipos. Es especialmente preocupante que mientras que hoy en día cualquier administrador preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos, etcétera), pocos administradores tienen en cuenta factores como la ingeniería social o el basureo a la hora de diseñar una política de seguridad.

Los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas se dividen en dos grandes grupos:

- **Los atacantes pasivos:** aquellos que curiosean por el sistema pero no lo modifican o destruyen. En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

- **Los atacantes activos:** aquellos que dañan el objetivo atacado, o lo modifican en su favor. Estos ataques implican algún tipo de modificación de la información o la creación de información falsa.

Dentro de estos grupos podemos destacar de manera particular los siguientes tipos de personas que pueden poner en riesgo los sistemas informáticos:

**Personal**

Las amenazas a la seguridad de un sistema y que provienen del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etcétera) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso los efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce los sistemas y sus debilidades), lo normal es que más que ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de archivos; en el primer caso, el "atacante" ni siquiera tiene acceso lógico (ni físico) a los equipos, ni conoce nada sobre seguridad en redes.

El 80% de los fraudes, robos, sabotajes o accidentes relacionados con los sistemas informáticos son causados por el propio personal de la organización, el ataque realizado por esa persona va a ser mucho más directo, difícil de detectar, y sobre todo, efectivo, que el de un atacante externo.

**Ex empleados**

Otro gran grupo de personas potencialmente interesadas en atacar el sistema son los antiguos empleados de la organización, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo. Pueden insertar troyanos, bombas lógicas, virus, etcétera o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después).

**Curiosos**

Los curiosos son los atacantes más habituales de sistemas en redes. Las personas suelen ser curiosas por naturaleza y esto produce una avalancha de estudiantes o personal intentando conseguir mayores privilegios de los que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Aunque en la mayoría de situaciones se trata de ataques no destructivos esto no beneficia en absoluto al entorno de fiabilidad que podamos generar en un

determinado sistema. Dentro de esta categoría podemos poner a los llamados "crackers", cuyo único objetivo es "romper" las barreras de seguridad de un sistema por mera satisfacción personal.

**Terroristas**

Bajo esta definición se engloba a cualquier persona que ataca al sistema de manera consciente simplemente por causar algún tipo de daño en él, dentro de esta categoría podemos mencionar a los comúnmente llamados "hackers"

**Intrusos remunerados**

Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía) o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.

### 1.1.1 Tipos de ataques a sistemas generados por personas

Después de haber visto los diferentes tipos de atacante que en la categoría de Personas puede tener el sistema, es necesario señalar los tipos de ataques que dichas personas pueden suscitar en el sistema; dentro de los ataques más comunes podemos citar:

**Ingeniería social**

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. El atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio.

**Shoulder Surfing**

Otro tipo de ataque relacionado con la ingenuidad de los usuarios del sistema (pero también con el control de acceso físico) es el denominado shoulder surfing. Consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.

**Masquerading**

El ataque denominado de masquerading o mascarada consiste simplemente en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno; esta suplantación puede realizarse electrónicamente (un usuario utiliza para acceder a una máquina un nombre de usuario y contraseña que no le pertenecen), o en persona.

El masquerading es más habitual en entornos donde existen controles de acceso físico, y donde un intruso puede "engañar" al dispositivo o persona que realiza el control, por ejemplo con una tarjeta de identificación robada que un lector acepta o con una credencial falsificada que un guardia de seguridad toma por buena.



TESIS CON
FALLA DE ORIGEN

Una variante del masquerading lo constituye el ataque denominado piggybacking, que consiste simplemente en seguir a un usuario autorizado hasta un área restringida y acceder a la misma gracias a la autorización otorgada a dicho usuario.

**Basureo**

La técnica del basureo está relacionada tanto con los usuarios como con la seguridad física de los sistemas; consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo. El basureo puede ser físico: buscar en botes de basura (*trashing*), listados de impresión o copias de documentos; o lógico: analizar buffers de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información.

Si deseamos evitar problemas lo más inmediato es utilizar una máquina trituradora de papel para destruir toda la documentación antes de arrojarla a la basura. En el caso de sistemas de almacenamiento lógico (discos, CD-ROMs, cintas, etcétera) también es importante una correcta inutilización de los mismos para que un potencial atacante no pueda extraer información comprometedora; no suele ser suficiente el simple borrado del medio o un leve daño físico (por ejemplo, partir un CD-ROM), lo más efectivo es un borrado seguro, seguido de una destrucción física importante que haga imposible la reconstrucción del medio.

## 1.2 Factores lógicos

Son otras de las amenazas comunes a los sistemas, bajo esta etiqueta encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como *malware*) o simplemente por error (bugs o agujeros). Dentro de esta clasificación es importante destacar los siguientes tipos:

**Software incorrecto**

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red del kernel o un error accediendo a memoria en un archivo, puede comprometer local o remotamente a cualquier sistema operativo.

**Exploit**

A los errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits. Representan la amenaza más común ya que cualquiera puede conseguir un exploit y utilizarlo contra la computadora sin ni siquiera saber cómo funciona y sin tener conocimientos mínimos del Sistema Operativo.

**Herramientas de seguridad**

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Estas herramientas pasan de ser útiles a ser peligrosas cuando las utilizan crackers que buscan información sobre las vulnerabilidades de un host o de una red completa. Si un administrador no utiliza herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), seguramente que un atacante podrá explotar dichas debilidades.



TESIS CON
FALLA DE ORIGEN

**Puertas traseras**

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les conoce como puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

**Bombas lógicas**

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa y los efectos obviamente pueden ser fatales.

**Canales ocultos o encubiertos**

Los canales ocultos son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Los canales ocultos no son una amenaza demasiado habitual en redes ya que suele ser mucho más fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia, y en este caso su detección suele ser difícil.

**Virus**

Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Todo el mundo conoce los efectos de los virus en algunos sistemas. En sistemas sobre plataformas IBM-PC o compatibles, ciertos virus, especialmente los de boot (arranque), pueden tener efectos nocivos, como dañar el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas, hay que tenerlos en cuenta.

**Gusanos**

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande. Se debe pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder al sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra



TESIS CON
FALLA DE ORIGEN

red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos, de ahí deriva su enorme peligro y sus devastadores efectos.

**Caballos de Troya**

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parece realizar las tareas que un usuario espera de él, pero realmente ejecuta funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

**Programas conejo o bacterias**

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etcétera), desembocando en una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar el bloqueo o paro total de la computadora.

**Técnicas salami**

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesos se roban unos centavos, nadie va a darse cuenta de ello; si se hace de manera automática para, por ejemplo, descontar un peso de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya computadoras dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, es conveniente comentar esta potencial amenaza contra el software encargado de estas tareas.

## 1.3 Factores Naturales

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales; sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen medidas básicas, ya que si se produjeran generarían los mayores daños.

Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud.

Hasta ahora se ha hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; para completar la visión de la seguridad, se debe hablar de las medidas de seguridad para garantizar un funcionamiento continuo y sin intromisiones en los sistemas, por lo que es imprescindible que a la seguridad se le dé un enfoque radicalmente diferente y de visión global, que vaya más allá de soluciones locales. Un tratamiento total de la seguridad incluye aspectos de la **seguridad tanto externa como interna**.



TESIS CON
FALLA DE ORIGEN

## 2. SEGURIDAD EXTERNA

La seguridad externa se ocupa de proteger el recurso de cómputo contra intrusos y desastres, asimismo se subdivide en **seguridad física y seguridad operacional.**

### 2.1 Seguridad Física

Engloba aquellos mecanismos que impiden a los agentes físicos la destrucción del equipo y de la información existente en el sistema; entre ellos se pueden citar el fuego, el humo, inundaciones, descargas eléctricas, campos magnéticos, acceso físico de personas no autorizadas, entre otros. En este tipo de seguridad son importantes los mecanismos de detección (detectores de humo, sensores de calor, detectores de movimiento, etcétera); de igual manera, para tratar de impedir la entrada de intrusos es necesario contar con sistemas de identificación física (tarjetas de identificación, sistemas de reconocimiento de huellas dactilares, identificación por reconocimiento de voz, etcétera).

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. Más claramente por "seguridad física" podemos entender todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema.

Cada sitio es diferente, y por tanto también son diferentes sus necesidades de seguridad; de esta forma, no se pueden dar recomendaciones específicas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave el sitio donde se encuentran los sistemas de cómputo (servidores, ruteadores, etcétera) y que en adelante denominaremos site) hasta medidas mucho más complejas, como la prevención de radiaciones; de cualquier forma, en cada caso se debe analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, y así, de acuerdo a los resultados obtenidos diseñar un plan de seguridad adecuado.

El hardware es frecuentemente el elemento más expuesto de todo sistema informático, en vista de que es un elemento tangible y fácil de encontrar. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización. La posibilidad de acceder físicamente a un equipo de cómputo hace inútiles casi todas las medidas de seguridad que se hayan aplicado.

Es claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger. Mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o las máquinas de los despachos, otros muchos estarán en lugares de acceso semipúblico, y es justamente sobre estos últimos sobre los que se deben extremar las precauciones, ya que lo más fácil y discreto para un atacante es acceder a uno de estos equipos y en segundos, lanzar un ataque completo sobre la red.

Es necesario prevenir el acceso físico a los equipos de cómputo, para ello existen soluciones para todos los gustos y también de todos los precios para prevenir un acceso físico no autorizado a un determinado punto: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta. De todos ellos, quizás los más adecuados a la seguridad física sean los biométricos (analizadores de retina o verificadores de la geometría de la mano) y los basados en alguna pertenencia (llaves, tarjetas, etcétera); aunque suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media. **Es necesario tomar en cuenta que si el sistema de protección es más caro en comparación a lo que se quiere proteger existe un grave error en los planes de seguridad.**

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano, etcétera) es deseable que un ataque potencial sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas de accesos físicos no autorizados intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales el esfuerzo en detectar estas amenazas debe centrarse en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos; sucede lo mismo que con la seguridad lógica: se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Es importante concienciar a todos de su papel en la política de seguridad del entorno; si por ejemplo, un usuario autorizado detecta la presencia de quien sospecha no tiene autorización para estar en una determinada estancia, debe avisar inmediatamente al administrador o al responsable de los equipos.

Dado que un dispositivo es fácilmente visible, presenta un punto de ataque bastante simple; afortunadamente, se pueden tomar medidas razonables para salvaguardarlos y protegerlos de los dos problemas más importantes: **el robo y la destrucción.**

Son muchas las amenazas al hardware en una instalación de cómputo (Fig. 3.5); aquí se presentarán algunas de ellas, sus posibles efectos y algunas soluciones, si no para evitar los problemas sí al menos para minimizar sus efectos.

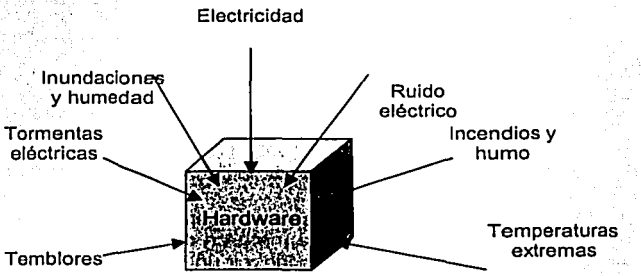


Fig. 3.5 Amenazas a la seguridad externa

### 2.1.1 Temblores

Aunque algunas medidas contra temblores son excesivamente caras no cuesta nada tomar ciertas medidas de prevención tales como:

- No situar nunca equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos a ras de suelo) ya que un pequeño temblor puede tirar desde una altura considerable un complejo hardware, lo que con toda probabilidad lo inutilizará.
- Utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los ruteadores.
- No situar objetos pesados en superficies altas cercanas a los equipos, ya que si cayeran también dañarán el hardware.

TESIS CON
FALLA DE ORIGEN

- No situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o hardware pierde importancia frente a los posibles accidentes, incluso mortales, que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se descuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

- Quizá no sea necesario el tener un temblor o terremoto para dañar a los equipos, las simples vibraciones podrían desencadenar daños en los circuitos. Para hacer frente a las pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de tal manera que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras: estos dispositivos generan vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima del CPU de una máquina no es una buena idea.

### 2.1.2 Tormentas eléctricas

Las tormentas generan intempestivamente subidas de tensión infinitamente superiores a las que pudiera generar un problema en la red eléctrica. Si cae un rayo sobre la estructura metálica del edificio seguramente se deberán reemplazar los equipos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son más o menos predecibles, lo que permite tomar ciertas medidas:

- Apagar las máquinas y desconectarlas de la línea eléctrica.

- Los medios magnéticos, especialmente las copias de seguridad; se deben almacenar lo más alejados posible de la estructura metálica de los edificios ya que un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas las cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de los sistemas.

### 2.1.3 Inundaciones y humedad

Para que los equipos funcionen correctamente es necesario contar con cierto grado de humedad; en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al hardware y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina. Algunas de las medidas que se toman son:

- Ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas.

- Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

En las inundaciones, los problemas generados son mucho mayores. Casi cualquier medio (una computadora, una cinta, un ruteador, etcétera) que entre en contacto con el agua automáticamente será inútil, ya sea por el propio líquido o por los cortocircuitos que se generan en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención (frente a las de detección):

- Utilizar detectores de agua en los suelos o suelos falsos de las salas y apagar automáticamente los sistemas en caso de que se activen.
- Instalar un sistema automático que corte la corriente para evitar situaciones de electrocución.
- Los detectores de agua deben ubicarse en un nivel más bajo del que se encuentran los equipos a proteger.
- Situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

### 2.1.4 Electricidad

Los problemas relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, etcétera a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

- La forma más efectiva de proteger los equipos contra estos problemas de la corriente eléctrica es utilizar un Sistema de Alimentación Ininterrumpida (UPS *Uninterrupted Power System*) conectado al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando durante cierto tiempo a los equipos incluso en caso de que no reciban electricidad, con el fin de que los equipos se puedan apagar correctamente sin pérdidas de información.

Un último problema es la corriente estática. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño, el equipo sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM.

- Contra el problema de la corriente estática existen muchas soluciones y muy baratas: spray antiestático, ionizadores antiestáticos y obviamente el evitar tocar directamente cualquier parte metálica, usar tapetes o brazaletes antiestáticos si se deben hacer operaciones con el hardware y no mantener el entorno excesivamente seco.

### 2.1.5 Ruido eléctrico

El ruido eléctrico suele ser generado por motores o por maquinaria pesada y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos se pueden tomar las siguientes medidas:

- No situar hardware cercano a la maquinaria que puede causar dicho ruido, o bien, instalar filtros en las líneas de alimentación que llegan hasta los equipos.

- Mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos pueden incluso dañar permanentemente al hardware si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

### 2.1.6 Incendios y humo

Los incendios generados por cualquier medio son una latente amenaza que hay que prevenir. Es necesario tomar en consideración las siguientes medidas:

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor, de preferencia no con base en agua (que al final daña los equipos) sino de halón o bióxido de carbono.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos.

Pero puede existir humo sin necesidad de que haya un fuego: por ejemplo, en lugares donde se fuma, la suciedad generada se deposita en todas las partes de una computadora, desde el teclado hasta el monitor por lo que el humo afecta directamente a todos los componentes.

De lo anterior se puede deducir que es conveniente instalar detectores de humo. Y obviamente evitar fumar cerca de los equipos.

### 2.1.7 Temperaturas extremas

La temperatura a la que opera un equipo electrónico es un factor importante para su desempeño, por lo que debe ser plenamente controlada considerando las siguientes recomendaciones:

- Es recomendable que los equipos en las salas de cómputo y los sites operen entre 18 y 20 grados centígrados.

- Para controlar la temperatura no hay nada mejor que instalar un sistema de aire acondicionado profesional.

- Los equipos deben estar correctamente ventilados, sin elementos que obstruyan los ventiladores de la CPU.

- La organización física de la computadora también es decisiva para evitar sobrecalentamientos; si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

### 2.1.8 Protección de los datos

La seguridad física también implica una protección a la información del sistema, tanto la que está almacenada como a la que se transmite entre diferentes equipos. Existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en dicho medio.

La intercepción o *eavesdropping*, también conocida por *passive wiretapping* es un proceso mediante el cual un agente capta información, en claro o cifrada, que no estaba originalmente dirigida a él. Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras se produce, de manera que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.

Un medio de intercepción bastante habitual es el *sniffing* (husmeo, curioseo), consistente en capturar tramas que circulan por la red mediante un programa que incorpora entre sus características el análisis de protocolos, lo que permite hacer una decodificación del tráfico de la red y hacerlo entendible.

Originalmente los programas sniffing comerciales eran usados para ayudar a mantener las redes (Networks Associates Sniffer for Windows, WinNT Server(Network Monitor), EtherPeek, Intellimax Lan Explorer, etcétera). Los usos típicos para estos programas incluyen:

- Obtención automática de contraseñas y nombres de usuario de la red.
- Conversión de los datos capturados a un formato perfectamente entendible para los humanos, así, cualquier persona podrá leer el tráfico en la red.
- Análisis de fallas, para descubrir problemas en la red.
- Análisis de desempeño para descubrir cuellos de botella.
- Detección de intrusiones en la red.
- Creación de bitácoras de tráfico en la red, de tal manera que se creen accesos que los hackers no puedan "romper" ni borrar.

Ahora los programas sniffers son usados para "meterse" en las computadoras, capturar el tráfico en la red, decodificarlo y analizarlo, y por último usarlo de acuerdo a los intereses; como ejemplo de estos programas podemos listar: snmpsniff, rootshell, ipsend, Net RawIP, Globber, Beholder, BlackICE Sentry IDS, etcétera.

Como se puede apreciar, después de saber el funcionamiento de este tipo de ataques y considerando que prácticamente se puede realizar en cualquier conexión de la red y que es prácticamente imperceptible, es importante tomar medidas de precaución contra este tipo de ataques, aquí se listan algunas de las soluciones:

- Ubicar las conducciones de cableado de red del edificio dentro de la sala, asegurando que dicha conducción "central" también esté protegida y que todos los puntos de acceso estén supervisados desde la sala de control (*site*).

- Asegurar que todo el cableado de comunicaciones esté protegido. Si el cableado tiene que pasar por un área no protegida, de ser posible se debe utilizar cable de fibra óptica.

- Usar aplicaciones de cifrado al realizar las comunicaciones o el almacenamiento de la información, de tal manera que aún cuando puedan husmear en la red, la información no sea legible. (Ver **Anexo 1. Criptografía**)

- Deshabilitar en los concentradores cualquier conector o servicio que no se utilice.

- Utilizar el cableado en vacío para evitar la intercepción de datos que viajan por la red: la idea es situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión; si un atacante intenta "pinchar" el cable para interceptar los datos, rompe el vacío o el nivel de presión y el ataque es detectado inmediatamente. Esta solución es enormemente cara y solamente se aplica en redes de perímetro reducido para entornos de alta seguridad.

- Para evitar el husmeo y obtención de contraseñas y nombres de usuario, existen otras soluciones para lograr una autenticación segura: SMB/CIFS, Kerberos v5, Stanford SRP, etcétera.

#### 2.1.8.1 Respaldos

Aún cuando formalmente los medios de respaldo no se consideren parte del hardware es necesario tener siempre presente que si las copias contienen toda la información, es necesario protegerlas igual que se protege a los sistemas.

- Los respaldos deben ser periódicos y de acuerdo a las necesidades de la organización.

- Se debe asegurar que el dispositivo de copias de seguridad está almacenado bajo llave.

- Etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido (sistemas de archivos almacenados, día y hora de la realización, sistema al que corresponde, etcétera).

- Proporcionar un lugar seguro para almacenar los medios de copia de seguridad, documentación y equipos esenciales. En este lugar también deberán ser instalados monitores y detectores de humo y agua.

La información también puede encontrarse en lugares menos obvios, como listados de impresora, facturas telefónicas o la propia documentación de una máquina.

- Las impresoras, plotters, faxes, o cualquier dispositivo por el que pueda salir información de nuestro sistema deben estar situados en un lugar de acceso restringido.

- También es conveniente que el lugar donde los usuarios recogen los documentos que salen de estos dispositivos sea de acceso restringido.

### 2.1.9 Algunas consideraciones generales:

- Ubicar la sala de cómputo (*site*) en el centro del edificio, o al menos, en una ubicación que no tenga muros externos y en lugares que no impidan la entrada y salida de los equipos.

- Ubicar las conducciones de cableado de red del edificio dentro de la sala, asegurando que dicha conducción "central" también esté protegida y que todos los puntos de acceso estén supervisados desde la sala de control.

- Disponer de un piso falso para acomodar el cableado de los sistemas y con la profundidad suficiente para facilitar el acceso y la reconfiguración.

- Instalar una puerta de seguridad ignífuga y con el ancho suficiente para facilitar la entrada y salida de los equipos de cómputo de mayor tamaño.

- Instalar un sistema de alarma sofisticado con sensores en todas las puertas y todos los puntos de acceso, incluyendo el techo y suelo falsos.

- Limitar el acceso a la sala solamente a las personas que requieran dicho acceso, mediante acreditaciones de seguridad (tarjetas de identificación, códigos de barra, sistemas de identificación por huellas dactilares o voz, etcétera).

- Instalar un sistema de control de acceso que supervise y registre los accesos que se hagan a la sala.

- Establecer un sistema que registre todos los detalles relacionados con la entrada y salida periódica de medios y equipos de copia de seguridad.

- Los equipos de cómputo y de comunicaciones deben fijarse a un soporte, para evitar el robo.

- Tener todos los concentradores, ruteadores y otros dispositivos de conexión bajo llave y de preferencia dentro de la sala.

- Implementar un proceso de auditoría periódico que compruebe todos los puntos de supervisión, los puntos de acceso y las comprobaciones ambientales.

- La adquisición de seguros, aunque no se considere una medida de prevención general, de alguna manera nos asegura que se recuperará el valor del equipo después de un siniestro.

## 2.2 Seguridad Operacional

Una vez que se comprenda como proteger físicamente el sistema, el paso siguiente consiste en establecer diversas políticas y mecanismos con el fin de salvaguardar la integridad, disponibilidad y confidencialidad del sistema, esto es lo que se conoce como **Seguridad Operacional.**

A los mecanismos utilizados para implementar las políticas de seguridad se les conoce como **mecanismos de seguridad** y son la parte más visible de nuestro sistema ya que se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: **de prevención, de detección y de recuperación.**

- Los **mecanismos de prevención** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un

mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red.

- Por **Mecanismos de detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.

- Los **mecanismos de recuperación** son aquellos que se aplican cuando una violación del sistema ya se ha detectado y se debe retornar a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Los tres tipos de mecanismos son importantes para la seguridad del sistema, se tiene que enfatizar el uso de mecanismos de prevención y de detección ya que evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina.

### 2.2.1 Políticas generales de la seguridad operacional

Existen varias políticas que de manera general deben establecerse para proteger un sistema de cómputo, entre ellas se pueden nombrar las siguientes:

- **Autorización:** Determina que acceso se permite a quien. De manera práctica es lo que los administradores conocen como asignación de privilegios o derechos de usuario. Los permisos son la protección más básica de los objetos del sistema operativo; definen quién puede acceder a cada uno de ellos, y de qué forma puede hacerlo.

- **Clasificación:** Los datos y los usuarios del sistema se dividen en clases y de esta manera a las clases se les conceden diferentes derechos de acceso. Es mucho más fácil tener control sobre el sistema si se crean grupos de usuarios con características comunes (mismo departamento, jerarquía, etcétera), de tal manera que los derechos se asignen a los grupos y no a usuarios en particular.

- **Formación de usuarios :** Como ya se ha mencionado, el personal constituye uno de los puntos débiles en un sistema informático. La solución a problemas relacionados con el personal es con frecuencia mucho más compleja que la de problemas de seguridad lógica o seguridad de la red. El responsable de seguridad debe crear conciencia en todas las personas sobre la necesidad de la seguridad para que el entorno de trabajo funcione como se espera de él; la seguridad informática se ha de ver como una cadena que se rompe si falla uno de sus eslabones: no importa que tengamos un sistema de cifrado resistente a cualquier ataque o una autenticación fuerte de cualquier entidad del sistema si un intruso es capaz de obtener un nombre de usuario con su correspondiente contraseña simplemente llamando por teléfono a una secretaria. Además de conciencia, para conseguir un sistema fiable es necesaria la formación de los mismos, no debería ser tan habitual que la gente utilice o administre una red sin unos conocimientos previos del sistema operativo. Las ideas básicas se pueden incluso resumir en una hoja que se le entregue a cada usuario al darlos de alta en el sistema. Si pasamos a hablar de administradores, sí sería recomendable exigirles un cierto nivel de conocimientos de seguridad.

- **Confianza en las personas:** Se debe contratar personal en quien se confíe. En una organización una norma básica sería verificar el currículo de cualquier aspirante a nuevo miembro (no simplemente leerlo y darlo por bueno, sino comprobar los datos y directamente descartar al aspirante si se detecta una mentira).

- **Necesidad de saber (*Need to know*) o mínimo privilegio:** A cada usuario se le debe otorgar el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, darle acceso a los recursos mínimos para trabajar correctamente y se le debe permitir que sepa solamente lo que necesita para trabajar.

- **Conocimiento parcial (*Dual Control*):** Las actividades más delicadas dentro de la organización en cuanto a seguridad se refiere, deben ser realizadas por dos personas competentes, de forma que si uno de ellos comete un error o intenta violar las políticas de seguridad el otro pueda darse cuenta rápidamente y subsanarlo o evitarlo. De la misma forma, aplicar este principio asegura que si uno de los responsables abandona la organización o tiene un accidente el otro pueda seguir operando los sistemas mientras una nueva persona sustituye a su compañero.

- **Rotación de funciones:** Quizás la mayor amenaza al conocimiento parcial es la potencial complicidad que los dos responsables de cierta tarea pueden llegar a establecer, de forma que entre los dos sean capaces de ocultar las violaciones de seguridad que nuestros sistemas puedan sufrir; incluso puede suceder lo contrario: que ambas personas sean enemigos y esto repercuta en el buen funcionamiento de la política de seguridad establecida. Para evitar ambos problemas, una norma común es rotar a las personas a lo largo de diferentes responsabilidades, de forma que a la larga todos puedan vigilar a todos; esto también es muy útil en caso de que alguno de los responsables abandone la organización, ya que en este caso sus tareas serán cubiertas más rápidamente.

- **División de responsabilidades:** No es en absoluto recomendable que una sola persona (o dos, si establecemos un control dual) posea o posean demasiada información sobre la seguridad de la organización; es necesario que se definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad de un sistema no posea al mismo tiempo la capacidad para violar dicha seguridad sin que nadie se percate de ello.

- **Vigilancia:** Se ocupa de supervisar el sistema y realizarle auditorías, así como de verificar la identidad de los usuarios del sistema sin que haya posibilidad de rechazar usuarios legítimos.

- **Supervisión de amenazas:** Para reducir al mínimo los riesgos de seguridad es preferible que el Sistema Operativo y no el usuario, controle las operaciones delicadas. Mediante la técnica de supervisión de amenazas, cuando el usuario desea obtener acceso a un recurso, hace la solicitud al Sistema Operativo, el cual puede conceder o denegar el acceso. Si el acceso es concedido, entra en un acción un programa de vigilancia (rutinas propias del Sistema Operativo) que se encargan del acceso real al recurso y pasa los resultados al programa del usuario. La supervisión de amenazas permite detectar los intentos de penetración en el momento en el que se producen y notificar inmediatamente al administrador del sistema.

- **Amplificación:** Se produce cuando un programa de vigilancia necesita mayores derechos de acceso de los que dispone el usuario para poder atender su solicitud.

- **Protección por contraseña:** Es un mecanismo para el control de los intentos de entrada o acceso al sistema, de tal forma que se permita la conexión si se pasa el control correspondiente o se rechace el intento en aquellos casos en que la identificación no sea satisfactoria. Existen tres clases de elementos para la verificación de la autenticidad con los cuales se puede establecer la identidad de una persona:

| | |
|---|---|
| **Algo característico de la persona:** | Huellas dactilares, fotografías, patrones de voz, firmas |
| **Algo que la persona posee:** | Llaves, tarjetas de identificación, credenciales, etcétera |
| **Algo que la persona sabe:** | Contraseñas, combinaciones de cerraduras, etcétera |

El esquema más común para verificar la autenticidad es la simple protección por contraseña, donde el usuario elige una palabra clave, la memoriza y la teclea para ser admitido en el sistema. La protección por contraseña tiene varios puntos débiles: los usuarios eligen contraseñas fáciles de recordar, no es muy común el cambio periódico de las contraseñas, el uso de contraseñas largas hace que a veces sea difícil recordarlas, etcétera, por lo que es recomendable utilizar los siguientes criterios cuando se establece una protección de este tipo:

- La contraseña no debe desplegarse en pantalla ni aparecer impresa.
- Requerir contraseñas no muy pequeñas que sean fáciles de adivinar ni demasiado largas que puedan ser difíciles de memorizar por los usuarios.
- Las contraseñas deben cambiarse frecuentemente.
- Limitar el número de intentos de entrada.
- La lista maestra de contraseñas debe guardarse en un archivo seguro y de manera cifrada, de tal manera que aún cuando sea encontrada resulte inútil para un intruso. (Ver **Anexo 2. Gestión de Contraseñas** )

- **Auditoría:** Suele realizarse a posteriori en sistemas manuales, es decir que se examinan las recientes transacciones de una organización para determinar si hubo ilícitos. La auditoría en un sistema puede implicar un procesamiento inmediato, pues se verifican las transacciones que se acaban de realizar.

Es importante llevar una bitácora de la auditoría ya que en ella se llevará un registro permanente de los acontecimientos importantes que ocurren en el sistema. La bitácora de auditoría es un mecanismo importante de detección por lo que debe cumplir con las siguientes características:

- Se debe realizar automáticamente cada vez que ocurra un evento.
- Debe ser almacenada en un área altamente protegida del sistema.

- Sin embargo, la simple producción de la bitácora de auditoría no garantiza una seguridad adecuada. Es necesario revisar la bitácora cuidadosamente y con frecuencia. Dichas revisiones deben llevarse a cabo de manera periódica con el fin de atender de manera regular los problemas de seguridad; o al azar con el fin de atrapar desprevenidos a los intrusos.

## 3. SEGURIDAD INTERNA

La segunda parte importante de la seguridad total es la **Seguridad Interna**. Este tipo de seguridad trata de los controles integrados al equipo y al Sistema Operativo para asegurar la confiabilidad, operabilidad y la integridad de los programas y datos.

Una de las principales causas de violaciones a sistemas informáticos son generadas por fallas intencionales o accidentales de los Sistemas Operativos. La mayoría de los Sistemas Operativos comerciales y de dominio público presentan grandes deficiencias en su base de seguridad, debido a que no fueron diseñados con este objetivo de manera primordial sino que han sido agregados como módulos independientes.

La clave para la seguridad interna es controlar el acceso a los recursos y datos almacenados ya que la pérdida o alteración no deseada de dicha información podría causar trastornos que en algunos casos pueden ser irreparables. De esta manera podemos decir que la seguridad interna engloba los mecanismos dirigidos a asegurar el sistema, siendo el propio sistema el que controla dichos mecanismos. Los principales enemigos de la seguridad interna son las amenazas lógicas, descritas anteriormente.

### 3.1. Mecanismos de Seguridad Interna

Después de repasar las amenazas lógicas, es importante saber que existen mecanismos dedicados a hacer frente a tales amenazas. Los mecanismos de prevención más habituales son los siguientes:

- **Mecanismos de identificación y autenticación.**

  Estos mecanismos hacen posible identificar entidades del sistema de una forma única y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

- **Mecanismos de control de acceso**

  Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

- **Mecanismos de separación**

  Cualquier sistema con diferentes niveles de seguridad debe implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso.

Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

- **Mecanismos de seguridad en las comunicaciones**

Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, se utilizan ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales (Ver **Anexo 1. Criptografía**). Aunque cada vez se utilizan más los protocolos seguros, aún es frecuente encontrar conexiones en texto claro ya no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.

La seguridad interna está íntimamente relacionada con los procesos en un Sistema Operativo, los cuales deben estar protegidos de las actividades de los otros. Lo ideal sería tener un Sistema Operativo seguro que pueda ofrecer las siguientes características:

- Identificar y autenticar a cada uno de los usuarios que ingresen al sistema.
- Controlar el acceso a todos los recursos e información.
- Auditar las acciones realizadas por los usuarios.
- Auditar los acontecimientos que puedan representar amenazas a la seguridad.
- Garantizar la integridad de los datos y mantener la disponibilidad de los recursos e información.

Con ese propósito se crearon diversos mecanismos de protección que pueden usarse para asegurar que los archivos, segmentos de memoria, CPU y otros recursos pueden ser usados sólo por los procesos que tienen autorización del Sistema Operativo.

Por ejemplo, el hardware de direccionamiento de memoria asegura que cada proceso sólo se ejecutará dentro de su espacio. El timer o reloj hardware asegura que ningún proceso acceda a la CPU y no la libere.

Dentro de la seguridad de la memoria, existen mecanismos para evitar que un usuario acceda a la información de otro sin autorización. Entre ellos podemos citar Registros límites o frontera y el estado protegido y no protegido del procesador.

El motivo de mayor importancia para la protección es la necesidad de asegurar que cada componente de programa activo en un sistema usa recursos de forma consistente con los permisos establecidos para el uso de los recursos.

Los derechos de acceso definen que acceso tienen varios sujetos a diversos objetos. Los objetos son entidades que contienen información. Pueden ser objetos físicos: discos, cintas, procesadores o palabras de almacenamiento; o bien, pueden ser objetos abstractos que corresponden a estructuras de datos o procesos.

Los objetos deben ser protegidos de los sujetos. La autorización dentro de un sistema de cómputo se otorgan a los sujetos. Los sujetos pueden ser usuarios, procesos, programas u otras entidades.

Los derechos de acceso más comunes son:

- Acceso de lectura
- Acceso de escritura

- Acceso de ejecución

Obviamente, un sujeto deberá acceder solo a los recursos a los que tiene permiso. Más aún, en cualquier momento sólo debe poder acceder a los recursos que necesita para su tarea.

### 3.2 Dominios de Protección

Cuando se inicia una sesión en el sistema después de haber pasado por los mecanismos de identificación y autenticación, el sistema operativo le asigna a cada usuario un **dominio de protección,** el cual especifica los recursos a los que puede acceder el sujeto. Cada dominio define un conjunto de objetos y los tipos de operaciones que se pueden invocar en cada objeto. La posibilidad de ejecutar una operación en un objeto es un derecho de acceso.

Un dominio es una colección de derechos de acceso, cada uno de los cuales es un par ordenado {nombre de objeto, conjunto de derechos}. Los dominios no son necesariamente disjuntos; pueden compartir los derechos de acceso.

De manera gráfica podemos representar las características de los dominios de protección de la siguiente manera (Fig.3.6):

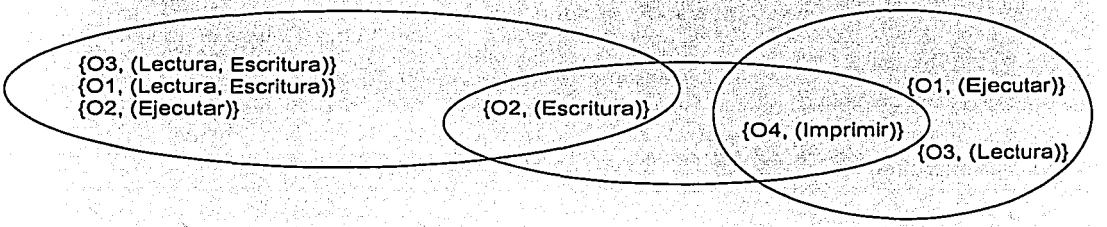


Fig. 3.6 Sistema con tres dominios de protección

En el modo estándar usuario/supervisor, cuando un proceso se ejecuta en modo supervisor, puede ejecutar instrucciones privilegiadas, y tomar control de todo el sistema. Por otro lado, si el proceso se ejecuta en modo usuario, sólo puede invocar instrucciones no privilegiadas. Estos dos modos protegen al sistema operativo de los procesos de usuarios. En un sistema operativo multiprogramado, dos dominios de protección son insuficientes, porque los usuarios quieren estar protegidos uno del otro, es necesario un esquema más elaborado.

### 3.3 Matriz de accesos

En general, los sistemas operativos almacenan la información relativa a los dominios en lo que se denomina **Matriz de accesos** (también conocida como **Matriz de Dominios**). Las filas de la misma representan los dominios, y las columnas a los objetos. Cada entrada en la matriz consiste de un conjunto de derechos de acceso. Como los objetos están definidos explícitamente por la columna, podemos omitir el nombre del objeto del derecho de acceso. Para ilustrar estos conceptos, tenemos la siguiente representación gráfica (Tabla. 3.2).

| Objeto / Dominio | F1 | F2 | F3 | Lector de Tarjetas | Impresora |
|---|---|---|---|---|---|
| D1 | Lectura | | Lectura | | |
| D2 | | | | Lectura | Impresión |
| D3 | | Lectura | Ejecución | | |
| D4 | Lectura Escritura | | Lectura Escritura | | |

Tabla 3.2 Matriz de Accesos

### 3.4 Tabla Global

La implementación más simple de la matriz de accesos es una tabla global que consiste de un conjunto de ternas {dominio, objeto, conjunto de derechos}. Cuando se ejecuta una operación en un objeto Oj dentro del dominio Di, se busca en la tabla {Di, Oj, Rk}, donde M pertenece a Rk. Si se encuentra la terna, se permite la operación, si no, ocurre una excepción. Esta implementación tiene varias desventajas ya que la tabla suele ser muy grande, y no puede mantenerse en memoria por lo tanto existen más entradas/salidas. Además es difícil agrupar objetos o dominios con características similares. Por ejemplo, si un objeto puede ser leído por cualquiera, deberá tener una entrada por separado en cada dominio.

### 3.5 Listas de acceso

Si la matriz anterior tiene poca información, se recurre a otro tipo de almacenamiento de información sobre dominios, que consiste en asociar a cada recurso una lista de dominios que pueden utilizarlo, denominándose **listas de acceso.** Las entradas vacías se obvian. La lista resultante para cada objeto consta de pares ordenados {dominio, conjunto de derechos}, que definen todos los dominios con un conjunto no vacío de derechos de acceso para ese objeto.

### 3.6 Listas de capacidades

También se puede obtener otro vector donde a cada dominio se le asigna una lista de recursos a los que puede acceder, denominándose en este caso, **lista de capacidades.** Aquí el orden está dado por las filas de la matriz, donde cada fila es para un dominio. Una lista de capacidades para un dominio es una lista de objetos, y las operaciones permitidas sobre él. Un objeto, en general, está representado por su nombre único o dirección única (llamado capacidad).

Este sistema es muy seguro si no se permite el acceso directo de la "capacidad" en el espacio de dirección del usuario (o sea, que el usuario no pueda tener acceso a ella, por lo tanto, no la puede modificar en forma directa). Si todas las "capacidades" están protegidas, el objeto al cual protegen está seguro. Las capacidades se distinguen de otros datos (tipos) por una de estas dos razones:

- Cada objeto tiene un rótulo (tag) para denotar su tipo como capacidad o como dato accesible. Los rótulos no deben ser accesibles por los programas de aplicación. Se usa al Hardware o al

Firmware para hacer esto más fuerte. El hardware debe distinguir los tipos de datos (enteros, apuntadores, instrucciones, puntos flotantes, etcétera).

- El espacio de direcciones de un programa debe ser dividido en dos partes: la de código y datos (accesible por el mismo), y la parte de lista de capacidades, accesible sólo por el Sistema Operativo.

Ejemplo:

Un ejemplo serían los semáforos, a los que sólo es posible acceder por medio de operadores.

Una forma de implementación sería la de memoria segmentada.

### 3.7 Implementación del mecanismo LOCK/KEY (llave/candado)

Es un compromiso entre listas de acceso y listas de capacidad en el que cada objeto tiene una lista de bits de candado (*locks*), y cada dominio tiene otra lista de bits de llave (*keys*).

Un proceso sólo puede ejecutar (acceder) al objeto si el dominio al cual pertenece tiene llaves que coincidan con los candados del objeto. Las llaves del dominio son manejadas solo por el sistema operativo.

### 3.8 Comparación de las implementaciones

Las Listas de Acceso corresponden a las necesidades de usuario. Cuando se crea un objeto especifica a qué dominio pertenece por lo que en sistemas con grandes cantidades de objetos (usuarios, recursos compartidos, etcétera), la búsqueda puede llegar a ser muy grande.

Las Listas de Capacidades no son sencillas de implementar. Pero una vez que se han implementado, sólo es necesario verificar que la capacidad es válida. La revocación de derechos es muy complicada debido a que las capacidades están distribuidas por todo el sistema.

El mecanismo de Llave/Candado es una solución de compromiso. Es efectivo y flexible. Si bien cualquier cambio sólo requiere cambiar la configuración de unos pocos bits, si el sistema posee una gran volatilidad (existen muchos dominios u objetos nuevos o que desaparecen, muchos permisos se cambian o se agregan constantemente), puede ser necesario replantear la función de mapeo lo cual, en estos casos, torna el mecanismo en algo muy complejo.

### 3.9 Estructuras de protección dinámicas

La asociación entre un proceso y un dominio puede ser estática si los recursos disponibles para ese proceso lo serán para toda la ejecución, o dinámica si existen cambios de accesos o dominios. Si se permiten estos cambios, posiblemente sean violadas las protecciones.

Un mecanismo que permite hacer esta implementación es incluir a los mismos dominios como objetos de la matriz de accesos, y cuando sean necesarios cambios en los accesos incluir a la propia matriz como objeto. Como lo que se quiere es que cada entrada pueda ser modificada en forma individual, se considera cada entrada como un objeto. Para poder realizar esto, es necesario incluir el derecho Switch, que se describe y representa gráficamente en la Tabla 3.3.

**Switch**

Un proceso puede cambiar del dominio D(i) al dominio D(j) si el derecho de acceso SWITCH pertenece al Acceso(i,j).

Este mecanismo se representa de manera gráfica en la siguiente tabla:

| Objeto / Dominio | F1 | F2 | F3 | Lector de Tarjetas | Impresora | D1 | D2 | D3 | D4 |
|---|---|---|---|---|---|---|---|---|---|
| D1 | Lectura | | Escritura | | | | Switch | | |
| D2 | | | | Lectura | Impresión | | | Switch | Switch |
| D3 | | Lectura | Ejecución | | | | | | |
| D4 | Lectura Escritura | | Lectura Escritura | | | Switch | | | |

Tabla 3.3 Representación gráfica del Mecanismo Switch

## 3.10 Cambio de contenido de la matriz de accesos.

El permitir cambios controlados en la matriz de acceso requiere de tres operaciones adicionales: **copy, owner y control.**

**Operación Copy**

La capacidad de copiar un derecho de acceso existente de un dominio a otro (fila) de la matriz de accesos se indica agregando un asterisco al derecho de acceso (Tabla 3.4).

| Objeto / Dominio | F(1) | F(2) | F(3) |
|---|---|---|---|
| D1 | Lectura | | Escritura* |
| D2 | | Lectura* | Ejecutar |
| D3 | Lectura | | |

Tabla 3.4 Representación gráfica de la operación Copy

El derecho COPY solo permite copiar el derecho de acceso dentro de la misma columna (es decir para el mismo objeto) en la cual está definido tal derecho (Tabla 3.5).

| Objeto / Dominio | F(1) | F(2) | F(3) |
|---|---|---|---|
| D1 | Lectura | | Escritura* |
| D2 | | Lectura* | Ejecutar |
| D3 | Lectura | Lectura | |

Tabla 3.5 La tabla anterior una vez aplicada la operación Copy

**Operación Owner**

Necesitamos además del copiado algún mecanismo para agregar nuevos derechos y eliminar otros, el derecho de acceso Owner controla estas operaciones. La representación gráfica de esta operación se muestra en la Tabla 3.6

| Dominio \ Objeto | F(1) | F(2) | F(3) |
|---|---|---|---|
| D1 | Lectura Owner | | Escritura |
| D2 | | Lectura Owner* | Lectura Owner* |
| D3 | Lectura | | |

Tabla 3.6 Representación gráfica de la operación Owner

Si en un acceso (i,j) dado tenemos Owner, significa que un proceso ejecutado en D(i) puede agregar o quitar accesos en toda la columna j (Tabla 3.7).

| Dominio \ Objeto | F(1) | F(2) | F(3) |
|---|---|---|---|
| D1 | Lectura Owner | | |
| D2 | | Lectura/Escritura Owner* | Lectura Owner* |
| D3 | | Escritura | Escritura |

Tabla 3.7 La tabla anterior una vez aplicada la operación Owner

**Operación Control**

El Copy y el Owner permite que un proceso altere entradas en una columna. Un mecanismo para alterar entradas en las filas (Dominios) es igual de necesario. Tal mecanismo es el derecho Control (Tabla 3.8) que habilita cambios (remover derechos) en otras filas (dominios) ver representación gráfica en la Tabla 3.9.

| Dominio \ Objeto | F(1) | D(1) | D(2) | D(3) |
|---|---|---|---|---|
| D(1) | Lectura | | Switch | Escritura |
| D(2) | Lectura | | | Switch Control |
| D(3) | Lectura/Escritura | Switch | | |

Tabla 3.8 Representación gráfica de la operación Control

| Objeto / Dominio | F(1) | D(1) | D(2) | D(3) |
|---|---|---|---|---|
| D(1) | Lectura | | Switch | |
| D(2) | Lectura | | | Switch<br>Control |
| D(3) | Lectura | Switch | | |

Tabla 3.9 La tabla anterior una vez aplicada la operación Control

D(2) puede cambiar el modo de acceso a F(1) de D(3) de Lectura/Escritura a Lectura.

Lo importante de esto es que con estos esquemas y los conceptos de objetos y capacidad, es posible crear un nuevo tipo de monitor, llamado "manager", que es usado para cada recurso, el cual planifica y controla el acceso a ese recurso. Cuando un proceso necesita un recurso, llama al manager, el cual le devuelve la capacidad para ese recurso. El proceso debe presentar la capacidad cuando usa el recurso. Cuando el proceso finaliza el uso del recurso le devuelve la capacidad al manager, quien lo asignara a otro proceso, de acuerdo al planificador (scheduler).

### 3.11 Revocación

En la Protección Dinámica es posible hacer una revocación de los accesos y podemos tener varias opciones:

- Inmediata/Postergada.
- Selectiva/General (para algunos usuarios, o para todos).
- Parcial/Total (todos los accesos a un objeto, o solo algunos).
- Temporario/Permanente (se podrá obtener nuevamente o no).

En la lista de accesos la revocación es fácil. Se busca la lista de accesos y se hacen los cambios, luego cualquier combinación anterior es posible.

En el esquema de Listas de Capacidad, la revocación es más difícil, pues las capacidades están distribuidas por todo el sistema, sin embargo, existen varios sistemas de revocación en Listas de Capacidad:

- **Readquisición.** Las capacidades son borradas periódicamente. Si un proceso intenta readquirirla, y la capacidad se revocó, NO puede hacerlo.

- **Back-pointers.** Una lista de apuntadores asocia a cada objeto con todas las capacidades asociadas. Siguiendo los apuntadores es posible cambiarlos. La implementación es general pero muy costosa.

- **Indirección.** Las capacidades no apuntan al objeto en forma directa, sino a una única entrada en una tabla global, la cual a su vez, apunta al objeto. La revocación se implementa buscando en la tabla global la entrada y borrándola. Puede ser reutilizada para otra capacidad. No se puede hacer revocación selectiva.

- **Llaves.** La revocación se hace cambiando la llave. Si un objeto tiene asociadas varias llaves es posible hacer la revocación selectiva.

Como se puede apreciar los mecanismos de protección y control del sistema se orientan básicamente a los siguientes aspectos: Errores, omisiones, cambios a los programas, seguridad lógica, validación de datos, reinicio y recuperación, manejo de errores, acceso a los programas, rutinas de control, etcétera.

Es mucho más fácil lograr la seguridad de un sistema si ésta se incluye en el diseño original del sistema en vez de hacer las adaptaciones posteriormente. Las medidas de seguridad deben ponerse en práctica en todo el sistema de cómputo. Si queremos desarrollar un sistema de alta seguridad es indispensable asegurar el núcleo (*Kernel*) del sistema operativo.

Las medidas de seguridad más vitales se ponen en práctica en el núcleo, el cual debe de mantenerse a propósito lo más pequeño posible. Esto hace más razonable la revisión cuidadosa del núcleo para detectar fallas y demostrar formalmente que esté correcto.

La seguridad de un Sistema Operativo depende sobre todo de asegurar las funciones que se encargan del control de acceso, las entradas al sistema y la supervisión, y que administran el almacenamiento real, el almacenamiento virtual y el sistema de archivos. Dichas funciones ocupan comunmente una buena parte del código del sistema operativo, de modo que es difícil lograr un núcleo pequeño.

### 3.12 Defectos Comunes en los Sistemas Operativos

Hacer que un sistema operativo sea absolutamente impenetrable es una tarea imposible, lo mejor que podemos esperar es hacer que el sistema sea altamente resistente a la penetración mediante mecanismos de protección, sin embargo, se han encontrado varios defectos comunes a muchos sistemas. Entre ellos están:

**Verificación de autenticidad**

En muchos sistemas, los usuarios no pueden determinar si el equipo y los programas son lo que deberían ser. Esto hace que un penetrador pueda reemplazar con facilidad un programa sin que el usuario se entere. Un usuario podría dar sin miramientos su contraseña a un programa falso de entrada al sistema.

**Cifrado**

La lista maestra de contraseñas debe almacenarse de manera que no pueda ser interpretada a simple vista, lo que se logra aplicando métodos criptográficos (Ver **Anexo 1. Criptográfia**).

**Realización**

Un diseño bien pensado para un mecanismo de seguridad puede llevarse a la práctica en forma inadecuada.

**Confianza implícita**

Es un problema muy común; una rutina supone que otra está funcionando correctamente, en vez de examinar con cuidado los parámetros suministrados por la otra.

**Compartimiento implícito**

El sistema puede depositar información vital del sistema en el espacio de direcciones de un usuario sin darse cuenta.

**Comunicación entre procesos**

El penetrador puede usar un mecanismo de transmisión/recepción para probar diversas posibilidades. Por ejemplo, el usuario no privilegiado, puede solicitar un recurso del sistema y suministrar una contraseña; la información de vuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el penetrador.

**Comprobación de legalidad**

El sistema quizá no verifique lo suficiente la validez de los parámetros del usuario.

**Desconexión de línea**

En sistemas de tiempo compartido y redes, cuando se pierde la línea (por cualquier motivo), el sistema operativo deberá clausurar de inmediato la sesión del usuario o ponerlo en un estado tal que sea necesaria una nueva autorización para poder volver a otorgar el control. Algunos sistemas dejan "flotar" un proceso después de un desconexión de línea, de esta manera un penetrador podría obtener control del proceso y utilizar los recursos a los cuales puede tener acceso dicho proceso.

**Descuido del operador**

Un penetrador puede engañar a un operador para que monte un disco de sistema operativo falso.

**Paso de parámetros por referencia en vez de por valor**

Es más seguro pasar parámetros directamente en registros y no hacer que los registros apunten a localidades donde están los parámetros. El paso por referencia puede conducir a una situación en la cual los parámetros siguen en el espacio de direcciones del usuario después de haberse realizado la verificación de autenticidad; así el usuario podría suministrar parámetros legítimos; hacer que sean verificados y después modificarlos justo antes de que los utilice el sistema.

**Contraseñas**

A menudo las contraseñas son fáciles de adivinar u obtener por medio de intentos repetidos.

**Trampas para el penetrador**

Los sistemas deben incluir mecanismos de trampas para atraer al intruso inexperto, lo que constituye una buena primera línea de detección. La mayor parte de los sistemas tienen mecanismos de trampa inadecuados.

**Privilegios**

En algunos sistemas, son demasiados los procesos con demasiados privilegios. Esto va contra el principio de menor privilegio.

**Confinamiento de programas**

Un programa prestado por otro usuario puede actuar como Caballo de Troya; podría robar o alterar los archivos de quien lo pidió prestado.

TESIS CON
FALLA DE ORIGEN

**Prohibición**

Muchas veces se indica a los usuarios que se abstengan de usar ciertas funciones porque los resultados pueden ser "indeterminados", sin embargo, dichas funciones siguen siendo accesibles para los usuarios.

**Residuo**

Muchas veces un penetrador puede encontrar una lista de contraseñas con sólo hurgar en las papeleras de reciclaje o cestos de basura. En ocasiones se dejan residuos en almacenamiento después de ejecutarse una rutina del sistema. La información confidencial siempre deberá reemplazarse o destruirse antes de liberar o desechar el medio (almacenamiento, papel, etcétera) que ocupa.

**Blindaje**

Una corriente en un alambre genera un campo magnético alrededor de éste; los penetradores pueden intervenir de hecho una línea de transmisión o un sistema de cómputo sin hacer contacto físico. El blindaje eléctrico puede servir para evitar esas "intrusiones invisibles".

**Valores de umbral**

El propósito de éstos es refrenar intentos repetidos de acceso al sistema. Después de cierto número de intentos de entrada no válidos, ese usuario (o el equipo desde el cual intenta entrar) deberá bloquearse, notificando al administrador del sistema.

### 3.13 Mecanismos de penetración a Sistemas Operativos

Aparte de los defectos en los sistemas operativos, también se deben tomar en cuenta ciertos mecanismos de penetración que se han usado con éxito, entre ellos contamos:

| **Asincronía** |
|---|
| Cuando varios procesos avanzan en forma asíncrona, es posible que un proceso modifique parámetros cuya validez ha sido verificada por otro, aun cuando este último no los haya usado; así un proceso puede pasar valores "malos" a otro aunque el segundo realice una verificación exhaustiva. |
| **Hojeo** |
| Un usuario revisa el sistema de cómputo intentando localizar información privilegiada. |
| **Entre líneas** |
| Se usa una terminal especial para intervenir una línea de comunicaciones empleada por un usuario inactivo que ya haya entrado en el sistema. |
| **Código clandestino** |
| Se instala un parche pretendiendo corregir un error en el sistema operativo; el código contiene agujeros, a través de los cuales se puede entrar posteriormente sin autorización. |
| **Rechazo de acceso** |
| Un usuario escribe un programa para hacer que se caiga el sistema, para ponerlo en un ciclo infinito o para monopolizar sus recursos. La intención en este caso es impedir que usuarios legítimos obtengan acceso o servicio. |
| **Introducción de procesos sincronizados** |
| Los procesos usan las primitivas de sincronización del sistema para compartir o pasar información entre ellos. |



TESIS CON
FALLA DE ORIGEN

| **Desconexión de línea** |
|---|
| El penetrador intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca que hubo una desconexión. |
| **Disfraz** |
| El penetrador asume la identidad de un usuario legítimo después de haber obtenido la identificación correcta por medios clandestinos. |
| **Ataque "NAK"** |
| Muchos sistemas permiten a un usuario interrumpir un proceso en ejecución, realizar otra operación y después continuar el proceso interrumpido. En algunos casos el penetrador puede "atrapar" al sistema en un estado no protegido y adueñarse con facilidad del control. |
| **Engaño del operador** |
| Un penetrador astuto a menudo puede engañar al operador del equipo para que realice una acción que ponga en peligro la seguridad del sistema. |
| **Parásito** |
| El penetrador utiliza una terminal especial para intervenir una línea de comunicación, logrando intervenir mensajes entre el usuario y el procesador y los modifica o los reemplaza por completo. |
| **Parámetros inesperados** |
| El penetrador suministra valores inesperados en una llamada al supervisor para aprovechar un punto débil en los mecanismos de verificación de legalidad del sistema. |

Tabla 3.10 Mecanismos de penetración a Sistemas Operativos

### 3.14 Seguridad por Hardware y Sistemas tolerantes a fallas

Una de las razones para diseñar sistemas de cómputo de alta seguridad es garantizar su disponibilidad y confiabilidad en todo momento. Sin embargo y como se pudo apreciar, el propio sistema operativo no puede proteger por completo al sistema de cómputo.

Al disminuir los costos en los equipos se hace cada vez más deseable incorporar algunas funciones del sistema operativo en el hardware. Este proceso es conocido como **SEGURIDAD POR HARDWARE** y esto tiene grandes ventajas respecto a la seguridad interna:

- La seguridad de estas funciones es mayor, ya que no están accesibles como las instrucciones de programa, que se pueden modificar fácilmente.
- Las funciones incorporadas en el equipo de cómputo se ejecutan mucho más rápido que en software.
- Diversas funciones de supervisión se pueden realizar con más frecuencia.

Una de sus aplicaciones son los **Sistemas tolerantes a fallas**. Estos son utilizados en sistemas donde se puede perder la información debido a un mal funcionamiento del sistema. Este aspecto es muy importante en los sistemas de control y supervisión en tiempo real. Un aspecto clave de la tolerancia a fallas es la **redundancia**. Si falla un componente, otro equivalente lo relevará. Algunos sistemas emplean mecanismos basados en redes de dos o más computadoras conectadas entre sí, de tal manera que, si alguna de ellas llega a fallar, pasará a modo inactivo y cualquiera de los otros equipos tomará el control.

La arquitectura de los microprocesadores ha evolucionado a diseños más confiables. Muchos de ellos usan estructuras de doble ducto para la comunicación. Es por ello que el multiprocesamiento es importante en cualquier sistema tolerante a fallas. Algunos de las características de la tolerancia a fallas son:



TESIS CON
FALLA DE ORIGEN

- Incorporación de los mecanismos a prueba de fallas en el equipo y no en los programas.
- El empleo de multiprocesamiento transparente; esto hace posible mejorar el desempeño sin tener que modificar los programas.
- Empleo de subsistemas múltiples de entrada/salida.
- Incorporación en el hardware de porciones importantes del sistema operativo.
- Incorporación de mecanismos de detección de fallas en el equipo y en los programas.

Los sistemas tolerantes a fallas ofrecen una degradación paulatina; cuando fallan componentes en un sistema de este tipo, se continúa dando servicio, pero a niveles reducidos. Los sistemas tolerantes a fallas están diseñados para poder desconectar un componente, repararlo y volverlo a conectar, todo mientras el sistema sigue dando servicio ininterrumpido.

## 4. PLAN DE SEGURIDAD

El número de amenazas a los entornos informáticos y de comunicaciones crece casi exponencialmente año tras año, alcanzando dimensiones inimaginables. Hoy en día la seguridad va más allá de lo que pueda ser un sistema de autenticación biométrico o una red de sensores de detección de intrusos; ya se contemplan aspectos que hasta hace poco se reservaban a entornos altamente cerrados, como bancos u organizaciones militares. Y es que ya se ha considerado imprescindible e importante contar con un plan de continuidad. Sin una política de seguridad correctamente implantada en una organización no sirven de nada los controles de acceso (físicos y lógicos).

Se habla ahora de la **gestión de la seguridad** como algo crítico para cualquier organización, igual de importante dentro de la misma que los sistemas de calidad o las líneas de producto que desarrolla.

En este punto se hablará de aspectos relacionados con la gestión de la seguridad corporativa, entendiendo por "corporativa", la aplicable a cualquier organización.

Para poder comenzar a gestionar la seguridad, el primer paso es la creación de un Plan de Seguridad. Un Plan de Seguridad es un documento que describe la forma en que una organización debe dirigir sus medidas de seguridad. Está sujeto a revisiones periódicas fijas, y revisiones de acuerdo a los cambios en las necesidades de seguridad. El plan de seguridad identifica y organiza las actividades de seguridad del sistema y contiene tanto la descripción de la situación actual, como un plan para los posibles cambios. Cualquier plan de seguridad debe contener ocho aspectos, que pueden ser aumentados de acuerdo al criterio del implementador, la Tabla 3.11 muestra un plan de seguridad tradicional.

| No. | Actividad | Situación Actual |
|---|---|---|
| 1 | Análisis de Riesgos | Proceso para determinar las exposiciones y los posibles puntos débiles. |
| 2 | Política de seguridad | Indicación de los objetivos del esfuerzo en seguridad informática y la voluntad del personal para trabajar para lograr estos objetivos. |
| 3 | Estado actual de la seguridad | Un panorama de cómo se maneja actualmente la seguridad dentro de la organización. |
| 4 | Recomendaciones | Pasos a seguir para lograr los objetivos de seguridad descritos anteriormente. |
| 5 | Responsabilidad de implementación | Una lista describiendo quién es responsable de cada actividad de seguridad. |
| 6 | Tabla de tiempos | Una tabla que describe cuándo se deben realizar las diferentes actividades de seguridad. |
| 7 | Atención continua | La indicación de una estructura de revisiones periódicas del plan de seguridad. |
| 8 | Aceptación del Plan | Presentación formal del plan. |

Tabla 3.11 Plan de Seguridad

A continuación se describirán formalmente cada uno de estos aspectos para tener una mejor compresión del tema.

### 4.1 Análisis de Riesgos

Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un **análisis de riesgos**, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre nuestra seguridad:

¿Qué queremos proteger?

¿Contra quién o qué lo queremos proteger?

¿Cómo lo queremos proteger?

Los pasos básicos que conforman un análisis de riesgos se describen a continuación:



TESIS CON
FALLA DE ORIGEN

### 4.1.1 Identificar los objetos valiosos.

Los activos deben clasificarse en distintas categorías tales como:

- **Hardware.** CPU's, tarjetas, teclados, monitores, terminales, estaciones de trabajo, unidades de cinta, impresoras, cables, conexiones, medios de comunicación, etcétera.
- **Software.** Programas fuente, programas ejecutables, programas comerciales (comprados), programas de utilidad, sistemas operativos, programas del sistema (compiladores), programas de mantenimiento y diagnóstico, etcétera.
- **Datos.** Durante la ejecución, datos almacenados, datos impresos, registros actualizados, registros de auditoría, etcétera.
- **Documentación.** De programas, del hardware, del sistema, de los procedimientos de administración, del sistema completo.
- **Consumibles.** Papeles, formularios, cintas, medios magnéticos y ópticos, cartuchos de toner, etcétera.

El análisis de riesgos comienza con la lista de todos los activos específicos del sistema. De alguna manera es un extensión del inventario del sistema ya que incluye elementos intangibles como los datos o las personas.

### 4.1.2 Determinar las vulnerabilidades.

Este paso requiere de imaginación con objeto de predecir que daños pueden sufrir estos activos y de donde proceden. Los tres objetivos de la seguridad son asegurar el secreto, la integridad y la disponibilidad. Una vulnerabilidad es cualquier situación que pueda dañar alguna de estas tres características y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad. Para que este punto sea más fácil de entender se comenzará por dividir las amenazas a los activos en tres grandes grupos, de acuerdo a la Tabla 3.12.

| | | |
|---|---|---|
| **Desastres del entorno** | En este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno informático o de la propia organización, así como con las personas que de una u otra manera están relacionadas con él. | Temblores, inundaciones, cortes eléctricos, peligros relacionados con operadores, programadores o usuarios del sistema. |
| **Amenazas en el sistema** | Se contemplan todas las vulnerabilidades de los equipos y su software que puedan acarrear amenazas a la seguridad. | Fallas en el sistema operativo, medidas de protección del mismo sistema operativo, fallas en los programas, copias de seguridad. |
| **Amenazas en la red** | Las amenazas que trae consigo el comunicar equipos mediante redes locales, Intranets o la propia Internet. | Cifrado de datos en tránsito por la red, proteger una red local del resto de Internet, instalación de sistemas de autenticación de usuarios remotos. |

Tabla 3.12 Amenazas a los activos

Se puede utilizar un diagrama como el mostrado en la Tabla 3.13 para organizar la consideración de amenazas y activos.

Las posibles vulnerabilidades pueden identificarse considerando las situaciones que podrían causar pérdida de secreto, de integridad o disponibilidad de un objeto particular. La tabla da una idea general de lo que le puede ocurrir a cada uno de los activos del sistema.

| ACTIVOS | SECRETO | INTEGRIDAD | DISPONIBILIDAD |
|---|---|---|---|
| **Hardware** | | Sobrecarga Destrucción maliciosa o no Daño | Falla, robo, destrucción, disponible |
| **Software** | Robado, copiado | Modificado dañado, Amenazas lógicas | Borrado, destruido |
| **Datos** | Revelado, accedido intrusos, interferido | dañado error, error de software, error de error de usuario | Borrado, destruido |
| **Personas** | | | salida, término, vacaciones, |
| **Documentación** | | | perdida, destruida |
| **Consumibles** | | | perdida, destruida |

Tabla 3.13 Consideración de amenazas y activos

### 4.1.3 Estimar la probabilidad de explotación.

Es el tercer paso del análisis de riesgo y determina la frecuencia con que cada activo puede ser explotado. La probabilidad de ocurrencia está relacionada con la severidad de los controles existentes y con la probabilidad de que alguien o algo pueda evadir estos controles. Existen varias formas de calcular esta probabilidad, aquí se mencionarán algunas de ellas:

- **A partir de los datos observados de la población general.** Las compañías de seguros tienen coleccionados una gran cantidad de datos a partir de los cuales se puede predecir anualmente el número de siniestros a ocurrir en n casas y con x pérdidas. Asimismo, los fabricantes tienen los datos referentes al tiempo de vida de los productos que fabrican.

- **A partir de los datos observados en un sistema específico.** Los sistemas operativos pueden llevar registro de las fallas de hardware, de los intentos fallidos de entrada al sistema, del número de accesos, etcétera.

- **Estimar el número de ocurrencias en un período determinado.** En este caso el analista trata de determinar el número de veces aproximado que un evento particular ocurrió en el año anterior, por ejemplo.

TESIS CON
FALLA DE ORIGEN

- **Estimar la probabilidad desde una tabla.** El analista estima la probabilidad de ocurrencia de un evento, eligiendo uno de los rangos de la Tabla 3.14. Lo completo de este análisis depende de la experiencia del analista.

| Frecuencia | Relación |
|---|---|
| Más de una vez al día | 10 |
| Una vez al día | 9 |
| Una vez cada tres días | 8 |
| Una vez cada semana | 7 |
| Una vez cada dos semanas | 6 |
| Una vez al mes | 5 |
| Una vez cada cuatro meses | 4 |
| Una vez al año | 3 |
| Una vez cada tres años | 2 |

Tabla 3.14 Probabilidad de ocurrencia de un evento

- **Aproximación Delphi.** Varios clasificadores estiman de forma individual la probabilidad de un evento. Las estimaciones se coleccionan, reproducen y se distribuyen a todos los clasificadores, los cuales pueden modificar las predicciones iniciales en base a las estimaciones de los demás. Si los valores de las estimaciones son inconsistentes los clasificadores deben reunirse para encontrar la razón de esta inconsistencia y tratar de seleccionar el valor final de la estimación.

### 4.1.4 Calcular la pérdida esperada anual.

El siguiente paso es determinar el costo de cada incidente. Algunos costos como el de reemplazar algún elemento del hardware e incluso de reemplazar algún elemento del software puede ser aproximado a partir del costo inicial. Sin embargo el costo de disponibilidad de un recurso de hardware o software , o el costo de la falta de unos datos es sustancialmente más complicado de medir. Aún cuando sea difícil hacer las estimaciones de estos costos es necesario hacerlo. Las estimaciones realistas de los daños potenciales están relacionadas con la seguridad informática, y ayudan a identificar las áreas que merecen atención especial.

Una vez estimados los daños que produce un incidente, este costo debe ser multiplicado por el número de incidentes esperados por año, para obtener así, la estimación de las pérdidas anuales (PEA, Pérdida Esperada Anual). Evidentemente los recursos que presenten un riesgo evaluado mayor son los que deberán tener más controles, ya que al ser atacados, el ataque causará pérdidas importantes.

### 4.1.5 Derivar los controles aplicables y sus costos.

Una vez realizados los pasos anteriores, se puede tener la siguiente situación. Si la PEA es inaceptablemente alta, se debe investigar la posibilidad de instalar nuevos controles. Una forma de identificar los controles adicionales en base a la exposición. Por ejemplo, el riesgo de la pérdida de información puede ser cubierta por:

- Realización de respaldos periódicos.
- Utilización de dispositivos de almacenamiento duplicados.
- Controles de acceso para prevenir el borrado no autorizado.
- Seguridad física para evitar que alguien entre al sitio (*site*) y dañe los discos con la información.
- Programas estándar que limitan el efecto de los programas en la información.

Se debe considerar la efectividad de cada uno de estos controles. Para identificar los controles a aplicar en una exposición determinada, se debe pensar en todos los aspectos de la seguridad y seleccionar los controles que cubran las exposiciones.

### 4.1.6 Proyectar los costos anuales de los controles.

Básicamente consiste en calcular el costo de implementar cada control. El cálculo de esto no debe ser complejo si conocemos las posibles medidas de prevención que tenemos a nuestra disposición. Se debe calcular el costo real de implementar los controles. El costo efectivo es el costo del control menos cualquier reducción en la PEA que implique dicho control; por tanto, el costo puede ser negativo si la reducción del riesgo es mayor que el costo del control.

Por ejemplo. Si se supone que un departamento ha tenido problemas con los accesos no autorizados al sistema. Se sabe que los intrusos han accedido al sistema, y han conseguido interceptar e incluso modificar datos importantes. Un posible control a esta amenaza es instalar un programa de control de acceso (software) más seguro. Aunque el costo de dicho programa es alto ($250,000 pesos), se puede justificar su compra con base en la siguiente Tabla 3.15.

| Elemento | | Costos |
|---|---|---|
| Riesgos: | pérdida de datos confidenciales de la empresa<br>cálculos basados en datos incorrectos<br>costo de la reconstrucción de los datos<br>10,000,000 pesos<br>10% de probabilidad anual | 1000,000 |
| Efectividad del control (software): 60% | | -600,000 |
| Costo del software de control de accesos | | 250,000 |
| PEA(1000,000-600,000+250,000) | | 650,000 |
| Costos anuales (1000,000-650,000) | | 350,000 |

Tabla 3.15 Proyección de los costos anuales de controles

Después de repasar cada uno de los pasos básicos del análisis de riesgos, es importante destacar los beneficios que proporciona realizarlos:

- Mejorar el conocimiento.
- Identificar los factores importantes, las vulnerabilidades y los controles.
- Proporcionar las bases para la toma de decisiones.
- Justificar la inversión en seguridad.

Además las discusiones que se realizan durante el análisis de riesgos puede incrementar el conocimiento general de la necesidad de medidas de seguridad y es parte fundamental de un plan general de seguridad.

## 4.2 Política de seguridad

El término **política de seguridad** se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general de dicho sistema. Al tratarse de "términos generales", aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de que es lo permitido y lo denegado en cierta parte de la operación del sistema, lo que se denomina **política de aplicación específica**. Una política de seguridad puede ser:

- **Prohibitiva**, si todo lo que no está expresamente permitido está denegado.
- **Permisiva**, si todo lo que no está expresamente prohibido está permitido.

Evidentemente la primera aproximación es mucho mejor que la segunda si se quiere mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y las no contempladas serían consideradas ilegales.

Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema informático:

- **Disponibilidad.** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Utilidad.** Los recursos del sistema y la información manejada en el mismo debe de ser útil para alguna función.
- **Integridad.** La información del sistema debe de estar disponible tal y como se almacenó por un agente autorizado.
- **Autenticidad.** El sistema debe ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- **Confidencialidad.** La información sólo debe estar disponible para agentes autorizados, especialmente su propietario.
- **Posesión.** Los propietarios de un sistema deben ser capaces de controlarlo en todo momento; perder este control a favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores y con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados **normativas** (también llamados Políticas, Estándares o Procedimientos Operativos) que se describen a continuación:

- **Seguridad Organizacional.** Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, *outsourcing*, estructura del área de seguridad).

- **Clasificación y control de activos.** Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.

- **Seguridad del Personal.** Formación en materia de seguridad, claúsulas de confidencialidad, reporte de incidentes, monitoreo de personal, etcétera.

- **Seguridad física y del entorno.** Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos (incluso humanos) de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.

- **Gestión de comunicaciones y operaciones.** Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la protección frente a malware, la gestión de copias de seguridad o el intercambio de software dentro de la organización.

- **Controles de acceso.** Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitoreo de accesos, etcétera.

- **Desarrollo y mantenimiento de sistemas.** Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de software, etcétera.

- **Gestión de continuidad de negocio.** Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.

- **Requisitos legales.** Evidentemente, una política debe de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de cifrado. Junto a todos los aspectos relacionados con registros de eventos en los recursos (*logs*) y su mantenimiento.

Mientras más precisa sea la definición de políticas, más sencilla será su interpretación e implementación.

### 4.3 Estado Actual de la seguridad

La base para la descripción actual de la seguridad suele ser el análisis de riesgos. El estado actual debe contener una lista de los activos de la organización, las amenazas de seguridad a dichos activos, y los controles para protegerlos.

El plan debe especificar como se guardan los datos, cuantas evaluaciones se realizan, y que suposiciones se hacen. Una de las partes más complejas es la valoración de los activos y de la probabilidad de fallas en la seguridad, que en algunos casos, están basados en datos actuales tales como: el costo de adquisición del hardware y del software, los salarios de las personas que deben reconstruir los datos perdidos, etc. En otros casos, la estimación se deriva a partir de una tabla de rangos de valores. Dado que estas dos aproximaciones afectan a la precisión de los resultados, su uso debe describirse en el análisis de la situación actual.

Finalmente, el plan debe presentar un procedimiento para situar las vulnerabilidades que no hayan sido consideradas. Dichas vulnerabilidades pueden provenir de la adquisición de nuevos equipos, de nuevos datos y de situaciones nuevas, o incluso de la falta de seguimiento de los planes de seguridad. Si alguien identifica una vulnerabilidad importante, debe estar instruido para integrar dicha vulnerabilidad en los procedimientos de seguridad existentes.

### 4.4 Recomendaciones

Un análisis de riesgos exhaustivo identifica las exposiciones con mayor pérdida potencial, las exposiciones de mayor pérdida esperada, los controles que proporcionan la mejor relación total, y los controles que proporcionan la mejor relación por peso invertido. Estos cuatro resultados son útiles al decidir que áreas requieren controles y al justificar la localización de fondos para las diferentes necesidades de seguridad.

Después de identificar las áreas de mayor riesgo y de mayor potencial de ahorro, el informe de seguridad debe recomendar los controles apropiados. Estos controles deben ordenarse según su deseabilidad (los que cubren más exposiciones o los que proporcionan los mejores resultados según la inversión). También se deben enunciar los costos totales y los gastos que implican los controles.

Si el precio del control necesario es excesivo o los riesgos son insignificantes, entonces las vulnerabilidades no son cubiertas. El plan de seguridad debe identificar estos riesgos no cubiertos y explicar por qué se ha optado por ello. El plan también debe describir las acciones de recuperación que se llevarán a cabo en caso de "explotación" de alguno de estos riesgos.

### 4.5 Responsabilidad de Implementación

Una de las secciones del plan debe identificar a las personas responsables de la implementación. De esta manera, cada persona comprenderá su función, y los individuos que compartan alguna responsabilidad, sabrán que deben coordinarse. Al establecer un registro, no será fácil que las personas evadan sus responsabilidades. A continuación se listan algunos ejemplos de grupos de responsabilidad en la seguridad:

- **Usuarios de computadoras;** cada uno será responsable de su propia computadora o bien existirá un coordinador de la seguridad en los equipos de cómputo.
- **Administradores de bases de datos;** pueden ser responsables del acceso y de la integridad de los datos que residen en las bases.
- **Encargados de Información;** se nombran en algunas organizaciones para observar la creación y uso de los datos, estos encargados serán responsables de la retención y borrado propio de los datos.
- **Miembros del personal directivo;** pueden ser responsables de la seguridad que involucra a los empleados, tal como investigar a los empleados, verificar su procedencia y organizar la distribución de programas a empleados y organización del entrenamiento (en caso de requerirse).

### 4.6 Tabla de tiempos

Debido a que los controles son costosos o bien, implican cierta complicación técnica, pueden ser adquiridos e implementados de manera gradual. De forma similar, los controles que implican

procedimientos pueden involucrar entrenamiento del personal, con el fin de que todos conozcan y acepten las razones por las que se está implementando el control.

El plan debe especificar el orden de implementación de los controles, asegurándose de que se cubran en primer lugar las exposiciones más serias. La Tabla de Tiempos también permite medir el avance del programa de seguridad.

### 4.7 Atención Continua

Una parte importante de la Tabla de Tiempos es el establecimiento de fechas para la revisión y evaluación del estado de la seguridad. A medida que cambian los usuarios, los datos y el equipo de cómputo y comunicaciones, se desarrollan nuevas exposiciones y los controles van siendo obsoletos e ineficientes. Se debe actualizar periódicamente el inventario de activos del sistema y la lista de controles, asimismo, el análisis de riesgos debe ser revisado. El plan de seguridad debe incluir la fecha de estas revisiones periódicas.

Queda una pregunta en el aire ¿Quién debe realizar el análisis y recomendar el plan de seguridad?.

Como cualquier otra función complicada, lo mejor es que esto lo realice una comisión. El tamaño de la comisión depende del tamaño y complejidad de la organización y del grado de compromiso con la seguridad.

El equipo de elaboración del plan de seguridad debe estar integrado por representantes relacionados con los diferentes aspectos de la seguridad informática. Se deben considerar a las personas de los siguientes grupos como ayuda en la planificación de la seguridad:

- Grupo de hardware.
- Programadores del sistema (Cifrado, protocolos, seguridad del Sistema Operativo y redes).
- Programadores de aplicaciones (Recomendaciones de medidas de seguridad de los programas).
- Capturistas y operadores.
- Personal de seguridad física (Controles de seguridad física contra ataques humanos y desastres naturales).
- Representantes de los usuarios (En vista de que los controles afectan a los usuarios del sistema. El plan debe abarcar los puntos de vista de los usuarios en cuanto a de los controles).

### 4.8 Aceptación del Plan de Seguridad

Una vez que se ha escrito el plan de seguridad, éste debe ser aceptado y las recomendaciones deben ejecutarse. La aceptación del plan de seguridad depende de la sensibilidad, entendimiento y compromiso de los gestores.

La explicación y la publicidad serán de gran ayuda para que se entienda y acepte el plan. Esto es muy importante debido a que las personas, sólo usarán los controles si entienden su necesidad y aceptan la importancia de los controles recomendados. Si los usuarios piensan que los controles no tienen sentido, intentarán evitarlos y trabajarán de forma habitual.

La otra clave del éxito es el compromiso de la gestión, la cual se consigue a través del entendimiento (conocimiento de las causas y los efectos potenciales de las fallas en la seguridad), de la efectividad de los costos y de la presentación del plan.

La presentación del plan es un aspecto muy importante, ya que algunos directivos no entienden los términos técnicos, por lo que el plan se debe explicar evitando la jerga informática, de tal manera que los directivos en verdad tomen conciencia y aprecien la seguridad informática.

Asimismo, existen directivos que se resisten a destinar fondos para la instalación de controles, por ello es importante presentar el plan aplicado a actividades diarias de la empresa para ayudar a que se entienda la necesidad de los controles.

Por último, el plan debe ser presentado mediante un informe bien organizado que incluya un plan de implementación. Las secciones del plan que detallan los aspectos contables, el tiempo de desarrollo y la revalorización continua son especialmente importantes.

## 5. EVALUACIÓN DE SISTEMAS SEGUROS

La elección de un producto de seguridad plantea el problema de medir el nivel de seguridad proporcionado por el producto. Aunque no es fácil imaginar como medir un concepto aparentemente tan poco formalizable como la seguridad, el interés sobre el tema ha hecho que desde 1983 ya se publicara un primer trabajo sobre la materia y que constituyó la primera norma en su género a nivel mundial.

### 5.1 Criterios de Evaluación Estadounidenses

La primera institución que asumió la responsabilidad de desarrollar normas de evaluación de la seguridad de los sistemas operativos, fue la *National Security Agency* (Agencia Nacional de Seguridad) dependiente de Departamento de Defensa de E.U., quien a través de su centro especializado, el Centro Nacional de Seguridad de Computadoras (NCSC, *National Computer Security Center*) , publicó en 1985 los Criterios de Evaluación Confiables de Seguridad de Computadoras (*TCSEC, Trusted Computer Security Evaluation Criteria*) , mejor conocido como Libro Naranja. En él se especifican distintos criterios de seguridad de hardware, de firmware y de software de base, así como las metodologías de evaluación de dichos sistemas operativos respecto a su seguridad. Los criterios citados fueron desarrollados para satisfacer tres propósitos:

- Suministrar normas de seguridad a los fabricantes.
- Proporcionar métricas con las cuales evaluar y clasificar los sistemas informáticos.
- Promover requisitos de seguridad para ser incorporados en las especificaciones de adquisición de sistemas.

Los requisitos de seguridad que se describen en el libro naranja se pueden dividir en dos tipos:

- **Requisitos de implementación**: hacen referencia a las funciones específicas de seguridad que deben incorporar los sistemas de información (política de seguridad, etiquetado de objetos, identificación de usuarios y auditoría).

- **Requisitos de adecuación**: tratan de garantizar que los requisitos de implementación están presentes y trabajan correctamente.

El TCSEC establece el concepto de **monitor de referencia**, como responsable de autorizar las relaciones de acceso permitidas entre sujetos y objetos. La implementación de este concepto se denomina mecanismo de validación de referencias. Para este mecanismo el TCSEC requiere:

- Que sea resistente a ataques.
- Que haga la mediación en todos los intentos de acceso.
- Que sea lo suficientemente pequeño para poder ser analizado y probado.

Un sistema diseñado y realizado para verificar estos criterios, se dice que implementa un **núcleo de seguridad.** Tales sistemas alcanzan los mayores niveles de seguridad.

Muchos sistemas implementan el mecanismo de validación de referencias como parte de un mecanismo más general (por ejemplo, todo el sistema operativo) por lo que no satisfacen el último de los requisitos anteriores. Para comprender a éstos que son la mayoría, el TCSEC define el *Trusted Computing Base* (TCB, Base de Cómputo Confiable) como aquella parte del sistema que contiene todos los elementos responsables de la seguridad.

### 5.1.1 Clasificación de los criterios

En el libro naranja, los criterios de evaluación están jerarquizados en cuatro divisiones: D, C, B y A, donde A está reservada para los sistemas con medidas de seguridad más rigurosas. Cada división supone una mejora respecto a la anterior.

#### DIVISÓN D: Protección mínima

Se otorga a aquellos sistemas que tras su evaluación, no satisfacen los requisitos de alguna clase superior. Por tanto no tiene requisitos.

No se ha evaluado hasta la fecha ningún sistema de esta clase, pues ningún vendedor quiere asumir el costo elevado de valorar un sistema que no posea un conjunto razonable de características de seguridad. **Dentro de esta categoría se encontrarían las computadoras bajo MS-DOS, Macintosh, Amiga, etcétera.**

#### DIVISION C: Protección discrecional

Las clases en esta división suministran protección discrecional e incluyen capacidades de auditoría de los sujetos y de las acciones que éstos inician. Dentro de esta clase se encuentran las siguientes divisiones:

**Clase C1. Protección mediante seguridad discrecional**

El TCB satisface los requisitos de seguridad discrecional mediante la separación de usuarios y datos, incorpora algunas formas de control capaces de reforzar las limitaciones de acceso, de modo que un usuario pueda proteger sus propios datos.

El sistema debe tener un dominio, que incluya al TCB, protegido contra agresiones. El sistema utiliza contraseñas para la identificación de usuarios. La arquitectura del equipo permite la protección del sistema.

**Casi todas las instalaciones UNIX previas al System V Release 4 pertenecen a esta clase.**



TESIS CON
FALLA DE ORIGEN

**Clase C2. Protección mediante control de accesos**

Incorpora a la clase anterior herramientas que permiten auditar los accesos (o intentos) a cada objeto, los acontecimientos relevantes para efectos de seguridad, el aislamiento de recursos, los procedimientos de entrada al sistema, etcétera, además elimina la exposición a los residuos (datos que permanecen en la memoria principal o secundaria) tras la conclusión de los procesos.

**La mayor parte de los sistemas UNIX pertenecen a esta clase (HP-UX, IBM AIX, SCO-Unix, Sun Solaris, etcétera).**

## DIVISÓN B: Protección Obligatoria

Las funciones especificas de seguridad preservan la integridad de las etiquetas de los objetos sensibles, y las usa en conjunción con las reglas de control de acceso, para llevar a cabo la política correspondiente no discrecional u obligatoria. Consta de las siguientes clases:

**Clase B1: Protección mediante etiquetas.**

En primer lugar, se requieren todas las características de la clase C2. Además debe haberse establecido un modelo de seguridad informal de etiquetado de datos y de control de accesos.

Cualquier falla detectada en la seguridad debe ser eliminada y se deberá volver a revisar el sistema para asegurar que no se ha producido una nueva vulnerabilidad en la seguridad.

**El sistema AT&T System V/MLS y el sistema OSF/1 pertenecen a esta clase.**

**Clase B2. Protección estructurada**

El TCB debe estar documentado y diseñado a partir de un modelo de seguridad formal, revisado y probado, que requiera que el control de accesos se extienda a todos los objetos y sujetos del sistema. También debe comprobarse que la implantación se ajusta fielmente al modelo.

Asimismo, los canales ocultos deben ser identificados y los mecanismos de autenticación deben ser reforzados.

El TCB debe estar constituido por módulos independientes y construido mediante el principio del menor privilegio. Además debe ejecutarse un dominio de protección a salvo de ataques y modificaciones maliciosas.

**Pertenecen a esta clase los sistemas Trusted XENIX y USL SVR4 Enhanced Security.**

TESIS CON
FALLA DE ORIGEN

### Clase B3: Dominios de seguridad

El conjunto de funciones de seguridad debe controlar todos los accesos a sujetos y objetos, y debe ser lo suficientemente pequeño para poder analizarlo y probarlo. Debe excluir líneas de código que no sean esenciales para implantar la política de seguridad. Esta clase exige un administrador de seguridad. Además los mecanismos de auditoría deben ser empleados para señalar acontecimientos relevantes que afecten a la seguridad. También se requieren procedimientos de recuperación. El sistema debe ser altamente resistente a la penetración e identificar la inminencia de una violación de la seguridad.

A partir de esta clase no existen sistema operativos evaluados que hayan cumplido las especificaciones.

## DIVISÓN A: Protección Verificada

Se caracteriza por el uso de métodos formales de verificación para asegurar que los controles protegen efectivamente la información sensible procesada por el sistema.

Requiere una exhaustiva documentación para demostrar que el TCB satisface todos los requisitos de seguridad de esta división, tanto en su diseño como desarrollo e implementación. Consta de las siguientes divisiones:

### División A1: Diseño verificado

Es funcionalmente equivalente al B3. La diferencia proviene de la incorporación de especificaciones de diseño y técnicas de verificación formales, que garanticen que las funciones de seguridad han sido correctamente implantadas. Existen cinco criterios importantes para la certificación de esta clase:

- Debe existir un modelo de política de seguridad bien documentado. La documentación debe incluir las demostraciones matemáticas de que el modelo es consistente con los axiomas, y suficiente para soportar la política de control de accesos que se ha marcado.
- Debe existir una especificación formal de alto nivel del sistema de protección.
- Se debe demostrar que la especificación anterior corresponde con el modelo.
- Debe demostrarse que la implantación del TCB es consistente con la especificación aludida.
- Deben emplearse técnicas formales de análisis para identificar canales ocultos.

Partiendo del libro naranja el NCSC ha ido tomando otras iniciativas, como parte de una estrategia global cuya tendencia es promover la mayor aceptación general posible de los criterios (que sólo obligan a departamentos gubernamentales). Por ello, se ha ampliado su ámbito de aplicación a bases de datos, redes, etcétera.

TESIS CON
FALLA DE ORIGEN

Así, el NCSC ha promovido la "Serie Arco Iris", sucesión de documentos que pretenden evaluar otros sistemas de información. Dentro de esta serie encontramos los siguientes:

**El libro amarillo**, que proporciona directrices para medir el nivel adecuado de seguridad en instalaciones informáticas específicas.

**El libro verde** (*Password Management Guideline*, Guía del manejo de contraseñas), que contiene guías para la elección de contraseñas, almacenamiento de las mismas, responsabilidades de los usuarios y administradores.

**Trusted Network Interpretation of TCSEC** (Interpretación de redes seguras del TCSEC) que trata sobre la seguridad en redes.

**Trusted Database Management System Interpretation of TCSEC** (Interpetación del sistema de manejo de bases de datos confiables del TCSEC), que trata sobre la seguridad en Bases de Datos. Bajo este criterio se han evaluado cuatro bases de datos certificadas con la clase B1: Trusted Oracle V.7 de Oracle Corp.; Online/Sec 4.1 de Informix; Secure SQL Server de Sybase y RDB V.4.1 de DEC.

### 5.1.2 Lista de Productos Evaluados

Para instrumentar el proceso de evaluación, el NCSC inició el "Programa de Evaluación de Productos Fiables". Este programa establece las condiciones bajo las cuales los fabricantes pueden someter sus sistemas operativos a evaluación, para obtener el nivel de seguridad correspondiente.

El proceso de certificación es usualmente complejo y largo (entre 2 y 3 años), lo que constituye una de las críticas más incuestionables al libro naranja. Trimestralmente se publica el Catálogo de Servicios y Productos de seguridad de Sistemas de Información, que contiene la Lista de Productos Evaluados, que contiene todos los sistemas certificados por el NCSC junto con el nivel obtenido después de la evaluación. Son ya numerosos los sistemas operativos comerciales que se han certificado; casi todos en la clase C2, aunque un número creciente se encuentra en las clases B1 y B2. A partir del nivel B3 no se han evaluado Sistema Operativos que hayan cumplido con las especificaciones, dichos resultados se reflejan en la Tabla 3.16.

| Nivel de Seguridad | Productos Certificados |
|---|---|
| C2 | Netware 4.0 de Novell |
| B1 | MVS/ESA con RACF de IBM<br>OS2200 Trusted Environment de Unisys<br>HP-UX BLS de Hewlett-Packard<br>USTS/MLS R.4 de Amdahl<br>Securics de Bull |
| B2 | UnixWare/SV R4.2 Enhanced Security de Novell |

Tabla 3.16 Productos Certificados



TESIS CON
FALLA DE ORIGEN

## 5.2 Criterios de Evaluación Europeos

Por su parte los europeos han hecho lo suyo a este respecto. Alemania, Francia, Gran Bretaña y los países bajos, bajo el patrocinio de la Comisión Europea, presentaron en septiembre de 1990 un borrador de criterios de evaluación de la seguridad informática, bajo el nombre de ITSEC (*Information Technology Security Evaluation Criteria*, Criterios de evalución de seguridad en Tecnología de Información) versión 1.0, posteriormente, en junio de 1991 apareció la versión 1.2. En realidad el ITSEC constituye una conjunción de diferentes normas en vigor en Alemania, Francia y Gran Bretaña. Fundamentalmente las ZS11 y ZS12, emanadas del Zentralstelle für Sicherheit in der Informationstechnik de Alemania.

En el ITSEC se definen los productos de T.I. (Tecnologías de Información) como aquellos equipos físicos o paquetes de programas que pueden trabajar en una diversidad de entornos. Por otra parte, los sistemas de T.I. son aquellos diseñados y construidos para las necesidades de un usuarios específico y funcionan en un entorno concreto. Además, con una visión mucho más actual, la seguridad de las T.I. se hace sinónima de confidencialidad, integridad y disponibilidad.

El ITSEC define diez clases de funciones de seguridad (funcionalidades). Las cinco primeras F-C1; F-C2; F-B1; F-B2; F-B3, están ordenadas jerárquicamente y coinciden con los cinco niveles de C1 a A1 definidos en el libro naranja. Sin embargo, las cinco últimas clases, F-IN a F-DX, no están jerarquizadas y se encuentran orientadas a aplicaciones, en vez de ser independientes como las primeras. Los objetivos de estas clases, tal como aparecen en el ITSEC, son:

- **F-IN:** Dirigida a sistemas con elevados requisitos de integridad de datos y programas.
- **F-AV:** Dirigida a sistemas con elevados requisitos de disponibilidad, ya sea del sistema en conjunto o de funciones especiales del mismo.
- **F-DI:** Establece elevados requisitos de seguridad para la protección de la integridad de datos durante el intercambio de los mismos.
- **F-DL:** Se establece para sistemas con alta demanda de confidencialidad de datos durante el intercambio de los mismos.
- **F-DX:** Esta clase se postula para redes con elevadas necesidades de confidencialidad e integridad de la información durante el intercambio de datos.

Un producto o sistema de T.I. que se quiere evaluar se denomina TOE (*Target of Evaluation*, Objeto de evaluación) y se llama patrocinador al que ofrece este TOE (generalmente el fabricante). El evaluador revisa el TOE y compara los resultados con el objetivo de seguridad propuesto por el patrocinador, emitiendo, si es el caso, el certificado correspondiente.

Son cuatro las partes directamente concernidas en la ejecución del proceso de evaluación: el patrocinador de la evaluación, los desarrolladores del producto o sistema de T.I., los laboratorios de evaluación (ITSEF) y el organismo nacional de certificación.

Son tres la etapas que debe seguir un laboratorio durante la evaluación: preparación, realización y elaboración de conclusiones:

- El primer paso incluye la discusión inicial entre el patrocinador y el laboratorio; el estudio de viabilidad y, en caso de ser positivo, la lista de materiales y documentos a entregar por el patrocinador y el programa detallado de trabajo. Como conclusión se firmará el contrato entre el patrocinador y el laboratorio.

- La segunda etapa, la más importante y laboriosa del proceso, comprende un estudio detallado del TOE (diseño de la arquitectura, diseño detallado, implementación) y de sus vulnerabilidades, realización de pruebas de penetración, etcétera.

- Finalmente, se concluye con la elaboración de un Informe Técnico de Evaluación, que es remitido al patrocinador y al organismo nacional de certificación para que este certifique el producto o sistema.

El proceso de evaluación está guiado por cuatro principios básicos:

- Las evaluaciones no deben tener sesgos que conduzcan a una conclusión predeterminada.

- La objetividad se logra si los resultados se obtienen de pruebas incuestionables, no afectadas por opiniones o por el parecer de los evaluadores.

- La evaluación es repetible, si una nueva evaluación del mismo TOE con el mismo laboratorio, conduce a las mismas conclusiones.

- La reproducibilidad implica que una nueva evaluación de un TOE con el mismo objetivo de seguridad pero en un laboratorio distinto al que hizo la anterior, obtiene los mismos resultados.

Hasta el momento sólo tres países europeos, Gran Bretaña, Alemania y Francia tienen completado su esquema nacional de conformidad con la norma europea, incluyendo el consiguiente organismo certificador (en ambos casos, gubernamental).

Hasta 1990 las especificaciones de seguridad de las computadoras gubernamentales estadounidenses que procesan información no clasificada, eran competencia del NCSC. Sin embargo ese mismo año, se transfirió la responsabilidad de establecer tales especificaciones a otro organismo también gubernamental, el NIST (*National Institute of Standard and Technology*, Instituto Nacional de Estándares y Tecnología), dependiente del ministerio de comercio.

El NIST está desarrollando un nuevo conjunto de normas de evaluación de la seguridad para reemplazar a las ya obsoletas contenidas en el llamado "Libro Naranja".

El nuevo estándar está tomando muy en consideración los trabajos sobre seguridad que han realizado los europeos (ITSEC e ITSEM) y los canadienses (TCPEC). Así, los criterios estadounidenses separarán los requisitos de funcionalidad (lo que se supone que hace el producto o sistema) de los requisitos de corrección y efectividad (la efectividad con que funciona el producto y la confianza que se tienen en que hará lo que ya estaba previsto).

Estos criterios ya no se centran en la confidencialidad, sino que trata de atender a los usuarios de entornos comerciales, también preocupados por la integridad y disponibilidad. Las especificaciones básicas de seguridad que se están desarrollando describen como se supone que trabaja un sistema operativo, como determinar si es fiable y cuál es la lógica de su uso (el nivel de seguridad del entorno en el que va a trabajar, las amenazas que debe contrarrestar y las políticas de seguridad que deben ponerse en práctica). Todo este conjunto de características de seguridad se conocen como perfiles de seguridad.

Naturalmente la importancia del tema no podía dejar indiferente a la Organización Internacional de Normas (*ISO, International Organization of Standard*), que desde 1990 comenzó a elaborar criterios de evaluación para su uso generalizado.

Finalmente, cabe destacar que los organismos responsables de los anteriores trabajos, de la Unión Europea, Estados Unidos y Canadá, han aunado esfuerzos para homologar criterios y establecer un

criterio único (*Common Criteria*). El propósito es evitar diferencias conceptuales y técnicas, para después de haber probado el resultado, elevarlo a ISO como una aportación a este esfuerzo común de dotar al mercado global de las Tecnologías de Información con un estándar que sea aceptado y asumido por todos.

### 5.3 *Common Criteria* (Criterios Comunes)

En Junio de 1993, las organizaciones que patrocinaban los criterios europeos, canadienses y norteamericanos, comenzaron el "Proyecto CC" con el fin de reemplazar los criterios y procesos de seguridad utilizados en los países participantes por un sólo conjunto de criterios de seguridad IT (*Information Technology*, Tecnologías de Información), con la meta de que las evaluaciones realizadas en un país fueran aceptadas en otros países.

En Enero de 1996, Estados Unidos, El Reino Unido, Alemania, Francia, Canadá y Holanda, liberaron la primera versión del estándar de evaluación para un mercado multinacional conocida como CCITSE (*Common Criteria for Information Technology Security Evaluation*, Criterios Comunes para la evaluación de la Seguridad de la Tecnología de Información), mejor conocida como CC (*Common Criteria*, Criterios Comunes).

Basado en un número de evaluaciones de prueba, la Versión 1.0 fue revisada exhaustivamente y la Versión 2.0 fue liberada en Abril de 1998. Esta nueva versión se ratificó como estándar internacional ISO 15408 en 1999. Los proyectos CC subsecuentemente incorporaron cambios menores que habían resultado en el proceso ISO, dando como resultado los CC Versión 2.1 en Agosto de 1999.

Esta conjunción de criterios ha sido exitosamente aceptada y el número de países que ahora aceptan los resultados de las evaluaciones en base a los CC han sido formalmente establecidos en el CCRA (*Common Criteria Recognition Arrangement*, Tratado de Reconocimiento de los Criterios Comunes) y ha crecido de los cinco países iniciales a actualmente catorce (Ver Tabla 3. 17).

| |
|---|
| **Alemania** |
| **Australia** |
| **Canadá** |
| **España** |
| **Estados Unidos** |
| **Finlandia** |
| **Francia** |
| **Grecia** |
| **Holanda** |
| **Israel** |
| **Italia** |
| **Noruega** |
| **Nueva Zelanda** |
| **Reino Unido** |

Tabla 3.17 Países participantes en el CCRA

El proceso de una Evaluación CC es muy recto. El patrocinador de un producto (generalmente el fabricante) primero designa un CLEF (*Commercial Licensed Evaluation Facility*, Facilidad de Evaluación Comercial Autorizada), una vez que el certificador es nombrado por el cuerpo de certificación local, la evaluación puede comenzar.

Los productos son directamente evaluados contra un subconjunto de los CC, llamados SFRs (*Security Functional Requirements*, Requisitos de Seguridad Funcional) y SARs (*Security Assurance Requirements*, Requisitos de Aseguramiento de la Seguridad) y que son reunidos en un documento llamado ST (*Security Target*, Objetivo de Seguridad), el cual contiene un resumen de las especificaciones del producto, los requisitos de seguridad, los objetivos de seguridad y su fundamento. Asimismo, describe la seguridad en función de la operación del producto, junto con una descripción del ambiente en que el producto intenta operar.

Una vez que el CLEF evalúa el ST y pasa la evaluación, el producto puede ser evaluado. El patrocinador le brinda al evaluador un conjunto de muestras y la evaluación determina si éstas satisfacen los requisitos de los criterios, es decir, determina si brinda una completa, consistente y exacta realización del ST. Si el evaluador está satisfecho con la evaluación, se hace un reporte y se presenta al certificador para su aprobación. Si el certificador lo aprueba, se genera un reporte de certificación y se otorga el certificado CC.

Obviamente, durante este proceso las responsabilidades del patrocinador son varias. Debe consolidar la evaluación, pagar al CLEF y al certificador, debe producir un conjunto apropiado de muestras y brindar tanto al evaluador como al certificador, el soporte que requieran en el curso de la evaluación.

Jerárquicamente, en los CC han sido seleccionados y nombrados un conjunto de siete requisitos de seguridad. Estos conjuntos son llamados EAL (*Evaluation Assurance Level*, Niveles de Evaluación de Aseguramiento). Estos niveles intentan, por una parte, brindar compatibilidad con los antigüos criterios y al mismo tiempo, brindar paquetes de aseguramiento de propósito general internamente consistentes; es decir, definen una escala para medir los criterios para la evaluación de PPs y STs; con EAL1 se representa el nivel más bajo de aseguramiento y EAL7 representa el mayor nivel.

En la tabla 3.18, se describen los Niveles de Evaluación de Aseguramiento, que conforman los CC.

| Nivel de Seguridad | Descripción |
|---|---|
| EAL0 | Aseguramiento inadecuado. |
| EAL1 | Funcionalmente Probado. Brinda un análisis de las funciones de seguridad, usando una especificación funcional y de interfaz del TOE (*Target of Evaluation*, Objetivo de la Evaluación), para entender el comportamiento de la seguridad. El análisis es soportado mediante pruebas independientes de las funciones de seguridad. |
| EAL2 | Estructuralmente probado. Análisis de las funciones de seguridad, usando una especificación funcional y de interfaz y el diseño de alto nivel de los subsistemas del TOE. Se llevan a cabo pruebas independientes de las funciones de seguridad, los evaluadores revisan la evidencia de la prueba del revelador "caja negra" y una búsqueda de vulnerabilidades obvias. |

| Nivel de Seguridad | Descripción |
|---|---|
| EAL3 | Metódicamente probado y comprobado. Este análisis es soportado por la prueba "caja gris", una confirmación independiente y selectiva de los resultados de la prueba del revelador y evidencia de búsqueda de las vulnerabilidades obvias. También se requieren controles ambientales del desarrollo y manejo de la configuración del TOE. |
| EAL4 | Diseñado, Probado y Revisado Metódicamente. Este análisis es apoyado por el diseño de bajo nivel de los módulos del TOE, y un subconjunto de la implementación. La prueba apoyada por una búsqueda independiente de las vulnerabilidades obvias. Los controles de desarrollo se soportan mediante un modelo del ciclo de vida, la identificación de herramientas y manejo automatizado de la configuración. |
| EAL5 | Diseñado y Probado Semiformalmente. Brinda el análisis de toda la implementación. El aseguramiento se completa con un modelo formal y una presentación semiformal del diseño de la especificación funcional y diseño de alto nivel, y una demostración semiformal de la correspondencia. La búsqueda de las vulnerabilidades debe asegurar una resistencia relativa a ataques de penetración. La búsqueda de canales ocultos debe ser sistemática. También se requiere el análisis de canales ocultos y diseño modular. |
| EAL6 | Diseño verificado y probado semiformalmente. El análisis se apoya en una aproximación modular y por capas del diseño, y una presentación estructurada de la puesta en práctica. La búsqueda independiente de las vulnerabilidades debe asegurar alta resistencia a ataques de penetración. La búsqueda de canales ocultos debe ser sistemática. Los controles del manejo del ambiente de desarrollo y configuración se fortalecen más. |
| EAL7 | Diseño verificado y probado formalmente. El modelo formal se suple con una presentación formal de las especificaciones funcionales y diseño de alto nivel que muestra la correspondencia. Se requiere la evidencia de la prueba del revelador "caja blanca" y una confirmación completamente independiente de los resultado de prueba del revelador. La complejidad del diseño debe ser reducida al mínimo. |

Tabla 3.18 Niveles de Seguridad para CC

Existen diferencias notables entre los Criterios Comunes y los criterios de seguridad del "Libro Naranja", que alguna vez fueron ampliamente usados:

- Los CC especifican meta-criterios (por ejemplo, criterios para la creación de criterios de seguridad) y proveen procedimientos para evaluación de productos contra criterios de seguridad.
- Los CC no especifican criterios de seguridad como su predecesor de los Estados Unidos, el libro naranja.

- En el proceso CC, los criterios de seguridad son incorporados en PPs (Protection Profiles, Perfiles de Protección) y STs (Security Targets, Objetivos de Seguridad). Esto permite la creación de criterios de seguridad a la medida para reunir aplicaciones y necesidades específicas.

- Los procesos CC también desacoplan las características de seguridad del aseguramiento, que fueron firmemente ligados en el libro naranja. Ahora es posible tener características de seguridad simples evaluadas en un aseguramiento de alto nivel o características de seguridad sofisticadas en un aseguramiento de bajo nivel.

- Los CC demandan un mayor grado de intuición en lo que respecta al problema de la seguridad en la parte de desarrollador y los usuarios de productos evaluados con CC.

Sin embargo, como se mencionó, los EAL´s se desarrollaron con el objetivo de preservar el aseguramiento y resultados de evaluaciones previas, llevadas a cabo usando los criterios "fuente". Las comparaciones son posibles por diseño, pero deben ser hechas con precaución. La Tabla 3.19 puede ser utilizada para realizar dichas comparaciones, aunque esto no significa que sean equivalencias exactas, en vista de que los niveles no consideran el aseguramiento de la misma manera.

| CC | TCSEC (Libro Naranja) | ITSEC |
|---|---|---|
| EAL0 | D: Protección Mínima | E0 |
| EAL1 | | |
| EAL2 | C1: Protección mediante Seguridad Discrecional | E1 |
| EAL3 | C2: Seguridad mediante control de accesos | E2 |
| EAL4 | B1: Protección mediante etiquetas | E3 |
| EAL5 | B2: Protección Estructurada | E4 |
| EAL6 | B3: Dominios de seguridad | E5 |
| EAL7 | A1: Diseño verificado | E6 |

Tabla 3.19 Equivalencias entre los diferentes criterios de seguridad

Hasta hoy ya han sido evaluados y certificados mediante estos criterios una gran cantidad de productos de TI: Sistemas Operativos, Firewalls, Web Servers, VPN, etc.

A continuación, se muestran las categorías en que un producto puede ser evaluados a través de los CC (Tabla 3.20).

| Defensa de la Red e Infraestructura | Defensa del perímetro | Defensa del ambiente de cómputo | Soporte a la infraestructura (PKI, Detección, Manejo) |
|---|---|---|---|
| Switches y Ruteadores | Firewalls | Mensajería segura | Recuperación de Claves |
| Ruteadores | VPNs | Tokens | Tarjetas Inteligentes |
| WLANS | Acceso Remoto | Web Servers de un solo nivel | PKI/KMI |
| | Código Móvil | Protección de datos susceptibles | IDS |
| | Soluciones de Dominio Múltiple | DBMS Confiables | Misceláneos |
| | Guardias | Control de Acceso a PC | |
| | | Código Móvil | |
| | | Peripheral Switch | |
| | | Misceláneos | |

Tabla 3.20 Evaluación de productos mediante CC

Los productos certificados por CC se muestran en la tablas 3.21 a 3.39, según corresponde a su categoría.

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | B1/EST-X, V2.0.1 con AIX, V4.3<br>Windows 2000 Professional, Server, y Advanced Server con SP3 y Q326886 |
| EAL4 | HP-UX (11i) Versión 11.11<br>Solaris 8 2/02<br>Sun Trusted Solaris v 84 /01<br>Sun Solaris Version 8 con AdminSuite V.3.0.1 |
| EAL3 | IRIX V 6.5.13 con parches 4354, 4451, 4452<br>Trusted IRIX/CMW v. 6.5.13 con parches 4354, 4451, 4452, 4373, 4473 |

Tabla 3.21 Sistemas Operativos

TESIS CON
FALLA DE ORIGEN

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | CyberGuard Firewall for Unix Ware Release 4.3/KnightStar Premium Appliance Firewall 4.3 |
| EAL4 | BorderWare V6.1.1 Firewall Server<br>Check Point VPN-1/Firewall-1 ® NG<br>DiamondTEK<br>Gauntlet Firewall Version 6.0 on Sun Solaris V2.8<br>Secure PIX Firewall V5.2(3)<br>SideWinder ® G2 Firewall™, V6.0<br>Symantec Enterprise Firewall v 7.0 |
| EAL3 | Safegate Firewall, V2.0.2 |
| EAL2 | Enterprise Telephony Management Paltform V3.0.1<br>Netscreen Appliances models 5XP, 5XT, 25, 50, 100, 204, 208, 500 y 5200<br>Sidewinder Firewall V5.2.1<br>TeleWall System V 2.0 para NT 4.0<br>Watchguard LiveSecurity System w/Firebox II |
| EAL1 | Conceal Private Desktop for Windows 95/98 |

Tabla 3.22 Firewalls

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL3 | Persona 5.0 |
| EAL1 | Bodacion Technologies' HYDRA Server Version 1.4 |

Tabla 3.23 Web Servers de un solo nivel

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | SecureSwitch Dual Network Switch Modelo #5000600 |

Tabla 3.24 Peripheral Switch

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL2 | Tumbleweed Messaging Management System V4.6 |

Tabla 3.25 Mensajería Segura



TESIS CON
FALLA DE ORIGEN

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | Windows 2000 Professional, Server, y Advanced Server con SP3 y Q326886 |
| EAL4 | DiamondTEK |
| EAL2 | BMC PATROL Perform/Predict, V6.5.30<br>BMC Software PATROL V 3.4.11 |

Tabla 3.26 Administración de Redes

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | DiamondTEK |

Tabla 3.27 VPN (*Virtual Private Network*, Redes Privadas Virtuales)

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | Windows 2000 Professional, Server, y Advanced Server con SP3 y Q326886 |
| EAL4 | Sentinel Model III<br>Supernet 2000 |
| EAL3+ | Cryptographic Security Chip for PC Clients, Manufactured by ATMEL (AT90SP0801) |
| EAL1 | Encryption Plus Hard Disk 7.0<br>Entrust TrueDelete Version 4.0 for WIN95/NT<br>SafeGuard Easy for Windows 2000 Version 1.0<br>SecureDoc Disk Encryption Version 2.0 for Windows 95/98 and Windows NT<br>Tripwire Manager 3.0 with Tripwire for servers 3.0, Tripwire Manager 3.0 with Tripwire for Servers Check Point Edition 3.0<br>UniShred Pro V3.3.1 |

Tabla 3.28 Protección de Datos

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL3 | SurfinGate V5.6 |

Tabla 3.29 Código Móvil

TESIS CON
FALLA DE ORIGEN

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL2 | Owl Computing Technologies Data Diode Version 1.0 and Version 2.0<br>DragonFly Companion V3.02 Build 129<br>DragonFly Guard Model G1.2 |

Tabla 3.30 Guardias

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL2 | Byoscript Enterprise for NT Logon, V2.1.3 |

Tabla 3.31 Biométricos

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | Oracle 8 Release 8.0.5.0.0<br>Oracle 8i Release 8.1.7.0.0<br>Oracle Label Security for Oracle 8i Database Server Enterprise Edition Release 8.1.7.3.0 |

Tabla 3.32 DBMS Confiables

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | Netscape Certificate Management System 6.1 Service Pack 1<br>RSA Keon CA System, Version 6.5 |
| EAL4 | Chrysalis-ITS Luna ® CA3 V3.97 Software Versions 8.0 and 8.1<br>SecureNet TrustedNet Connect Ver 2.0 |
| EAL3 | UniCERT Timestamp Server Version 2.0.2<br>Entrust/Authority from Entrust/PKI 5.1<br>Entrust/RA from Entrust/PKI 5.1<br>RSA Keon CA System Version 6.5 |

Tabla 3.33 PKI/KMI (Public Key Infraestructure/Management Infraestructure, Infraestructura de Clave Pública/Infraestructura de Manejo de Clave)

TESIS CON
FALLA DE ORIGEN

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | GemXpresso Pro E64 PK – Java Card Platform, Embedded Software V3 (Core)<br>GemXplore 'Xpresso V3 – Java Card Platform, Embedded Software V3 (Core)<br>Sony FeliCa Contactless Smart Card RC-S860 |
| EAL3 | Philips Smart Card Controller P8WE5032 VoB |

Tabla 3.34 Tarjetas Inteligentes

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | Sentinel Model III |

Tabla 3.35 Control de Acceso a PC

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL2 | Intrusion, Inc. SecureNet Pr™<br>Intrusion Detection System Version 4.1 |

Tabla 3.36 Sistemas de Detección de Intrusos

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL2 | Sharp Corporation Multifunction Device with Data Security Kit (AR-FR4 V.M.10, AR-FR5 V.E. 10, AR-FR6 V.J. 10)<br>Sharp Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for Sharp Imager Family (FR-287, AR-337, AR-407, AR-507) |

Tabla 3.37 Misceláneos para Defensa del Ambiente de Cómputo

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4+ | Netscape Certificate Management System 6.1 Service Pack 1<br>RSA Keon CA System Version 6.5 |

Tabla 3.38 Administración de Certificados

TESIS CON
FALLA DE ORIGEN

| Nivel de Seguridad | Productos Certificados |
|---|---|
| EAL4 | Trend Micro InterScan™ VirusWall 3.52 for NT<br>Trend Micro InterScan™ VirusWall 3.6 for Solaris, HP-UX and Linux |

3.39 Antivirus

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

# CAPÍTULO 4
# SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES

En estos tiempos, las personas y organizaciones disfrutan y hacen uso de los servicios que Internet ofrece; asimismo, las empresas han dedicado esfuerzos y fijado metas en el comercio electrónico a través de Internet, ofreciendo la compraventa de bienes y servicios sin la necesidad de trasladarse de su casa u oficina.

En las tendencias de globalización, Internet representa algo más que el simple concepto de red pública, es un amplio mercado donde confluyen miles de personas desde diferentes regiones, con diferente idioma, idiosincrasia, cultura, religión y política. A través de Internet, las empresas tienen la posibilidad de dar a conocer sus productos o servicios, invirtiendo en publicidad directa o en patrocinio, con la intención de cautivar al cliente mediante páginas con excelente presentación ofreciendo cubrir sus demandas en la comodidad de su hogar u oficina, por ello cada vez más organizaciones desean afiliarse a esta nueva línea de negocios.

El esquema general de comercio a través de Internet, se desarrolla en portales que requieren o solicitan obligadamente el registro del usuario o cliente, quien debe contar con tarjeta de crédito y proporcionar datos de identificación y de ubicación con la finalidad de poderle entregar los productos o servicios que éste adquiera. En otros casos, los portales pertenecen a tiendas departamentales que han utilizado Internet como medio para establecer puntos de venta, en este tipo de sitios, el registro como usuario o cliente puede resultar más simple sólo si se es tarjetahabiente de la tienda. Los servicios bancarios y financieros son otro ámbito más del comercio electrónico, el cliente o usuario realiza procesos similares de registro para estar en posibilidades de efectuar a través de Internet las operaciones de pago, transferencias e inversiones.

Esta tecnología que se nos ofrece y en la que nos vemos inmersos más y más conforme el tiempo avanza, también está a expensas de ser vigilada por terceras personas con fines ilícitos. Los actos cotidianos de asalto, robo, atentado, perversión y manipulación afectan sensiblemente al desarrollo libre y sano de nuestras vidas pero son situaciones que por seguridad no debemos ignorar. La diversidad de personas que usan Internet y la cualidad de esta red como medio masivo de comunicación, establecen condiciones ideales para la intervención de personas o grupos con fines ilícitos que podrían poner en riesgo nuestra seguridad, integridad y economía. Cuando requerimos de un producto o servicio proporcionado a través de Internet y se nos solicita registrarnos como usuarios proporcionando datos personales, por instinto, la mayoría somos cautelosos por temor a que éstos puedan ser utilizados indebidamente pero difícilmente pensamos en que pueden ser interceptados por personas que intentan cometer un delito con ellos.

Desde un punto de vista individual, corremos riesgos al hacer uso de Internet, pero desde un punto de vista empresarial, debemos recordar que la información es el principal activo que representa dinero, oportunidad y desarrollo; por ello, es conveniente establecer políticas de seguridad que minimicen los riesgos que implica el intercambio de información y la comunicación a través de Internet, entendiendo

como información cualquier tipo de dato electrónico que sea parte de una operación, transacción o conversación.

Ha sido causa de titulares a ocho columnas en periódicos y tiempo de noticieros televisivos, la narración incrédula e irónica de cómo se han burlado sofisticados esquemas de seguridad a través de equipos remotos, debido, principalmente, al conocimiento de los protocolos de comunicación, su configuración y vulnerabilidades, lo que hace imprescindible concebir claramente las políticas y cultura de seguridad, así como los servicios y mecanismos de protección al proceso de datos y su transferencia que deben implantarse en una empresa que enviará y recibirá información a través de Internet.

Una política de seguridad conjunta elementos de hardware, software y reglamentación interna reduciendo riesgos en el manejo de información, debiéndose implantar en toda organización aún si no está conectada a Internet. Asimismo, la cultura de seguridad es un elemento que reforzará sustancialmente cualquier esquema establecido para garantizar la integridad de la información, pues ni el mejor esquema de protección evitará que un cajero salte el mostrador y salga corriendo del Banco con una bolsa repleta de dinero o que el cajero olvide concluir la sesión de trabajo en su equipo de cómputo. Por otra parte, ya sea individualmente o actuando como parte de una empresa, existen servicios y mecanismos de protección aplicables a la transferencia electrónica de datos, los cuales pretenden garantizar que el emisor es quien dice ser, el destinatario es quien debe recibir y que la información viajó sin alteraciones y no pudo ser vista por terceros.

En el presente capítulo, se discutirán las diferentes herramientas que pueden ser utilizadas para construir una buena política de seguridad cuando una red privada es conectada a Internet y definiremos un modelo que incluirá servicios y mecanismos de protección a la transferencia electrónica de datos y los aspectos más relevantes sobre una cultura de seguridad.

## 1. POLÍTICAS DE SEGURIDAD ENTRE UNA RED PRIVADA E INTERNET

Los principales temores que existen cuando una organización decide utilizar Internet como medio de comunicación con los equipos externos a su red privada son:

- Acceso no autorizado a los recursos de la red privada, lo que puede traducirse en espionaje.
- Uso ilícito de información o pérdida de integridad en los datos.
- Uso inapropiado de los servicios de Internet por parte de los usuarios internos.
- Bloqueo de comunicación (disponibilidad).

Para superar estos temores sería conveniente contar con un elemento que fuera capaz de intermediar la comunicación de la red interna o privada con el exterior, cuya finalidad estuviera concentrada en filtrar el tipo de enlace, la información que se transmite y los recursos a los que se puede tener acceso.

Para cumplir con lo anterior, es necesario que el administrador de la red privada establezca políticas de seguridad que brinden protección a sus sistemas y al mismo tiempo brinden la mejor comunicación a sus usuarios internos, traducida en velocidad de comunicación y acceso a los servicios requeridos; para ello debe conocer las necesidades y riesgos de su información y comunicación, evaluar los riesgos del acceso a Internet y establecer las medidas necesarias que los minimicen.

Un **"firewall"** es un elemento de seguridad esencial cuando se desea conectar una red privada a Internet, puede definirse como un sistema que implanta una política de seguridad entre ambas redes.

El **"firewall"** es un puente de comunicación entre dos redes, normalmente una privada y una pública, puede construirse con hardware, software o una combinación de ambos (ver figuras 4.1 y 4.2); para que sea efectivo, toda la comunicación entre las dos redes debe ser administrada por él. Los **"firewalls"** más sencillos son los ruteadores.

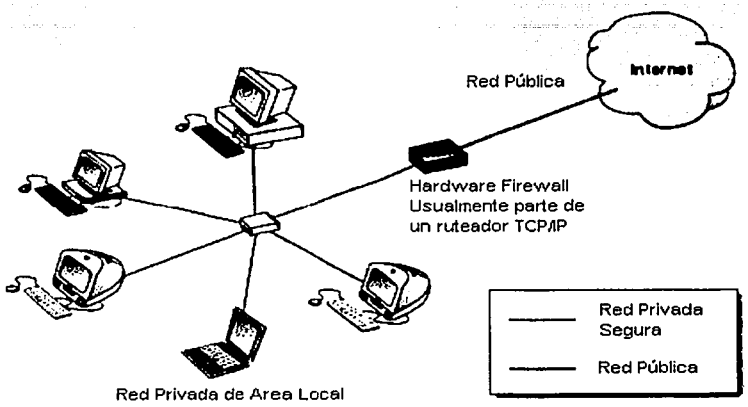


Fig. 4.1 Hardware "Firewall"

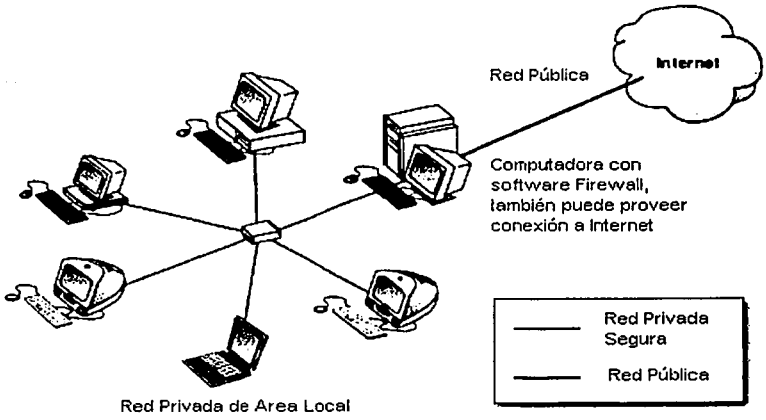


Fig. 4.2 Software "Firewall"

Un "**firewall**" administra el tráfico de información entre las dos redes conectadas a él, siguiendo los criterios establecidos por el administrador, por lo tanto, previene el acceso no autorizado de usuarios a la red privada y determina los servicios que un usuario autorizado puede utilizar. Adicionalmente, registra los accesos hacia Internet realizados por los usuarios de la red privada, lo que permite auditar estos registros con el objeto de evitar el abuso en el uso de Internet. Asimismo, filtra información basada en su origen,



TESIS CON
FALLA DE ORIGEN

direcciones de destino y números de puerto, permite el monitoreo de tareas activando alarmas ante la posibilidad de un ataque o problema de tráfico de información, traduce direcciones de red (NAT) facilitando mantener espacio de direccionamiento acortando y eliminando lo necesario para reenumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs) y centraliza el sistema de seguridad en un solo punto.

Por otra parte, un **"firewall"** no puede prevenir que los usuarios de la red privada utilicen equipos modem para conectarse a Internet, saltando así la protección establecida; no puede prohibir la copia de datos importantes a medios magnéticos y que después éstos sean sustraídos de la empresa; no puede prevenir el ataque de un virus informático obtenido a través de archivos y software que el usuario ingrese a la empresa o baje de Internet y por último, no puede protegerse contra los posibles ataques en la transferencia de datos; por ejemplo, una transferencia de datos podría modificar la seguridad permitiendo el acceso a un intruso.

## 1.1 Herramientas para acceder un equipo remoto

Para crear un buen esquema de seguridad en una red privada conectada a Internet, es necesario, primero, entender la manera en que una persona actúa para anular el perímetro de seguridad implantado.

Es difícil establecer una técnica para inhabilitar un esquema de seguridad a través de un equipo remoto, esto depende del nivel técnico, características, experiencia y propósito que se posea, sin embargo, podemos deducir que la secuencia lógica de los aspectos a cubrir, es la siguiente:

- Identificación de la distribución y administración en la red privada.
- Exploración y reducción de la seguridad.
- Acceso a los servicios de red.

### 1.1.1 Identificación de la distribución y administración en la red privada.

La primera actividad a desarrollar, es establecer cómo se encuentra distribuida y administrada la información dentro de la red privada, lo que posibilita el conocimiento de los datos que pueden ser manipulados para invalidar los dispositivos de seguridad establecidos por el administrador de la red. Las herramientas disponibles y que podrían ser utilizadas se describen a continuación.

***Protocolo SNMP*** *(Simple Network Management Protocol,* Protocolo para el manejo de red simple).

SNMP es una solución ampliamente utilizada para la administración de elementos en Internet, cuyas virtudes son un pequeño lenguaje o conjunto de comandos y la confianza que establece en una liga de comunicación sin supervisión o de mínima conexión.

La implementación SNMP se compone de un administrador (que provee una interfase entre el sistema de administración y el responsable de la red), un agente (interfase entre el administrador y los dispositivos físicos u objetos), una base de datos de administración, los objetos administrados y el protocolo de red, ver Figura 4.3.

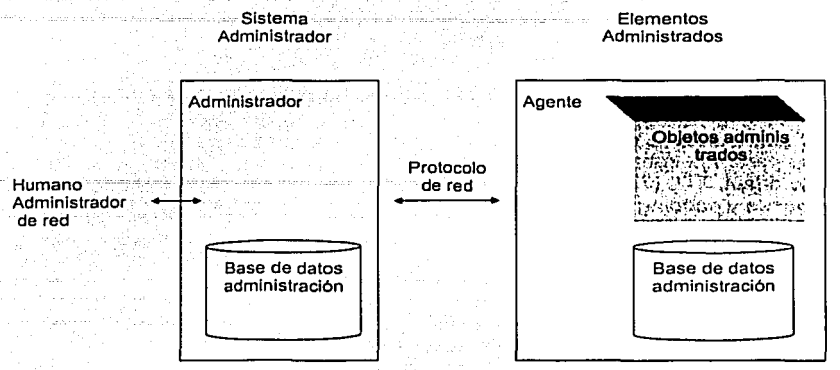


Fig. 4.3 Implementación SNMP

El administrador y el agente interactúan mediante el intercambio de cinco mensajes básicos, los cuales se describen a continuación:

- Get y Get-Next. El administrador solicita al agente información sobre el estado de los objetos administrados.
- Set. El administrador solicita un cambio de estado referente a un objeto. En general alarmas remotas que operarán un relevador.
- Get-Response. El agente responde al administrador enviando la información solicitada, la indicación de un cambio efectuado o la indicación de causa de error.
- Trap. El agente enviará este mensaje al administrador tan pronto como una condición de alarma o evento importante ocurra en los objetos administrados, sin esperar a que se solicite dicho estado.

SNMP se considera una solución robusta derivada de la independencia que existe entre el administrador y el agente.

Este protocolo comunmente es utilizado para monitorear y manejar los dispositivos de la red, con él se puede examinar la tabla de ruteo en un dispositivo inseguro, lo que sirve para aprender los detalles más íntimos de la topología de red perteneciente a una organización.

**TraceRoute.**

Internet es una red de computadoras basada en el modelo TCP/IP, mediante el protocolo IP cada equipo es identificado mediante un número de 32 bits que debe ser único para cada computadora, con esta dirección se reconoce no sólo el equipo sino también la red a la que pertenece, distinguiendo así a las computadoras que se encuentran conectadas a una misma red.



TESIS CON
FALLA DE ORIGEN

Una de las funciones más importantes del nivel IP es el enrutamiento, ya que éste proporciona los mecanismos para conectar físicamente dos computadoras, cuando un paquete de información es enviado utilizando Internet como medio de comunicación, puede que sea necesario transportarlo a través de varios servidores o computadoras para llegar a un destino.

La información enviada a través de Internet es manipulada en pequeños paquetes llamados Datagramas con un formato predefinido y longitud mínima de 20 bytes. Un Datagrama está formado por una cabecera de 20 bytes y una parte de datos de longitud variable; los campos que conforman la parte fija son: versión, opciones, tipo de servicio, longitud total, identificación, flags, fragmento de offset, TTL (*Time to live*, Tiempo de vida), protocolo, checksum, dirección de origen y destino, opciones y padding.

El campo TTL es un contador que se utiliza para limitar el tiempo que los paquetes tienen para llegar a su destino, si llega a cero el paquete es destruido.

TraceRoute, es un programa que identifica el número de redes y ruteadores por los que un paquete debe transportarse para llegar a un servidor específico.

Este programa envía un datagrama de prueba a una dirección IP específica, determinando y mostrando los tiempos de respuesta así como las direcciones IP de cada uno de los servidores por los que ese datagrama tiene que pasar hasta llegar a su destino. El campo TTL del datagrama de prueba puede ser modificado con la finalidad de detectar una posible ruptura en la conexión.

Existen diversos programas en el mercado, la mayoría de ellos están disponibles en forma gratuita a través de Internet, entre ellos podemos mencionar, los siguientes:

- Necrosoft Traceroute
- Belnet Traceroute
- Tracert

**Protocolo Whois.**

Este protocolo provisto por las organizaciones que administran el crecimiento y la evolución de Internet y sus servicios, permite obtener información referente a los dominios o servidores y a los correspondientes propietarios o contactos técnicos.

Whois puede ser utilizado a nivel de desarrollo de sistemas en forma de librerías, como aplicación específica, a través de una sesión telnet a ds.internic.net o directamente en la dirección URL http://rs.internic.net/cgi-bin/whois.

El funcionamiento de este protocolo se desarrolla mediante búsquedas genéricas basadas en cadenas de caracteres sobre diversas bases de datos mantenidas por InterNIC.

**Servidores DNS.**

Como se ha mencionado Internet opera en base a direcciones IP, pero este funcionamiento más que facilitar la localización de destinos complicaría al usuario al tener que recordar series de números asociados a los equipos con los que se desea conectar. Como solución a esta problemática y simplificación del uso de direcciones IP, se implementaron Servidores de Nombres conocidos como DNS (*Domain Name System*, Sistema de Nombres de Dominio) cuya finalidad es permitir la traducción automática de nombres de dominio por la dirección IP asignada.

La traducción de nombres por direcciones IP puede realizarse directamente por el servidor DNS que la contiene o a través de una cooperación de servidores DNS preguntándose entre sí; como ejemplo, del funcionamiento de un servidor de nombres, puede consultarse a través de Internet la aplicación Nslookup.

**Protocolo Finger.**

Este protocolo provee una interfaz dirigida a la comunicación con programas remotos que proporcionan información detallada referente a los usuarios de un servidor específico, tal como: nombre de registro, nombre de usuario y registro de accesos.

El procedimiento de comunicación, se desarrolla de la siguiente forma:

- En un servidor local, se establece una conexión TCP con un servidor remoto, utilizando el puerto 79 decimal o 117 octal, envía una solicitud de información utilizando la especificación del protocolo Finger.

- En el servidor remoto, el programa que provee información del usuario procesa el requerimiento de información, envía la respuesta en formato ASCII y cierra la conexión.

Los programas que proporcionan información de usuarios, en un servidor, son implementaciones del protocolo Finger y son adquiridas con los distribuidores de los sistemas operativos o software de red.

Finger puede ser utilizado a nivel de desarrollo de sistemas en forma de librerías o como aplicación específica; tal es el caso de Ifingered.

**Ping.**

El protocolo ICMP (*Internet Control Message Protocol*; Protocolo de Mensajes de Control en Internet) se utiliza para evaluar la disponibilidad de rutas hacia otros equipos y obtener información sobre la red.

Existen diversos programas implementados sobre el protocolo ICMP y que, como se mencionó, son utilizados para determinar la disponibilidad de un servidor en particular, a través de éstos programas es posible monitorear la red y construir una lista de los servidores que es necesario acceder para localizar un servidor específico.

En el mercado, existen diversos programas que integran más de una de las herramientas que se acaban de describir, muchos de ellos están disponibles en forma gratuita a través de Internet y entre ellos, podemos mencionar los siguientes:

- Nmap
- Ws_Ping
- VisualRoute
- Belnet Traceroute

### 1.1.2 Exploración y disminución de la seguridad.

Una vez que se han podido indagar datos suficientes sobre el esquema de distribución y administración de la red a la cual se desea ingresar, se explora individualmente cada uno de los servidores conocidos, con la intención de identificar servicios disponibles y especificaciones de seguridad particulares; asimismo, se construye una lista de vulnerabilidades relacionadas con los servicios que servirá para implementar el ataque o estrategia de disminución de la seguridad.

Esta exploración de servicios y detección de vulnerabilidades se realiza con base en una práctica común de prueba y error, lo que permite al intruso deducir e inducir los caminos a seguir para burlar la seguridad.

Las herramientas disponibles y que podrían ser utilizadas se describen a continuación.

***Programas de computadora propios.***

Con base en la lista de vulnerabilidad de los servicios de red y haciendo uso de las implementaciones para desarrollo de los protocolos de comunicación, es posible construir un programa de computadora capaz de intentar conexiones iterativas a un puerto y de variar parámetros de comunicación en forma automática, especificando el tipo de servicio que está asignado a un servidor determinado. Adicionalmente, el programa puede presentar una relación de los servidores que soportan servicios de Internet y que están expuestos al ataque.

***Programas de computadora de dominio público y comerciales.***

En adición a la construcción de programas de computadora propios, a través de Internet es posible encontrar productos y algoritmos implementados por personas o grupos dedicados a romper esquemas de seguridad, disponibles en forma gratuita.

Por otra parte, en el mercado de aplicaciones para monitoreo y supervisión de red, se encuentran disponibles herramientas para detectar fallos o errores de seguridad, tales como:

- ISS (*Internet Security Scanner,* Rastreador de Seguridad en Internet).
- SATAN (*Security Analisis Tool for Auditing Networks,* Análisis de Seguridad para Auditar Redes).

Este tipo de aplicaciones comerciales, realizan la búsqueda de una subred o un dominio y determinan los puntos vulnerables comunes en un sistema; el intruso aprovecha esta información para intentar el acceso no autorizado al sistema.

### 1.1.3 Acceso a los servicios de red

Las pruebas deductivas e inductivas realizadas durante la exploración y disminución de la seguridad, dan como resultado final, tener acceso libre a los servicios de red, una vez dentro no hay límites, todo está a disposición del usuario no autorizado y será conveniente para él, realizar las siguientes actividades:

- Destruir la evidencia del asalto y crear mayores vulnerabilidades en el sistema, de tal suerte que permitan el acceso sin que el ataque original sea descubierto.

- Instalar paquetes de sondeo o inspección que incluyan códigos binarios conocidos como "Caballos de Troya", protegiendo su actividad y actuando en forma transparente para los administradores de red. En forma general, los paquetes de sondeo o inspección colectan cuentas y contraseñas para los servicios de Telnet y FTP con la intención de expandir el ataque a otros equipos.

- Encontrar servidores o servicios que realmente comprometan al sistema, insignias de reconocimiento a la labor realizada u objetivo específico de la intrusión.

- Tener acceso privilegiado en los sistemas compartidos para leer correo, buscar archivos y alterar opciones de configuración del sistema.

Las herramientas analizadas hasta este punto, deben ser conocidas y utilizadas por el administrador de la red con cierta frecuencia, con el objeto de conocer los puntos vulnerables de su sistema y reforzar su seguridad actualizando el software de sus servidores.

## 1.2 Diseño de un "firewall"

Para abordar el diseño de un "**firewall**" y los beneficios que su implantación tendrá a nivel de seguridad, es necesario observar las siguientes fases:

| | |
|---|---|
| **Primera Fase** | Determinar el grado de vulnerabilidad que presenta la red privada que se desea proteger de posibles ataques externos. A tal fin, el administrador de red deberá aplicar algunos de los conceptos y aplicaciones descritos en el apartado "Herramientas para Acceder a un Equipo Remoto", en este mismo capítulo. |
| **Segunda Fase** | Decidir si la solución a la vulnerabilidad detectada en la red es la implantación de un "**firewall**", considerando la premisa descrita a continuación y que se trató con mayor detalle al inicio de este capítulo:<br><br>*"El "**firewall**" es, en esencia, el intermediario de la comunicación entre una red privada y una red pública, el cual actúa estableciendo políticas de seguridad y manteniendo el control de la información que se envía y recibe".*<br><br>En consecuencia, se deberá tener presente el alcance del mismo para estar en condiciones de iniciar la tercera y última fase. |

| | |
|---|---|
| **Tercera Fase** | Diseño e implementación del "**firewall**", conforme a los cuatro pasos siguientes:<br>• Establecimiento de políticas de funcionamiento del "**firewall**".<br>• Establecimiento de políticas internas de seguridad.<br>• Establecimiento de límites de costo para el "**firewall**".<br>• Construcción del "**firewall**". |

**Políticas de funcionamiento del "firewall"**

En forma general, un "**firewall**" permite el acceso hacia la red privada, siguiendo una de las dos metodologías siguientes:

- Permitir el tráfico de información a menos que exista una política de seguridad que niegue el acceso. Con esta postura establece una amplia seguridad pero no facilita el uso de servicios.

- No permitir el tráfico de información a menos que exista una política de seguridad que autorice el acceso. Esta postura facilita el uso de servicios a los usuarios pero debilita la seguridad.

Se recomienda, que inicialmente se nieguen todos los accesos a través del "**firewall**" y después se otorguen privilegios de entrada conforme se determine que son necesarios, es una política conservadora pero efectiva para asegurar la información contenida en la red.

Para otorgar privilegios de acceso, es necesario realizar un análisis sobre los servicios, la información y su disponibilidad a través de la red, que permita establecer lo siguiente:

- Políticas de entrada.
- Políticas de salida.
- Políticas de conexión a Internet.

**Políticas de entrada**

Si todo el tráfico de Internet se origina en la red privada puede restringirse fácilmente los accesos con un ruteador NAT, éste bloqueará todos los accesos de entrada que no hayan sido solicitados dentro de la red privada; además, las direcciones IP de los equipos internos jamás serán revelados al exterior, dificultando la intrusión. Los paquetes en el lado público del ruteador, a los cuales se les permite el acceso, son encaminados a números de puerto dinámicos, cambiándolos continuamente, lo que dificulta a un intruso determinar los números de acceso.

Si los requerimientos implican un acceso seguro a la red privada desde Internet, es necesario determinar los criterios que se utilizarán para decidir cuando un paquete puede acceder a la red privada; por ejemplo, puede decidirse que direcciones IP pueden acceder servicios de la red privada o restringir el acceso a determinados protocolos, tales como FTP o http.

Si no se conocen las direcciones IP de entrada y no es posible restringir el uso de protocolos, entonces será necesario implementar las políticas de seguridad sobre un sistema más complejo, tal es el caso de un "**firewall**" de inspección de estados multinivel.

### Políticas de salida

Si los usuarios de la red privada, requieren únicamente tener acceso a Internet, un servidor proxy puede proporcionar un nivel de seguridad alto concediendo acceso selectivamente, la desventaja es que este tipo de servidores requieren configuración manual en la parte del cliente.

Es posible, por otra parte, implementar el acceso a Internet sin sacrificar seguridad a través de un ruteador filtrador de paquetes. Sin embargo, en el caso de un ruteador NAT, no es posible limitar el acceso a Internet y la responsabilidad total recae en los usuarios, lo que pone en riesgo la seguridad de los sistemas de la red privada.

### Políticas de conexión a Internet

En caso de que sea necesario, para los usuarios, contar con una conexión directa a Internet, ésta se debe establecer mediante conexiones seguras, a través de las cuales sea imposible acceder a la red privada. Lo mejor, es aislar físicamente la computadora y evitar, en la medida de lo posible, este tipo de conexiones.

## Políticas internas de seguridad

Como se mencionó, el "**firewall**" por si solo no establece la seguridad completa de un sistema, es necesario que este dispositivo sea sólo una de las partes que componen el esquema global de seguridad, si no se cuenta con información detallada sobre políticas internas de seguridad establecidas a nivel organizacional y son observadas en toda la empresa, aunque el "**firewall**" esté cuidadosamente implementado, la red estará expuesta a un posible atentado.

Las políticas de restricción o acceso establecidas en un "**firewall**" deben ser reflejo de las políticas internas sobre seguridad de la información, las cuales son establecidas y observadas por la empresa.

## Costo del "firewall"

Una vez que se ha establecido la relación entre las políticas de seguridad y el "**firewall**" y que la adquisición de éste último es inminente, es conveniente revisar el presupuesto económico destinado a su implantación, mantenimiento y actualización pues de ello dependerá, en gran medida, la decisión acerca del tipo de "**firewall**" que se deberá adquirir.

Un "**firewall**" puede ser construido con sistemas de dominio público, lo que redunda en un costo mínimo, o puede implementarse con sistemas comerciales robustos existentes en el mercado, cuyo costo puede variar entre $3,000 y $25,000 USD.

Cabe señalar que, en adición a la inversión inicial, otro aspecto de la misma relevancia que se debe considerar y no se debe omitir, es el costo de mantenimiento y actualización que cada uno de estos sistemas requerirá durante su tiempo de vida, el cual podría resultar mayor en el caso de utilizar software de dominio público, esto a consecuencia de que, en muchos de los casos, no existe soporte técnico para realizar cambios o adaptaciones específicas.

**Construcción del "firewall"**

Una vez establecidas las políticas de seguridad que serán implementadas, debe decidirse la mejor forma de implantar el "**firewall**", según las siguientes opciones:

- Adquisición de un producto comercial completo.
- Implementación a través de un sistema integrador.
- Implementación propia.

Esta decisión depende de la complejidad de las políticas de seguridad establecidas y de la experiencia que la persona encargada de la implantación tenga sobre el tema.

En forma general, existen cuatro tipos de "**firewalls**", los cuales se indican a continuación:

| |
|---|
| "**Firewall**" Filtra-paquetes |
| Gateways a nivel de circuito |
| Gateways a nivel de aplicación |
| "**Firewall**" de Inspección de estados multinivel |

***"Firewall" Filtra-paquetes***

Este dispositivo funciona sobre el nivel 3 (nivel de red) del modelo OSI o en el nivel 3 (capa IP) del modelo TCP/IP, usualmente es parte de un ruteador, el cual recibe y envía paquetes.

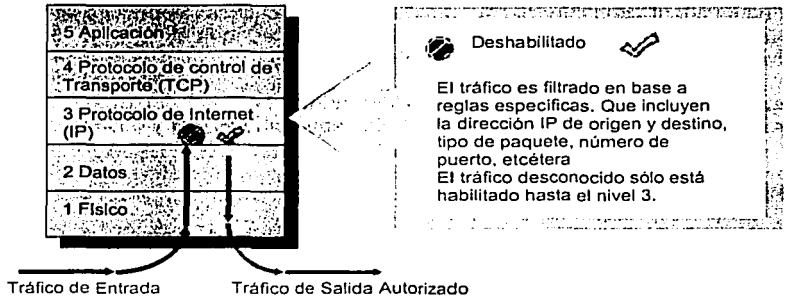


Fig. 4.4 Funcionamiento del "Firewall" Filtra-paquetes

La información enviada a través de Internet es manipulada en pequeños paquetes llamados Datagramas con un formato predefinido y longitud mínima de 20 bytes. Un Datagrama está formado por una cabecera de 20 bytes y una parte de datos de longitud variable; los campos que conforman la parte fija son: versión, opciones, tipo de servicio, longitud total, identificación, flags, fragmento de offset, TTL (*Time to live*, Tiempo de vida), protocolo, checksum, dirección de origen y destino, opciones y padding.



TESIS CON
FALLA DE ORIGEN

El dispositivo ruteador es implantado entre dos redes; cuando recibe un paquete de información, revisa los datos de la cabecera del datagrama correspondientes a la dirección IP fuente y destino, el protocolo de encapsulado (UDP, ICMP o IP túnel), el puerto fuente y destino TCP/UDP, el tipo de mensaje ICMP y la interfaz de entrada y salida del paquete; si el datagrama corresponde a uno de sus paquetes filtrados y las políticas de filtrado permiten el paso del paquete, se desplaza de acuerdo a la información en la tabla de ruteo; si se niega el paso, el paquete es descartado; si no corresponden a las reglas, un parámetro por incumplimiento, configurable en el ruteador, descarta o desplaza el paquete.

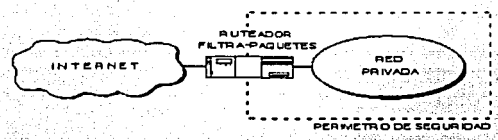


Fig. 4.5 Esquema de seguridad mediante un "Firewall" Filtra-paquetes

Algunas reglas de filtrado usuales son:

- Validar direcciones IP origen y destino
- Validar número de puerto origen y destino
- Validar sesiones Telnet conforme a políticas de autorización
- Validar sesiones FTP conforme a políticas de autorización

Un ruteador traductor de direcciones de red (NAT; *Network Address Translation*) ofrece las mismas ventajas que un ruteador filtrador de paquetes, pero además oculta las direcciones IP de las computadoras que conforman la red privada y puede establecer reglas de filtrado basadas en el nivel de circuito.

**Ventajas**

La implantación es sencilla y no es costosa, las reglas de acceso tienen un bajo impacto en el desempeño de la red, además de que el ruteador de filtrado es, generalmente, transparente para los usuarios finales, por lo que no es necesaria capacitación extra para los usuarios o adicionar software a los servidores.

**Desventajas**

Definir los estándares para el filtrado de paquetes resulta complejo, pues es necesario conocer en forma detallada los servicios de Internet, así como los datos y formato del encabezado de un datagrama; además, dado que únicamente se trabaja en la capa de red, no soporta reglas sofisticadas basadas en modelos.

Asimismo, debido a que los datos contenidos en un paquete no son revisados, es posible que éstos modifiquen la seguridad del ruteador facilitando el acceso no autorizado al sistema; por lo tanto, es posible permitir o negar el uso de un servicio, pero no se abarca el contexto de datos del servicio.



TESIS CON
FALLA DE ORIGEN

***Gateway a nivel aplicación***

Este tipo de dispositivos están diseñados para filtrar paquetes de información en la capa de aplicación del modelo OSI o del modelo TCP/IP; su operación se consigue instalando en el gateway un código de propósito general (servicio Proxie) para cada aplicación deseada. Si este código no está instalado, el servicio no es soportado y los paquetes que entran o salen del gateway no serán procesados.

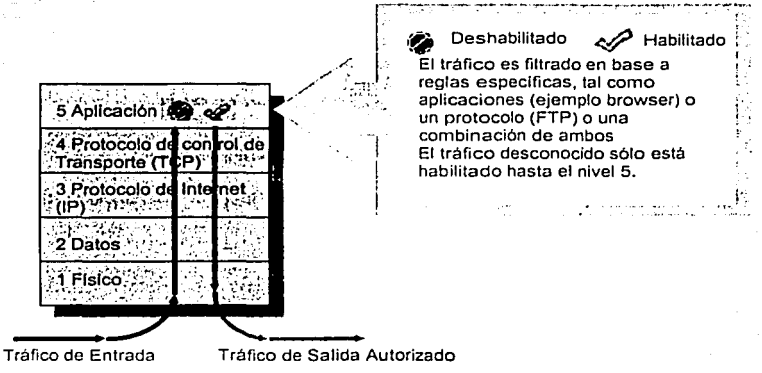


Fig. 4.6 Funcionamiento del Gateway a nivel aplicación

Los gateway a nivel aplicación permiten establecer una política de seguridad más estricta que los ruteadores filtra-paquetes, ya que pueden negar todo tipo de tráfico; por ejemplo, servicios de FTP, GOPHER o TELNET. En virtud de que manipulan la información en la capa de aplicación, también tienen la capacidad de filtrar paquetes bajo características específicas de un servicio; por ejemplo, es posible negar el acceso al comando http: post and get.

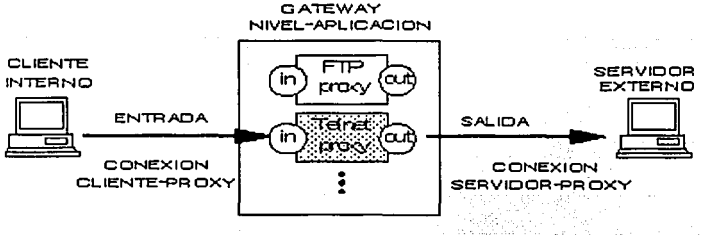


Fig. 4.7 Funcionamiento del Gateway a nivel aplicación

TESIS CON
FALLA DE ORIGEN

Cada proxie es un sencillo y pequeño programa diseñado específicamente para proveer seguridad entre redes, por lo tanto, en comparación con aplicaciones típicas que proveen servicios de red, puede revisar y analizar posibles intrusos y fugas de seguridad.

Es posible instalar más de un servicio proxie, con la ventaja de que cada uno de ellos es independiente del otro, si alguno de ellos presentara una falla o se descubriera que es vulnerable puede dejar de funcionar sin afectar al resto del sistema.

Generalmente, el servicio proxie funciona sin realizar accesos continuos al disco, solo lee su archivo de configuración al iniciar el servicio dificultando, a cualquier usuario no autorizado, la instalación de virus, caballos de Troya o archivos que alteren el sistema de defensa.

El gateway a nivel de aplicación también es conocido como "servidor de defensa", porque es un sistema diseñado específicamente para proveer alto nivel de protección contra cualquier tipo de ataque. Asimismo, este servidor es ideal para colocar un sistema fuerte de supervisión de autorización, tal como la tecnología "una sola vez" de contraseña; donde, a través del uso de tarjetas inteligentes, se genera un código único de acceso mediante procedimientos criptográficos.

A continuación, se describen algunas características de diseño que pueden ser consideradas para implementar un servidor de defensa:

- Ejecutar una versión "segura" del sistema operativo correspondiente al hardware del servidor de defensa.
- Mantener instalados, en el sistema, sólo los servicios requeridos por los usuarios o aquellos que se van a proveer.
- Autenticar cada uno de los servicios proxie para autorizar o denegar el acceso a ellos.
- Establecer condiciones de filtrado en la información a nivel aplicación así como a nivel comando, en cada servicio instalado.
- Configurar el acceso a los servidores de la red privada, considerando condiciones de autorización sólo para aquellos que intervienen en los servicios que se proveen y denegándolo para cualquier otro.
- Habilitar herramientas de auditoría del sistema proxie para registrar datos relacionados a tráfico de información, conexiones, tiempos de conexión y usuarios con la finalidad de detectar y neutralizar ataques o intrusos.
- Instalar todos los servicios proxie que se requieran, pues mantendrán la independencia de operación y funcionamiento entre sí.
- Configurar cada servicio proxie al iniciar su ejecución, evitando acceso continuos a disco.
- Ejecutar cada servicio proxie registrándolo como un usuario no-privilegiado en un directorio privado y seguro del servidor de defensa.

Los gateway a nivel de aplicación son similares a los gateway a nivel de circuito, la diferencia es que los primeros utilizan aplicaciones específicas para el filtrado de información.

**Ventajas**

Tiene un nivel de seguridad alto, las reglas para filtrar la información de entrada y salida son mucho más fáciles de configurar que en un ruteador filtra-paquetes y puede monitorear los registros de los usuarios y su actividad en la red, creando herramientas de auditoría que pueden ser consultadas por el administrador para modificar o ajustar las políticas de seguridad, en caso de ser necesario.

**Desventajas**

El costo de implementación es considerable y se incrementa aún más por cuestiones de administración y soporte técnico, pues es necesario un experto que configure convenientemente el equipo de seguridad. Además, como el proceso de filtrado es exhaustivo provoca un impacto significativo en el rendimiento de la red. Por último, no es transparente al usuario ya que requiere una configuración manual en cada cliente de la red privada y puede ser que los servicios no se encuentren disponibles cuando el usuario los requiera.

***Gateway a nivel circuito***

Este dispositivo funciona en el nivel 5 (capa de Sesión) del modelo OSI o en el nivel 4 (capa TCP) del modelo TCP/IP.

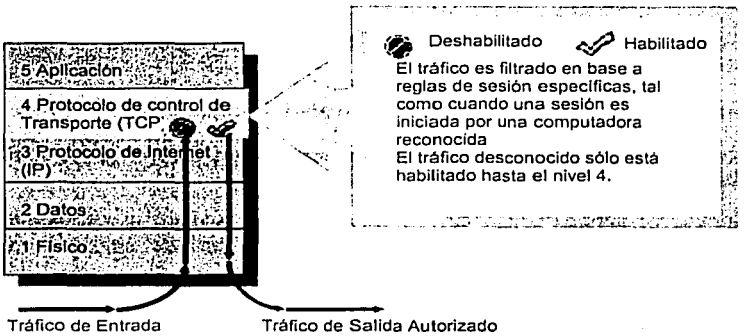


Fig. 4.8 Funcionamiento del gateway a nivel circuito

Se dice que este dispositivo es una función perfeccionada de un gateway a nivel de aplicación.

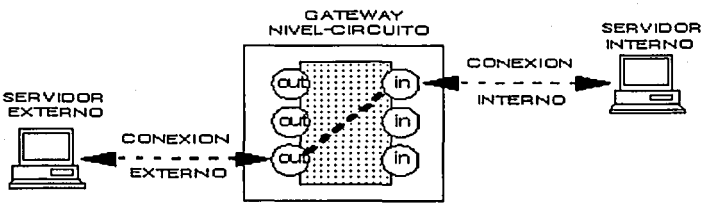


Fig. 4.9 Funcionamiento del gateway a nivel circuito



TESIS CON
FALLA DE ORIGEN

El gateway a nivel de circuito transmite la conexión a través del dispositivo sin examinarlo o filtrarlo, únicamente copia los bytes antes y después de la conexión interna y externa, donde la información se comporta, para esta última, como si se originara en el "**firewall**", protegiendo los datos de la red privada.

Un servidor de defensa puede ser implantado como un sistema híbrido, a través del siguiente esquema:

- Gateway a nivel de circuito para controlar las conexiones de salida.
- Gateway a nivel de aplicación para controlar las conexiones de entrada.

**Ventajas**

Asegura la información de redes protegidas a un costo relativamente bajo.

**Desventajas**

No se realiza el filtrado de paquetes individuales.

***"Firewall" de Inspección de estados multinivel***

Este dispositivo combina el "**firewall**" filtra paquetes, el gateway a nivel de circuito y el gateway a nivel de aplicación permitiendo filtrar paquetes a nivel de red, determinar si una sesión de red es legítima y evaluar el contenido del paquete a nivel de aplicación eliminando las limitaciones del gateway a nivel de aplicación.

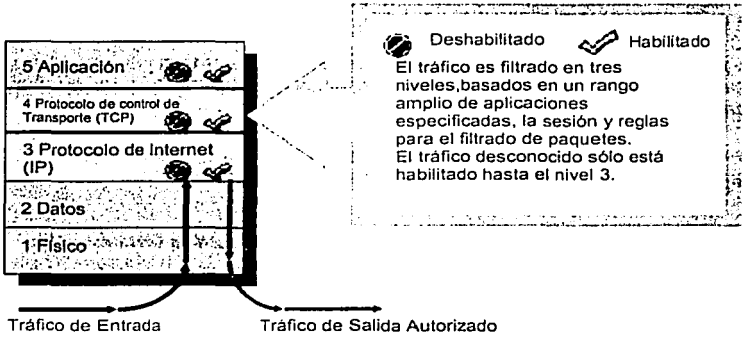


Fig. 4.10 Funcionamiento del "Firewall" de Inspección de estados multinivel

TESIS CON
FALLA DE ORIGEN

**Ventajas**

Ofrecen un alto nivel de seguridad y su implantación es transparente para los usuarios.

**Desventajas**

El costo de implantación es alto así como la administración, operación y mantenimiento generalmente resultan complejos, requiriendo para su realización personal técnico altamente calificado y con experiencia que, de no cumplirse, puede redundar en problemas de inestabilidad del sistema o fallas de seguridad.

## 2. SERVICIOS DE PROTECCIÓN AL PROCESO DE DATOS Y SU TRANSFERENCIA

A lo largo de este capítulo, se ha mencionado reiteradamente que un "**firewall**" es parte de un sistema integral de seguridad y que no es el sistema de seguridad por sí mismo. El "**firewall**" es un dispositivo que crea, alrededor de la red privada, una zona de protección para mantenerla a salvo de usuarios no autorizados intentando ingresar a sus servidores e información, previniendo posibles ataques.

El uso de Internet como red de comunicación implica que, a través de sus canales, viaja la información que deseamos intercambiar con otros sistemas o usuarios. Con el "**firewall**", la información procesada dentro de la red privada se encuentra protegida por nuestras políticas de seguridad, pero fuera de esa zona la información viaja libremente y es susceptible de sufrir ataques, es decir, puede ser vista, alterada, suplantada, interferida o destruida.

Para que las políticas de seguridad garanticen la validez de la información enviada o recibida, a través de una red pública, también debe asegurarse la integridad de los datos, la integridad de los servicios o de las aplicaciones, la confidencialidad de la comunicación y la autenticación de usuarios.

Como punto de partida para estar en posibilidades de establecer un esquema seguro de comunicación o de intercambio de información, a través de una red pública, es necesario dejar en claro la existencia de los siguientes conceptos:

- Riesgos en la comunicación o amenazas a la seguridad de la información.
- Tipos de ataque a la comunicación o a la seguridad de la información.

### 2.1 Riesgos en la comunicación o amenazas a la seguridad de la información

Debe entenderse por riesgo o amenaza, a un conjunto específico de condiciones que forman parte del entorno del sistema y que como tal, tiene la oportunidad o posibilidad latente de producir una violación a la seguridad de la información, transgrediendo sus atributos de confidencialidad, integridad, disponibilidad o autenticidad (uso legítimo).

La clasificación de estos riesgos o amenazas, considerando que la información es un flujo de datos con origen y destino, queda determinada conforme a las siguientes cuatro categorías:

- ***Interrupción o Disponibilidad.*** Que la información no llegue a su destino porque los recursos o servicios no estén disponibles por falla o destrucción.

- ***Intercepción o Confidencialidad.*** Que la información llegue a un destino no previsto porque una entidad no autorizada tenga acceso a recursos o servicios restringidos.

- ***Modificación o Integridad.*** Que la información sufra alteraciones porque una entidad no autorizada, además de tener acceso a recursos o servicios restringidos, tenga la posibilidad de aplicar cambios en ellos.

- ***Falsificación o Autenticidad.*** Que la información disponible o que llega a un destino sea apócrifa, generada por una entidad no autorizada o ambas.

## 2.2 Tipos de ataque a la comunicación o a la seguridad de la información

Los ataques a la comunicación o a la seguridad de la información, son aquellos actos que materializan los riesgos o amenazas descritas en el apartado inmediato anterior y su tipificación está directamente vinculada con la forma de actuar, quedando como sigue:

- **Ataques Pasivos**
- **Ataques Activos**

- ***Ataques pasivos.*** Cuando una entidad no autorizada observa la comunicación o la información sin alterarla, con el fin de obtener un conocimiento sobre su contenido y en casos específicos, realizar análisis de tráfico para afinar la administración del servicio. Este tipo de actos son difíciles de detectar y vulneran la confidencialidad mediante la intercepción de datos, cuyos principales objetivos podrían ser:

  - Identificar origen y destinatario.
  - Control de tráfico.
  - Control de horarios de demanda del servicio.
  - Identificar patrones de operación.

- ***Ataques activos.*** Cuando una entidad no autorizada realiza interrupciones, alteraciones o falsificaciones en la comunicación o la información, dividiéndose en las cuatro categorías siguientes:

  - ***Suplantación.*** La entidad no autorizada obtiene y adopta una identidad que no es la suya para actuar con derechos o privilegios sobre los recursos o servicios.

  - ***Reactuación.*** La entidad no autorizada detecta acciones válidas entre un origen y un destinatario repitiéndola hasta producir un efecto no deseado sobre los recursos o servicios.

  - ***Modificación.*** La entidad no autorizada detecta acciones válidas entre un origen y un destino alterando parcialmente los términos, condiciones o contenido así como el orden, tiempos de ejecución o terminación.

  - ***Degradación.*** La entidad no autorizada interfiere con el uso normal de los recursos y servicios impidiendo o inhibiendo la disponibilidad o gestión de los mismos.

## 2.3 Servicios de seguridad

La arquitectura del modelo OSI proporciona una descripción general de los servicios y mecanismos de seguridad utilizados para hacer frente a los ataques o amenazas que pueden realizarse sobre la información en el proceso de datos y en la transferencia de información.

La arquitectura de seguridad OSI clasifica los servicios de seguridad, de la siguiente manera:

- Servicios de autenticación
- Servicios de control de acceso
- Servicios de confidencialidad
- Servicios de Integridad
- Servicios de no repudio
- Servicios de disponibilidad

### Servicios de autenticación

En un proceso de comunicación es posible identificar tres elementos: el emisor, el receptor y el mensaje; cuando esta comunicación se establece a través de medios digitales el emisor y el receptor son personas representadas por una computadora, dado que las computadoras pueden ser manipuladas por cualquier persona, es necesario establecer reglas que garanticen que las personas apropiadas se están comunicando.

Los servicios de autenticación garantizan la identidad del emisor y/o del receptor, asegurando que el intercambio de información se realice entre las personas adecuadas.

Los servicios de autenticación son importantes, ya que tienen un impacto directo sobre las tareas de autorización y contabilidad. La autorización se refiere al proceso de concesión de derechos, la contabilidad se refiere a la propiedad que asegura que las acciones de un principal guardarán traza sólo para ese principal. Estos servicios se clasifican en dos:

- *Autenticación de entidad.*
- *Autenticación del origen de la información.*

#### Autenticación de entidad

Asegura que una entidad, emisor o receptor, es la autorizada para iniciar un proceso de comunicación, típicamente se realiza en la fase de conexión o, en ocasiones, durante la fase de transferencia de datos.

Pueden utilizarse diversos medios para realizar este proceso, tales como, pruebas biométricas (identificación de huellas dactilares o iris), uso de tarjetas de banda magnética o solicitud de contraseñas.

#### Autenticación del origen de la información

Asegura que la información recibida proviene de la persona apropiada, típicamente se realiza durante la transferencia de datos.

Para la autenticación del origen de la información, la firma digital es el procedimiento más utilizado, el cual se detalla en el apartado de mecanismos más adelante en este mismo capítulo.

**Servicios de control de acceso**

Estos servicios están orientados a la protección contra la utilización no autorizada de los recursos del sistema, tales como: información, capacidad de cálculo, nodos de comunicaciones y entidades físicas, entre otros.

Los servicios de control de acceso se encuentran estrechamente relacionados con los servicios de autenticación, ya que todo usuario o proceso debe autenticarse antes de que un servicio de control de acceso le permita ingresar a los recursos del sistema.

**Servicios de confidencialidad**

A través de los servicios de confidencialidad se asegura que, las entidades involucradas directamente en una comunicación, serán las únicas que tendrán acceso a los mensajes transmitidos.

El cifrado es el proceso más utilizado para implementar el servicio de confidencialidad, aunque también es posible incrementar el tráfico en la red mediante datos falsos para que el mensaje verdadero sea indistinguible para un intruso.

La desventaja, es que estos métodos incrementan drásticamente el tráfico en la comunicación y repercuten directamente en la velocidad de transmisión al disminuir el ancho de banda bajo demanda.

Los servicios de confidencialidad pueden proporcionarse a diferentes niveles:

- *Servicios de confidencialidad orientados a conexión.* Proporcionan privacidad a todos los datos transmitidos durante una conexión.
- *Servicios de confidencialidad no orientados a conexión.* Se busca la privacidad de unidades simples de datos.
- *Servicios de confidencialidad de campo selectivo.* Proporcionan privacidad de campos específicos de los datos durante una conexión o para una unidad de datos.
- *Servicios de confidencialidad de flujo de tráfico.* Protegen la información susceptible de obtenerse indirectamente mediante un análisis de tráfico, ocultando la identidad del origen, del destino o destinos y el mensaje.

**Servicios de integridad**

Previenen la modificación de la información enviada, lo que incluye escritura, cambio, eliminación, creación y reactuación de los mensajes enviados utilizando, en forma general, procedimientos criptográficos (Ver **Anexo 2. Criptografía**)

Los servicios de integridad pueden subdividirse en cinco tipos:

- *Servicios de integridad orientados a conexión con recuperación.* Los servicios se proporcionan a todos los datos durante una conexión y si es posible, permiten la recuperación cuando se detecta una alteración en la integridad de la información.

- *Servicios de integridad orientados a conexión sin recuperación.* Los servicios se proporcionan a todos los datos durante una conexión, no es posible recuperar los datos una vez que se detecta una alteración en la integridad de la información.

- *Servicios de integridad de campo seleccionado orientado a conexión.* Se proporciona integridad a campos específicos de los datos durante una conexión.

- *Servicios de integridad no orientados a conexión.* Se proporciona integridad a unidades de datos.

- *Servicios de integridad de campo seleccionado no orientados a conexión.* Proporciona integridad a campos específicos dentro de las unidades de datos.

**Servicios de no repudio**

Con estos servicios se garantiza la recepción o envío de la información transmitida en un proceso de comunicación, es decir, al implementar este servicio se coleccionan datos que prueban que un emisor envió información y que un receptor la recibió.

La clasificación de estos servicios es la siguiente:

- *Los servicios de no repudio con prueba de origen.* El receptor cuenta con los datos exactos del emisor de la información.

- *Los servicios de no repudio con prueba de destino.* El emisor cuenta con datos que confirman que el mensaje ha sido recibido por su destinatario.

**Servicios de disponibilidad**

Aseguran que los recursos del sistema podrán ser utilizados por usuarios autorizados cuando así se requiera.

## 3. MECANISMOS PARA PROVEER SERVICIOS DE PROTECCIÓN

Los servicios establecidos en la arquitectura de seguridad OSI se proveen a través de mecanismos de seguridad, no existe un mecanismo capaz de proveer todos los servicios mencionados, pero la mayoría de ellos utilizan técnicas criptográficas basadas en el cifrado de la información.

La arquitectura de seguridad OSI diferencia entre mecanismos de seguridad específicos y mecanismos de seguridad generalizados.

### 3.1 Mecanismos de seguridad específicos

La clasificación de los mecanismos de seguridad específicos, de acuerdo al modelo seguido por la arquitectura OSI, se encuentra establecido de la siguiente manera:

- Cifrado.
- Mecanismos de firma digital.

- Mecanismos de control de acceso.
- Mecanismos de integridad de datos.
- Mecanismos de intercambio de autenticación.
- Mecanismos de relleno de tráfico.
- Mecanismos de control de encaminamiento.
- Mecanismos de certificación.

Estos mecanismos pueden combinarse entre sí para proporcionar servicios de seguridad. Es conveniente indicar que los mecanismos de seguridad poseen tres componentes principales:

| | |
|---|---|
| **Información Secreta** | Claves y contraseñas conocidas sólo por entidades autorizadas. |
| **Algoritmos de Cifrado** | Procesos de cálculo que permiten la encriptación y desencriptación de información. |
| **Procedimientos de Aplicación** | Especificaciones de como y cuando se usaran los algoritmos de encriptación y desencriptación. |

**Cifrado**

Cuando la información viaja fuera de una red privada, deja de ser controlada y manipulada por los mecanismos y/o dispositivos de seguridad, implantados dentro de la red; por lo tanto, es posible que sufra un ataque pasivo, activo o ambos.

El cifrado de la información o criptografía, es la técnica que se encarga de proteger la información cuando se encuentra fuera de la red privada, garantizando que la información será comprendida únicamente por personas autorizadas a intervenir en el proceso de comunicación y consiste en la transformación de datos mediante la aplicación de procesos especializados. En el **Anexo 1, Criptografía**, se detallan los diferentes procesos y características del cifrado de información.

Este mecanismo puede ser utilizado de dos maneras:

- Para proteger la confidencialidad de las unidades de datos y la información de flujo de tráfico.
- Para complementar otros mecanismos de seguridad.

**Mecanismos de firma digital**

La firma digital es la rúbrica electrónica que identifica a una persona y de manera análoga a la manuscrita debe proveer la seguridad suficiente de no ser falsificada, permitir la posibilidad de ser verificada por los receptores y evitar la negación del suscriptor.

Para garantizar las propiedades de la firma digital que se mencionan en el párrafo precedente, es necesario disponer de una infraestructura capaz de asociar la identidad de una persona con elementos lógicos que, al aplicarlos sobre un documento, no conserve patrones de comportamiento a través de los cuales sea posible su falsificación o reproducción no autorizada.

Por lo anterior, la firma digital es una cadena de bits generada a partir de los datos a firmar en conjunto con la identificación electrónica privada del signatario, conforme al siguiente procedimiento:

- El firmante debe contar con una identificación compuesta de una pareja biunívoca de claves conocidas como pública y privada, respectivamente.

- El documento a firmar se somete a un algoritmo cuyo resultado es un número único e irrepetible que se utiliza en forma de resumen.

- El resumen es sometido a un proceso de cifrado mediante la clave privada del firmante, aplicación de un algoritmo cuyo resultado es la firma digital, cadena de bits que hace ilegible el resumen y sólo puede ser restaurado mediante la clave pública correspondiente.

- El documento original junto con la firma digital componen un documento firmado.

- La verificación del documento firmado se realiza descifrando el resumen mediante la clave pública del firmante y su comparación con un resumen del documento sin firma.

La diferencia entre la firma digital y la manuscrita, es que la firma digital varía y es única para el documento al que acompaña, en virtud de que, si se mantuviera siempre igual o siguiera patrones de comportamiento, podría ser identificada y permitiría generar documentos falsos.

Existen esquemas de firma digital arbitrados y no arbitrados. Los esquemas de firma digital arbitrados, se basan en la criptografía de la clave secreta, una tercera entidad de confianza que valida la firma y que la envía en lugar del firmante. Los esquemas de firma digital no arbitrados, no utilizan una tercera entidad para validar la firma, requieren el uso de criptografía con clave pública.

En general, un esquema de firma digital consta de los siguientes elementos:

- *Algoritmo para generación de claves*. Procedimiento de cálculo que permite la selección aleatoria de una pareja de claves denominadas pública y privada.

- *Algoritmo de firma*. Procedimiento de cálculo que mediante un mensaje de entrada y una clave privada generará como resultado un mensaje firmado digitalmente.

- *Algoritmo de verificación de firma digital*. Procedimiento de cálculo que mediante un mensaje firmado digitalmente y una clave pública generará como resultado información indicando si la firma corresponde o no a quien debió firmar.

**Mecanismos de control de acceso**

Con estos mecanismos se garantiza que, únicamente los usuarios autorizados por el administrador del sistema, podrán ingresar a los recursos del sistema.

Este mecanismo debe tener la habilidad de rechazar a los usuarios no autorizados y mantener una bitácora de incidentes. Adicionalmente, debe determinar los recursos que puede utilizar un usuario determinado.

En el **Anexo 2, Gestión de claves**, se trata con mayor detalle y profundidad el tema relativo a la administración de claves de usuarios.

### Mecanismos de integridad de datos

A través de estos mecanismos, se asegura que la información recibida por una entidad no ha sufrido alteraciones durante el proceso de comunicación.

Normalmente, este mecanismo implica la encriptación de una cadena de datos a transmitir, llamada valor de comprobación de integridad (ICV, *Integrity Check Value*). Este mensaje de resultado, se anexa al mensaje originalmente enviado para que, cuando sea recibido, la entidad receptora decodifique el ICV y compruebe que los datos no han sido alterados.

Es posible que solo se resguarden unidades de datos y campos dentro de las mismas unidades o secuencias de unidades de datos y campos dentro de dichas secuencias.

Los mecanismos de integridad de datos no protegen contra ataques tipo réplica, los cuales se refieren a la repetición sucesiva de eventos de transmisión y recepción de información hasta causar un efecto nocivo en los recursos, servicios o en la misma información.

### Mecanismos de intercambio de autenticación

Permiten corroborar que una entidad, origen o destino, es la autorizada en el proceso de comunicación. Se dice que, un mecanismo de intercambio de autenticación, es fuerte si se basa en el uso de criptografía para proteger el intercambio de información.

Las técnicas utilizadas para la autenticación se pueden dividir o agrupar conforme a los datos que conocen para autentificar una entidad, esta clasificación es la siguiente:

- Prueba por conocimiento
- Prueba por posesión
- Prueba por propiedad

La mayoría de los mecanismo de autenticación, implantados hoy en día, se basan en pruebas por conocimiento.

#### Prueba por conocimiento

Se basa en datos que el solicitante conoce, por ejemplo: los números de identificación personales (PIN, *Personal Identification Number*) y los números de autenticación de transacción (TAN, *Transaction Authentication Numbers*).

#### Prueba por posesión

Se basa en algo que el solicitante posee, por ejemplo, claves, tarjetas de identificación y otros dispositivos físicos o elementos personales.

#### Prueba por propiedad

Se basa en algunas características biométricas del solicitante, por ejemplo, las huellas dactilares, imágenes faciales, imágenes de retina y los patrones de voz.

**Mecanismos de relleno de tráfico**

Se utilizan para la protección del análisis de tráfico. Consiste en enviar tráfico ilegítimo junto con los datos válidos, el objetivo es no revelar si los datos transmitidos son reales o no. Los mecanismos de relleno de tráfico sólo serán efectivos si son protegidos por un servicio de confidencialidad de datos.

**Mecanismos de control de encaminamiento**

Se pueden utilizar para determinar rutas específicas para la transmisión de datos, permite enviar información sólo por determinadas redes o servidores de enlace consideradas como clasificadas. Del mismo modo, permite solicitar una ruta alternativa en caso de que se detecte una violación en la seguridad.

**Mecanismos de certificación**

El certificado digital puede definirse como un identificador único que garantiza la identidad y la capacidad del emisor y del receptor en un mensaje electrónico, la confidencialidad del contenido del envío, la integridad de la transacción y el no repudio.

Los certificados digitales son archivos o documentos electrónicos, que vinculan a una persona física o moral con una clave pública, vinculada a su vez a una clave privada. Este documento está firmado electrónicamente por una Autoridad de Certificación.

Una Autoridad de Certificación es la entidad encargada de gestionar el proceso de emisión de los certificados, la Autoridad de Registro es la autoridad que se responsabiliza del contenido de los certificados digitales, de su emisión y su validez.

## 3.2 Mecanismos de seguridad generalizados

Estos mecanismos no están asociados a un servicio en particular y pueden ser contemplados como aspectos de la administración de la seguridad. La arquitectura OSI diferencia cinco mecanismos de seguridad generalizados:

| |
|---|
| Funcionalidad de confianza |
| Etiquetas de seguridad |
| Detección de eventos |
| Rastreo de auditoría de seguridad |
| Recuperación de seguridad |

**Funcionalidad de confianza**

La funcionalidad de confianza se refiere a que el conjunto de medios, operaciones y procedimientos destinados a proveer mecanismos de seguridad o el acceso a los mismos son fiables, por lo que cumplen o cumplirán con el propósito o los propósitos para los que fueron hechos. En este sentido, la funcionalidad de confianza permite establecer la efectividad de los mecanismos de seguridad y abarca, de éstos, las propiedades que permiten extenderse hacia otros mecanismos ampliando la funcionalidad.

**Etiquetas de seguridad**

Se refiere a los elementos de información implícitos o adicionales que se asocian a los recursos, servicios o información protegidos; los cuales, implican o indican los niveles de seguridad aplicados y el estado que guardan. Por ejemplo, es posible indicar si un recurso compartido de impresión es público o privado, si un servicio de certificación está disponible o bloqueado, la técnica utilizada en el cifrado de datos, la fuente y ruta de los datos transmitidos, entre otros.

**Detección de eventos**

Son los mecanismos de seguridad destinados al control de eventos relativos al acceso, uso o disponibilidad de los recursos, servicios e información protegidos, permitiendo la detección de violaciones a la seguridad y el encadenamiento con otros eventos de registro, anulación, aislamiento, ubicación o prevención.

**Rastreo de auditoría de seguridad**

Se refiere a los datos e información que permiten el análisis de registro de actividades y la evaluación del funcionamiento de los sistemas. El análisis de registro de actividades, comprende la revisión particular de la información recopilada y registrada en bitácoras correspondientes a las diversas actividades que se realizan a través de o por los sistemas. La evaluación del funcionamiento, es el examen aplicado al conjunto de medios, operaciones y procedimientos que conforman el sistema incluyendo aquellos que proveen mecanismos de seguridad.

El rastreo de auditoría es utilizado por el administrador del sistema como apoyo a la toma de decisiones, en relación a la gestión de controles de seguridad, con la finalidad de asegurar la correcta operatividad y el cumplimiento de políticas y procedimientos operacionales, así como, para estar en condiciones de proponer los cambios o ajustes correspondientes.

**Recuperación de seguridad**

Son mecanismos de seguridad orientados a realizar acciones para que los recursos, servicios o información protegidos reestablezcan sus condiciones o estado de seguridad previos a un evento determinado, observando la aplicación de reglas específicas de recuperación.

Los mecanismos de recuperación atienden solicitudes provenientes de las funciones de gestión o de otros mecanismos, tales como: los gestores de eventos.

## 4. CULTURA DE SEGURIDAD

Si tomamos en consideración los niveles de conectividad, automatización e infraestructura tecnológica que existen, así como las tendencias de evolución y crecimiento que mantienen, es simple entender que la seguridad tiene un papel preponderante para garantizar que, la información junto con los sistemas, estarán en posibilidades de mantener sus atributos y flujos de comunicación, seguirán funcionando y no serán alterados o interrumpidos.

En este sentido, implantar un esquema de seguridad podría parecer suficiente, sin reparar en el costo o las implicaciones que pudiera tener. El establecimiento de una infraestructura dedicada a robustecer la protección de la información y de los sistemas de cómputo y telecomunicaciones, así como para reducir las vulnerabilidades, es equivalente a equipar nuestro hogar con sistemas de detección de intrusos, chapas y alarmas electrónicas, vigilancia por circuito cerrado y más.

Sin embargo, basta revisar el comportamiento del ser humano para darnos cuenta de la falta de elementos que complementen la simple imposición de restricciones o medios de vigilancia y supervisión, pues bastará que algún integrante de la familia deje la puerta abierta, sea sorprendido antes de entrar al hogar o permita el paso a personas desconocidas para provocar que el sistema de seguridad implantado quede inhabilitado para cumplir su función.

De lo anterior, podemos desprender lo siguiente:

- La implantación de un esquema de seguridad es el conjunto de elementos que permiten restringir, vigilar o supervisar el acceso, uso y disponibilidad de los recursos protegidos.

- Los resultados y el buen desempeño de la función del esquema de seguridad está ligada directamente a la forma de actuar de los individuos que administran, operan y utilizan tanto los recursos protegidos como el esquema de seguridad mismo.

Ahora bien, el reto surge ante la necesidad de lograr fiabilidad en las acciones de los individuos que participan en la administración, operación y uso tanto de los recursos protegidos como del esquema de seguridad. En este sentido, no importa cuan redundante puedan ser los elementos de control y supervisión, los actos voluntarios e involuntarios del ser humano en contra de la seguridad siempre existirán y permanecerán latentes, con fines específicos o sin ellos.

Detenernos en una discusión filosófica sobre la naturaleza del ser humano podría consumirnos y probablemente llegaríamos a la conclusión de que los individuos respondemos de diversas formas ante un mismo hecho o mejor aún, que un individuo responderá de forma distinta ante un mismo evento que se repite, mientras que otro actuará de una misma forma ante un evento que se repite bajo distintas circunstancia. En consecuencia, tendríamos un sin fin de configuraciones con las que sólo complicaríamos más la concepción de un sistema seguro, pues es claro que cada individuo tiene un mundo propio por así decirlo.

Bajo el esquema descrito, encontrar el camino hacia los sistemas integrales de seguridad, donde el factor humano deja de ser un riesgo y se convierte en un valor agregado parece una tarea titánica. Sin embargo, el análisis y revisión del concepto general de cultura nos hace concluir lo siguiente:

***Los actos, en la mayoría de los individuos, son el resultado de los valores, creencias y actitudes aprendidas a lo largo de sus vidas, lo que determina la percepción que tienen del medio y su comportamiento.***

La afirmación anterior, seguramente expresada de formas distintas pero conocida por muchos, es uno de los legados más comunes entre padres e hijos, cuando estos últimos son recriminados por la forma de comportarse o de vivir e invariablemente devaluados por el tipo de decisiones tomadas o compañías seleccionadas, siendo estas últimas la influencia nociva que ha modificado todas las buenas costumbres enseñadas dentro de la familia.

La reflexión sobre esta expresión está encaminada a que el ser humano establece redes sociales en las que actúa y aprende, generando a su vez un entretejido de símbolos y significados que le permitirán interpretar su existencia, así como las experiencias vividas. En adición, durante la interacción social, el individuo también cubre necesidades fisiológicas y emocionales, entre las que destaca la búsqueda de comodidad, supervivencia y reproducción.

Con la intención de generalizar nuestra afirmación, debemos recordar que cuando nos referimos a una sociedad, estamos refiriéndonos a un grupo de gente con determinadas estructuras y manifestaciones sociales, religiosas, políticas, económicas e intelectuales aceptadas y compartidas por cada uno de los integrantes del grupo. Tales manifestaciones son el conjunto de valores, creencias y actitudes que

determinan la ***cultura de una sociedad***, con base en la cual, los integrantes de dicha sociedad interpretan el medio y sus actos.

En este entendido, si establecemos como ***sociedad*** al grupo de gente que administra, opera y utiliza tanto los recursos protegidos como la infraestructura de seguridad y deseamos que las manifestaciones de ese grupo de gente sean el conjunto de valores, creencias y actitudes que coadyuven al mejor desempeño de la función de protección y disminución de vulnerabilidades, resulta imponderable la necesidad de constituir una ***cultura de seguridad*** que oriente la forma de interpretar el medio y los actos de los individuos.

### 4.1 Definición

Para nuestros propósitos, la cultura de seguridad es el conjunto abstracto de conocimientos, conductas y herramientas que se requiere para lograr flujos de información libres y protegidos, manteniendo el derecho a la privacidad personal y a mantenerse informado mediante la adopción de patrones de comportamiento compartidos por el grupo de individuos que participan en el proceso administrativo, operativo y de uso de la información y de los sistemas de cómputo y telecomunicaciones en que ésta se procesa y distribuye.

### 4.2 Objetivos

La promoción y logros de una cultura de seguridad, deberán estar sustentados en los siguientes objetivos:

- Conocimiento profundo sobre las amenazas y ataques a los que están expuestos la información, los sistemas de cómputo y telecomunicaciones e individuos.
- Uso y aprovechamiento efectivo de la infraestructura de seguridad implantada.
- Definición clara del papel que ocupa cada individuo, así como de los alcances y límites de su participación.
- Adopción de conductas dentro y fuera de las instalaciones para prevención de incidentes.
- Observación de patrones de comportamiento para la detección y atención de incidentes.
- Protección de los intereses de grupo e individuales mediante el respeto al derecho de privacidad y de estar informado.

### 4.3 Características

Como se ha mencionado, hablar de cultura es hablar del cúmulo de culturas individuales o personales compartidas en un grupo social; es decir, la cultura de un grupo social es el resultado de la relación circular que existe entre la interpretación del medio, los actos, la experiencia adquirida y sus efectos en otros individuos del grupo.

Pensar que para lograr una cultura de seguridad, basta con aplicar un modelo predefinido, implicaría que los resultados serían tan diversos como cada grupo social al que se aplique.

Debemos comprender que la cultura es un proceso especial y único para cada grupo social y se logra respetando los principios universales que la caracterizan; por lo tanto, para definir la forma en que se debe implantar un proceso de culturización basta con describir tales características:

- ***Es un código simbólico.*** Se debe establecer un medio de comunicación eficaz que permita expresar y entender ideas claras y precisas relativas a la seguridad ya sea a través del lenguaje, señales o cualquier otra expresión simbólica.

- ***Está clasificada.*** Se deben establecer taxonomías que permitan estandarizar la clasificación que se hace de la realidad, incluyendo eventos, incidentes, operaciones y definiciones entre otros.

- ***Es arbitraria.*** Se debe orientar y convencer sobre los beneficios de adoptar una cultura de seguridad, permitiendo y motivando la participación activa de los integrantes del grupo social, con la intención de alcanzar un modelo propio de comportamiento que coadyuve a la protección y la seguridad.

- ***Se aprende.*** Se deben establecer esquemas continuos de enseñanza y aprendizaje en el sentido estricto de la seguridad.

- ***Se comparte.*** El crecimiento de una cultura se sustenta en generar más conocimiento compartiendo el que ya se tiene. Todos los integrantes del grupo tienen algo que aportar en materia de seguridad, conocimiento que se debe aprovechar y reunir haciendo del conocimiento un bien público.

- ***Es conocimiento.*** La cultura de seguridad deben ser los actos cotidianos aprendidos en forma implícita o explícita bajo causas y efectos del comportamiento que presente cada integrante del grupo.

- ***Es adaptable.*** La cultura de seguridad debe estar continuamente adaptándose a los nuevos requerimientos tecnológicos y funcionales así como a los cambios de otros grupos sociales con los que se interactúa.

- ***Es mutualista.*** Se deben dedicar esfuerzos para lograr que cada integrante acepte el hecho de que el beneficio individual es resultado de la cooperación y participación en grupo. Observando iguales patrones de comportamiento es posible la convivencia y beneficio recíproco.

- ***Es continua.*** Deben establecerse esquemas que permitan la incorporación de nuevos integrantes al grupo, asimilando en forma organizada y estructurada el conocimiento sobre seguridad.

- ***Es subjetiva.*** La cultura por si misma es el resultado de como interpretamos el medio, la experiencia y nuestros actos pero no necesariamente concuerda con la realidad que está ocurriendo. Es conveniente establecer procesos de revisión de eventos e incidentes que permitan esclarecer la realidad de las interpretaciones sobre seguridad.

En este sentido, es posible consultar las ***Guías para la Seguridad de los Sistemas de Información y Redes*** desarrolladas por la Organización de la Cooperación y Desarrollo Económicos (OCDE).

## 4.4 Reglamentación

Como elemento final, debemos abordar el tema de la reglamentación, pues como podemos deducir, la cultura y la sociedad están vinculadas estrechamente, debiendo existir reglas básicas que fomenten el respeto entre individuos y permitan sancionar la no observancia de estas reglas a manera de medida disciplinaria, correctiva o de educación.

La cultura de seguridad también debe comprender el conjunto de reglas y principios que determinen la forma en que deben actuar los integrantes de un grupo. Cada regla se debe referir específicamente a una acción, medio o procedimiento detallando las condiciones, derechos y obligaciones de los participantes, con la finalidad de lograr la protección y seguridad de la información y sistemas de cómputo y telecomunicaciones en que se procesa y distribuye.

El objetivo principal de contar con una reglamentación sobre seguridad es: proteger el derecho a la privacidad y mantenerse informado; asegurar que la información es oportuna, confiable y completa; mantener el uso racional de los recursos de cómputo y telecomunicaciones; y, establecer los criterios de actualización de tecnología en materia de seguridad, informática y telecomunicaciones.

La característica más sobresaliente de la reglamentación, es que debe constituirse como un documento oficial aceptado por el grupo social estableciendo derechos y obligaciones para cada uno de los participantes, debiendo estar disponible para consulta de todos ellos.

Adicionalmente, deberá contemplar las condiciones en que un acto podrá ser considerado en contra de la seguridad o no y manejar en forma clara, exacta y precisa cada uno de los términos y condiciones en que una acción se considere ataque o amenaza a la seguridad, requiriendo seguramente un análisis de riesgos y vulnerabilidades.

### Legislación

En complemento a lo expresado en el apartado de Reglamentación, es necesario resaltar que el uso de los medios electrónicos conlleva a una serie de implicaciones legales, en lo que a operaciones comerciales, económicas o gubernamentales se refiere. Si bien, el número de transacciones realizadas se incrementa sustancialmente con la incorporación de los medios electrónicos de comunicación, también es cierto que los riesgos de una operación no válida se incrementan.

Los esfuerzos internacionales por establecer leyes, normas y estándares que regulen las transacciones electrónicas deben encontrar eco en los esfuerzos internos de cada país por regular este tipo de operaciones. No obstante, los niveles tecnológicos, económicos, culturales, sociales y políticos de cada nación, son factores determinantes para marcar el ritmo con que esta legislación puede crecer. La idiosincrasia de un pueblo puede o no permitir que se regulen formalmente las operaciones electrónicas, quizá es irremediable que suceda pero, hasta la fecha, falta mucho por hacer en materia de legislación electrónica internacional y la no menos importante, la legislación nacional.

En este sentido, aunque no menos incipiente que como en otros países considerados de primer mundo, México está alcanzando importantes avances en materia de normas para el comercio electrónico y el uso de firma electrónica, el 4 de junio de 2002, se publicó en el Diario Oficial de la Federación la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos. Dicha norma persigue el siguiente objetivo:

***"establece los requisitos que deben observarse para la conservación del contenido de mensajes de datos que consignen contratos, convenios o compromisos y que en consecuencia originen el surgimiento de derechos y obligaciones".***

En México, es claro que aún falta mucho para alcanzar jurídicamente un Derecho Electrónico o de Informática, sin embargo, existen leyes que establecen un marco de referencia, tales como:

- Ley Federal de Telecomunicaciones.
- Ley Federal del Derecho de Autor.
- Ley de Información Estadística y Geográfica.
- Ley de la Propiedad Industrial.

Por otra parte, en el Código Penal se contemplan formas de delito informático e incluye temas como la "Revelación de Secretos y el Acceso Ilícito a Sistemas y Equipos de Informática".

Asimismo, la Administración Pública Federal ha instrumentado diversas instancias con atribuciones en materia de informática, operaciones electrónicas y telecomunicaciones dentro de sus organismos, que son:

- Las Secretarías de Gobernación, Economía, Hacienda y Crédito Público, Comunicaciones y Transportes, Educación Pública, Contraloría y Desarrollo Administrativo y Relaciones Exteriores.

- Otros organismos especializados como son la Comisión Federal de Telecomunicaciones y el Consejo Nacional de Ciencia y Tecnología.

La importancia de la legislación se deriva de la necesidad que existe de contar con instancias ante las cuales sea posible recurrir para comprobar si una operación se efectuó o no, si los servicios proporcionados cumplen con un mínimo razonable de calidad o si se dio cumplimiento a los compromisos contraídos o contratados electrónicamente. En términos generales y en materia de operaciones electrónicas y sistematización, es necesario que existan leyes que garanticen lo siguiente:

- Protección a los derechos y determinación de obligaciones (privacidad, información pública, confidencial y restringida, niveles mínimos de prestación de servicios, propiedad intelectual, etcétera).

- Protección a los activos individuales o de grupo (información, comunicación, equipo, sistemas, servicios, productos de desarrollo técnico, etcétera).

- Fundamentación de la reglamentación interna de las organizaciones públicas o privadas (seguridad, recursos humanos y materiales, condiciones generales para la prestación de servicios, etcétera).

# CAPÍTULO 5
# PROPUESTA DEL TEMA DE SEGURIDAD EN REDES PARA LA ASIGNATURA DE REDES DE COMPUTADORAS

Como se ha mencionado a lo largo de este trabajo de tesis, las redes de computadoras de área local junto con las de área amplia e Internet han gestado cambios drásticos en la actividad humana, estos van desde la reducción de tiempos en la comunicación hasta la creación de nuevas formas de comercialización. Hoy día existen mercados electrónicos en los que es posible encontrar y comprar casi cualquier cosa, es posible mantener comunicación en línea entre los lugares más remotos del mundo por el costo de una llamada local, las instituciones bancarias y financieras proporcionan servicios de transferencia de fondos e instrucciones de compraventa donde el dinero puede moverse de un país a otro en tiempos verdaderamente cortos y la información así como las noticias están disponibles prácticamente al instante, entre otras características, esto es parte del mundo moderno.

La política de globalización desarrollada en el mundo sin duda tiene beneficios y aún cuando la intención no es opinar sobre este tema, debemos considerar que los primeros efectos evidentes son el desquiciamiento económico y la crisis financiera que sufren los países ante un evento de desequilibrio político o social. En este contexto, imaginemos a un inversionista que, en determinado país, tiene a su alcance información relativa a la devaluación de la moneda antes de que tenga efecto la declaración pública; sin mayores riesgos, seguramente transferirá su capital a otro país o por lo menos cambiará el tipo de moneda de su inversión. Lo que aparentemente resulta una situación conveniente para un individuo que pudo hacerse de información privilegiada, tiene efectos totalmente perjudiciales para un país completo y sólo son suficientes unos breves minutos.

Situaciones similares a la descrita, más allá de causar desaliento o de provocar desaprobación hacia el uso y evolución de los sistemas de comunicación, deben sensibilizarnos en la necesidad de los esquemas de seguridad y en la importancia de una cultura que, en ese mismo sentido, desarrolle cotidianamente una frontera preventiva en el hogar, la escuela, el trabajo y cualquier sitio en el que nos encontremos. La simbiosis entre datos y medios de enlace promueve un campo de batalla en el que los sistemas de comunicación luchan por proporcionar servicios que garanticen la integridad, confiabilidad y oportunidad de la información transmitida librando obstáculos mediante la prevención, detección y corrección.

Así, para llevar a cabo el diseño, desarrollo e implantación de un sistema de comunicación, es necesario lo siguiente:

- Determinar los requerimientos de información y de servicios de enlace e intercambio de datos a proporcionar.
- Conocer las herramientas y técnicas aplicables para garantizar la integridad, confiabilidad y oportunidad de los flujos de información.
- Determinar los dispositivos que se utilizarán en la implantación de la solución.

Adicionalmente, otro aspecto a considerar por el Profesional responsable de proponer la solución a los requerimientos de información y servicios de comunicación es que, en muchos de los casos, los sistemas son parte integral de las estrategias de negocio; por lo tanto, debe realizar y documentar la identificación de los riesgos asociados al proceso y sus efectos, considerando que el establecimiento de mecanismos de prevención, detección o corrección modifican los escenarios de control de la organización.

En lo relativo a la educación sobre riesgos y seguridad, los especialistas presentan criterios divergentes acerca de los resultados a obtener. Algunos opinan que al proporcionar capacitación sobre situaciones peligrosas o ilícitas como el secuestro, por ejemplo, sólo constituye una forma de especializar al secuestrador o de incentivar al delito a aquellos que no lo consideraban como una opción. Otros, siguiendo con el mismo ejemplo, mantienen la postura de que el conocimiento sobre la forma de operar del secuestrador permite estar en condiciones de establecer medidas de control y seguridad encaminadas a limitar su campo de acción minimizando el riesgo.

Ahora bien, debemos tener presente que tanto la sociedad como la tecnología se encuentran en franca evolución y conllevan efectos impredecibles, los cuales, sólo con el paso del tiempo serán identificables.

En este ambiente, consideremos que somos profesores y tenemos información fidedigna sobre secuestros que están ocurriendo fuera del centro escolar. ¿Debemos hablar sobre este tema con los alumnos? ¿Debemos explicarles la forma en que el secuestro se está llevando a cabo?.

De igual manera que en los temas de seguridad personal, podría resultar cuestionable la conveniencia de proporcionar conocimientos específicos sobre seguridad en sistemas operativos y redes, necesarios para prevenir un ataque a los equipos de cómputo o a los sistemas de comunicación. Sin embargo, un maestro ineludible, la historia, nos ha enseñado que la ignorancia, la desinformación, la falsa educación así como la información en exceso son nocivas, y sólo el equilibrio entre información, conocimiento y cultura permite el adecuado aprovechamiento de los medios y de los recursos. Por lo tanto, consideramos que la difusión de información y conocimiento es el único medio por el cual se puede crear una conciencia de seguridad informática, soportada en una cultura del mismo género que establezca tanto principios como valores de respeto y convivencia para una sociedad interconectada electrónicamente.

La evolución electrónica de los servicios y del comercio a influido directamente en la aparición e incremento de los delitos informáticos, derivando en la concebida necesidad de contar con personal capacitado en el área de seguridad en informática para contrarrestarlos o prevenirlos. En esta tendencia, las universidades del mundo han creado e incorporado programas de estudio específicos con el objetivo de formar profesionales especializados en las áreas de seguridad en cómputo y telecomunicaciones. Asimismo, en algunos casos, abordan el tema de cultura de seguridad, el cual ha tomado tal relevancia que, como se menciona en el capítulo anterior, es motivo de unas guías emitidas por el OCDE, conjunto de los principales elementos necesarios para conformar dicha cultura determinados por ese organismo internacional.

Los programas de estudio referidos están orientados a egresados de las carreras de computación, telecomunicaciones y sistemas entre otras; en su mayoría, se imparten con el grado de diplomado basándose en temarios que abarcan los diferentes aspectos de seguridad en Informática, en forma por demás amplia, y con una duración que va desde los seis meses hasta los dos años.

Nuestra Universidad Nacional Autónoma de México (UNAM), no es la excepción en este proceso de atención a las necesidades de preparación en materia de seguridad, a través del Centro Educativo Multidisciplinario (CEM), ubicado en la colonia Polanco del Distrito Federal, Ciudad de México, imparte el Diplomado Seguridad Informática, con duración de seis meses y se está aplicando como opción para titulación en la Licenciatura en Informática de la Facultad de Contaduría y Administración, de la misma UNAM.

Desde otro punto de vista, las condiciones de costo, horario y difusión para impartir el diplomado citado en el párrafo precedente, le convierten en una posibilidad de estudio prácticamente inaccesible para los profesionistas activos del país en las áreas de computación, telecomunicaciones y sistemas.

Con otros alcances, el mismo CEM cuenta con Talleres de Seguridad Informática en los que ofrece preparación y conocimiento sobre herramientas de seguridad, existentes en el mercado, así como el correspondiente análisis de los aspectos de adquisición, instalación, configuración y uso. Las condiciones en que se desarrollan dichos talleres y que limitan su demanda, son: corta duración, herramientas específicas, conocimientos previos indispensables, alto costo y horarios poco flexibles.

La Carrera de Ingeniería en Computación que se imparte en la Facultad de Ingeniería de la UNAM, como parte de su plan de estudios, incluye la materia optativa Temas Especiales de Computación cuya lista de temas disponibles abarca el curso referente a riesgos de la información y sus correspondientes mecanismos de seguridad. Sin embargo, por tratarse de una materia que propone la elección de un tema en particular para un curso específico, el temario y su desarrollo quedan a criterio del profesor designado para impartirlo; además de que, por ser optativa o de carácter opcional, los alumnos están en posibilidad de decidir si cursar dicha materia o elegir otra en sustitución. En consecuencia, no es posible garantizar que semestre a semestre los diferentes alumnos de cada generación escolar aprenderán sobre el tema de riesgos de la información y sus mecanismos de seguridad.

En virtud de lo expuesto en este capítulo, con la firme intención de obtener los mejores resultados de análisis y para estar en condiciones de proponer la mejor opción de modificación al temario de Redes de Computadoras, realizamos un trabajo de investigación relacionado con los temas de seguridad informática que se imparten a través de diferentes planes de estudio, en reconocidas universidades del mundo, para su posterior comparación con el alcance y temas que conforman este trabajo de tesis.

Cabe recordar y señalar, que el presente trabajo de tesis se refiere al tema de seguridad en Internet a diferencia del tema de seguridad informática que se abarca en los planes de estudio investigados.

A continuación, se presenta el cuadro resumen resultado de la investigación y comparación de los temas sobre seguridad. Para su mejor comprensión, en dicho cuadro, cada tema desarrollado en este trabajo de tesis ha sido identificado mediante un matiz de gris en particular, con este mismo matiz, en los planes de estudio de las diversas universidades se identificaron los temas coincidentes.

| Temas de esta Tesis | Temario de Temas Especiales de Computación F.I. UNAM Ciudad Universitaria | Universidad Politécnica de Madrid Posgrado en Seguridad Informática | Universidad de Granada Materia Optativa: Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| Conceptos Fundamentales y Arquitecturas Básicas. Definición de red. Objetivos de las redes. Tipos de Redes. Modelo OSI. Modelo TCP/IP. Direcciones IP. | Introducción Panorama General de la seguridad (antecedentes, desarrollo y necesidades) | Introducción a la Seguridad Informática: Amenazas, salvaguardas y objetivos de la seguridad. Organización, Administración y Control de la Seguridad. | Introducción a la seguridad de sistemas informáticos. Métodos de protección: Problemas de seguridad en sistemas informáticos. Necesidades de protección. Métodos utilizados. | How to think about security Storing data securely on insecure media: Integrity Authenticating People Message authentication codes and random numbers | NETWORK TECHNOLOGY. Networking concepts, network topologies, network architectures, network operating systems, LANs, WANs, networking protocols, cabling, routers, bridges, repeaters, wireless technologies, OSI model, and emerging networking tech. |



TESIS CON
FALLA DE ORIGEN

| Temas de esta Tesis | Temario de Temas Especiales de Computación F.I. UNAM, Ciudad Universitaria | Universidad Politécnica de Madrid, Posgrado en Seguridad Informática | Universidad de Granada, Materia Optativa: Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| INTERNET<br>Historia de la Internet<br>Definición de la Internet<br>Servicios<br>Tendencia<br>Vulnerabilidad de la Internet | Ataques de Seguridad<br>Definición<br>Clasificación General (Interrupción, Intercepción, Modificación, Fabricación)<br>Otras clasificaciones (Ataques Pasivos, Ataques activos)<br>Métodos de ataque | Metodología para el análisis y evaluación de riesgos. La gestión del riesgo | Técnicas criptográficas básicas y avanzadas:<br>Técnicas de cifrado elementales.<br>Criptoanálisis.<br>Algoritmos de llave privada: DES<br>Algoritmos de llave pública: RSA. | Stream Ciphers<br>Block Ciphers<br>Public Key Crypto<br>Key exchange and key management<br>Putting it together: The SSH Protocol<br>Protecting Host from malicious programs | OPERATING SYSTEMS<br>review of the main operating systems used in networking today. |
| REDES Y SISTEMAS OPERATIVOS SEGUROS<br>Amenazas a la seguridad<br>Seguridad Externa<br>Seguridad Interna<br>Mecanismos de Seg. Interna<br>Planes de Seguridad<br>Evaluación de Sistemas Seguros | Fundamentos de la Seguridad<br>Definiciones<br>Niveles de Seguridad<br>La seguridad en las configuraciones de los sistemas. Los sistemas operativos | La seguridad física. Amenazas y medidas de salvaguarda<br>La seguridad de los datos: Control de acceso de datos, criptografía, software de seguridad<br>La seguridad en las configuraciones de los sistemas. Los sistemas operativos | Protocolos básicos:<br>Firmas digitales.<br>Funciones Hash.<br>Protocolos de intercambio de llaves.<br>Otros protocolos | Buggy programs and security<br>Access Control<br>Information Flow and Multi-Level Security<br>Network Security<br>Protecting the Infrastructure | DATA ARCHITECTURE AND MANAGEMENT<br>data architecture and management are discussed including database design, database security, and data integrity. Data warehouses, database servers and database reporting applications. |
| SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES<br>Políticas de Seguridad entre una red privada e Internet<br>Servicios de protección de datos y su transferencia<br>Mecanismos para proveer servicios de protección<br>Cultura de seguridad | Servicios de Seguridad<br>Definición<br>Clasificación (Confidencialidad, Autentificación, Integridad, No repudio, Control de acceso, Disponibilidad) | La seguridad en las comunicaciones.<br>Las redes físicas.<br>Los entornos. Los contenidos en los mensajes.<br>Virus y Hackers.<br>El negocio electrónico y el comercio electrónico | Seguridad en sistemas operativos:<br>Debilidades de los S.O.<br>Elementos de diseño en la seguridad de los S.O.<br>Clasificación de los S.O. En cuanto a seguridad | Firewalls and Virtual Private Networks<br>Privacy and anonymity<br>E-commerce security<br>E-Commerce security: Off line systems<br>Formal methods<br>Protecting programs against hosts<br>Intellectual property and copy protection | TCP/IP ARCHITECTURE<br>Full in-depth coverage of the current TCP/IP protocol. Overview of the implications of the upgrade to 128 bit TCP/IP due within 2 years. |

TESIS CON
FALLA DE ORIGEN

| Temas de esta Tesis | Temario de Temas Especiales de Computación F.I. UNAM Ciudad Universitaria | Universidad Politécnica de Madrid Posgrado en Seguridad Informática | Universidad de Granada Materia Optativa: Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| Anexo 1 CRIPTOGRAFÍA | Criptografía Principios de la criptografía Criptografía simétrica o de clave secreta Criptografía asimétrica o de clave pública | Seguridad en los entornos departamentales. Las políticas de seguridad de la información | Seguridad en bases de datos: Requisitos de seguridad. Integridad. Datos sensibles. Seguridad multinivel | INTRODUCTION TO SYSTEMS SECURITY - The course covers a basic understanding of information systems security issues, policies, practices, and procedures applicable to information systems security. The course also covers the analysis of basic security methods for Microsoft, Novell, and Unix operating systems. The importance of physical security measures will be covered in depth, as it is the most important security element in information systems security. | E-COMMERCE SERVER APPLICATIONS Network protocols are covered at an advanced level. Examination of performance, capacity, routability, security and integrity issues surrounding today's major LAN/WAN internet working protocols. |
| Anexo 2 GESTIÓN DE CLAVES | Seguridad en una organización Objetivos o misión de la organización Definición de política (principios fundamentales) Definición de modelos (criterios) Modelos de Control de acceso (Matriz de control de acceso, Modelo Take-Grant, Modelo Bell-LaPadula) Modelos de Flujo de información Modelos de Integridad (Modelo Biba, Modelo Clark-Wilson) | La seguridad en la operación de Sistemas. La operación de las computadoras y de las redes. La preparación de los datos. La gestión de librerías. El help desk y soporte técnico. Planificación de la capacidad y la evaluación del rendimiento. La gestión de la externalización de servicios (Outsourcing) | Seguridad en redes de computadoras Seguridad en las comunicaciones Soluciones: Autentificación e identificación. | | ADVANCED NETWORK SECURITY Review of the network environment and any enterprise resource considerations for planning network connectivity and security. Security components for authentication access control, and security software are highlighted and applied in labs. Protection mechanisms that are designed into operating systems to protect information systems. |

TESIS CON
FALLA DE ORIGEN

| Temas de esta Tesis | Temario de Temas Especiales de Computación, F.I. UNAM, Ciudad Universitaria | Universidad Politécnica de Madrid, Posgrado en Seguridad Informática | Universidad de Granada, Materia Optativa: Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| ANEXO 3 NETIQUETTE | Mecanismos de Seguridad Tipos (Intercambio de autentificación, Integridad de datos, Firma Digital, Control de acceso, Tráfico de relleno, Control de encaminamiento, Unicidad, Cifrado) | La seguridad en el diseño y construcción de aplicaciones. Garantía de calidad del software. La propiedad y certificación del software | Seguridad del software: Métodos básicos. Módulos inteligentes. Identificación | | CRYPTOGRAPHY AND SECURE NETWORKS COMMUNICATIONS Securing data through authentication, cryptographic algorithms, access control, public key encryption and public key distribution. |
| | Seguridad en Internet Vulnerabilidades Estándares de seguridad Mejorías de los protocolos Seguridades en WWW | La seguridad y las personas. Los controles de seguridad. Identificación Personal. | Virus informáticos. Tipos de virus. Métodos de protección de programas y sistemas. | | FIREWALL FUNDAMENTALS Introductory concepts on firewall technology. Planning, formation, management, and operation of security inside, outside and through the firewall. Evaluation of the effectiveness of a firewall design. |
| | | Plan de seguridad. Los planes de contingencia. Planes de recuperación de desastres | Análisis de riesgos y auditoría. Análisis de riesgos. Plan de seguridad. Auditoría de seguridad. | | FINANCIAL MANAGEMENT AND ANALYSIS Financial management theory and financial statement analysis. Financial proposals for new equipment needed for an information security enhancement. |
| | | Privacidad y Legislación sobre protección de datos | Seguridad y privacidad en Internet. Problemas de seguridad en Internet Servidores y hojeadores seguros. Los protocolos SSL y S-HTTP. Anonimidad en la red. | | SYSTEMS DEVELOPMENT AND PROJECT MANAGEMENT concepts and techniques for designing, developing and/or revising software using a planned approach. Both the software development life-cycle model and project management approach is presented. |

TESIS CON
FALLA DE ORIGEN

| Temas de esta Tesis | Temario de Temas Especiales de Computación F.I. UNAM Ciudad Universitaria | Universidad Politécnica de Madrid Posgrado en Seguridad Informática | Universidad de Granada Materia Optativa Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| | | Elementos de seguridad física. Normas, diseño y dispositivos. | | | SECURITY POLICIES, STANDARDS AND MANAGEMENT Standards for creating an enterprise-wide network policy. Topics include: security management principles; defining security requirements; planning and documenting security policies; asset identification and control; system access control; and, internet security. |
| | | Paquetes de seguridad lógica. Análisis comparativo. Su implantación. | | | DISASTER RECOVERY AND PLANNING Disaster recovery planning including, techniques to prevent, detect, and recover from loss of information. |
| | | Implantación de la seguridad en las redes y en los entornos departamentales. Paquetes para la seguridad. Herramientas. La seguridad en los entornos. Intranets, extranets. Firewalls y otros. Elementos de seguridad | | | RISK MANAGEMENT AND ANALYSIS Principles and techniques applied to security risk analysis. How to conduct vulnerability assessment, the use of risk assessment tools and how to establish a cost benefit analysis for specific safeguards. New trends in risk management of networks and their environments. |
| | | Comercio electrónico y negocio electrónico. La seguridad en las aplicaciones y ERP's y PKI's | | | INFORMATION TECHNOLOGY SECURITY LAWS AND ETHICS An overview of International and Canadian laws, legislation, and legal issues relevant to the information systems security profession. |



TESIS CON
FALLA DE ORIGEN

| Temas de esta Tesis | Temario de Temas Especiales de Computación, F.I. UNAM Ciudad Universitaria | Universidad Politécnica de Madrid Posgrado en Seguridad Informática | Universidad de Granada Materia Optativa: Seguridad y protección de sistemas informáticos | Princenton University Course Schedule | Concordia University College of Alberta (Canadá) |
|---|---|---|---|---|---|
| | | La firma electrónica y la certificación por terceras partes. Principales paquetes y aplicaciones. | | | |
| | | La seguridad en la comunicación móvil | | | |
| | | Seguridad en las nuevas aplicaciones: Workflow, Trabajo en grupo, Call centres | | | |
| | | Antivirus. Principales paquetes | | | |

Tabla. 5.1 Comparación de temarios

La UNAM siempre se ha caracterizado y diferenciado de otras universidades por su carácter universal y plural, por lo que sus egresados pueden especializarse en cualquier ámbito de la carrera que hayan elegido; es decir, los planes de estudio están orientados para desarrollar en el alumno las habilidades suficientes que le permitan comprender los conceptos básicos que sustentan el origen de su carrera, analizar dichos conceptos para aplicarlos a la realidad del alumno y evolucionar sobre estos conceptos, para dar así, paso a nuevas ideas.

Si bien es cierto que la UNAM, a través del CEM Polanco y la Facultad de Ingeniería, ha dado los primeros pasos para desarrollar una cultura de seguridad en nuestros profesionistas mediante diplomados y materias optativas, consideramos conveniente que tales conocimientos se incorporen al plan de estudios de la carrera de Ingeniería en Computación, con carácter de obligatorios, dada la creciente necesidad de contar con expertos en materia de seguridad en informática y de implantar controles de seguridad a nivel internacional.

Se propone que los temas relativos a seguridad informática, se incorporen al plan de estudio de la carrera de Ingeniería en Computación, conforme a lo siguiente:

- La moral y ética de los jóvenes se encuentra suficientemente formada como para encaminar adecuadamente los conocimientos adquiridos.
- El alumno adquiere conocimientos en materia de telecomunicaciones y computación, por lo que los temas de seguridad en informática pueden ser analizados ampliamente.
- El alumno podrá conocer las herramientas existentes en materia de seguridad y enriquecer sus conocimientos con las experiencias de compañeros.
- El egresado de la Facultad de Ingeniería cubrirá las expectativas de los mercados nacionales e internacionales para el establecimiento de sistemas de comunicación global, seguros, etcétera.



TESIS CON
FALLA DE ORIGEN

- Los alumnos egresados tendrán la oportunidad de convertirse a especialistas en seguridad informática, teniendo un amplio campo de acción, pues en México y otros países, la existencia de recursos humanos especializados en seguridad informática es extremadamente escasa.

En las materias de Programación Estructurada y Características de lenguaje, Sistemas Operativos, Bases de Datos, así como, de Organización y Administración de Centros de Cómputo, deben incorporarse temas específicos de seguridad para completar el ciclo de conocimiento y aprendizaje sobre esta materia.

Los conceptos relacionados con la seguridad en redes pueden incorporarse en el plan de estudios de la carrera de Ingeniería en Computación, siguiendo una de las siguientes formas:

1. Incorporar el tema "Seguridad en Redes", en la materia de Redes de Computadoras.
2. Incorporar la asignatura de "Seguridad en Internet, herramientas y soluciones", con carácter optativo.
3. Incorporar la asignatura de "Seguridad en Internet, herramientas y soluciones", con carácter obligatorio.

## 1. Incorporar el tema "Seguridad en Redes", en la materia de Redes de Computadoras

**Ventajas**

- El alumno está condicionado a revisar los temas de seguridad en redes.
- Los conocimientos básicos requeridos para tratar el tema de seguridad son revisados durante el mismo semestre, por lo que se presupone un dominio de ellos.

**Desventajas**

- El temario de redes será extenso, más de lo que actualmente es, reduciendo el tiempo dedicado a tratar cada tema, los alcances y el contenido.
- De acuerdo a la libertad de cátedra, el profesor puede omitir o reemplazar un tema de acuerdo a su criterio, dado que el objetivo de la materia no es el análisis de la seguridad en redes, estos temas podrían ser omitidos por el profesor.

**Programa de la Asignatura: REDES DE COMPUTADORAS**

Número de créditos: 8

Carrera: ING. EN COMPUTACIÓN

Semestre: 10

Duración del curso:

Semanas: 16
Horas: 64

Horas a la semana:

Teoría: 4
Prácticas: 0

Obligatoria: SI

**Objetivo del curso.**

El alumno describirá y aplicará los conocimientos sobre redes de computadoras que les permitan tener una visión general del problema a resolver y en particular los aspectos de diseño tanto de software como de hardware.

**Temas**

| Número | Nombre | Horas |
|---|---|---|
| I. | CONCEPTOS BÁSICOS. | 7 |
| II. | COMPONENTES DE LA RED. | 12 |
| III. | PROCEDIMIENTOS PARA CONTROL DE ENLACE Y TRANSFERENCIA. | 10 |
| IV. | ASIGNACIÓN DE CAPACIDADES EN LOS ENLACES. | 9 |
| V. | NODOS O CONMUTADORES DE PAQUETES. | 9 |
| VI. | REDES Y PROCEDIMIENTOS. | 5 |
| VII. | SEGURIDAD EN REDES | 12 |
| | TOTAL | 64 |

**Antecedentes, objetivos y contenidos de los temas.**

I. CONCEPTOS BÁSICOS

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:

El alumno explicará las funciones de una red de computadoras, sus estructuras principales y las posibles formas de enviar información.

CONTENIDO:

I.1 Funciones de las redes de computadoras.
I.2 Tipos de enlaces básicos: punto a punto, multipunto.
I.3 Topologías principales.
I.4 Conmutación de circuitos, mensajes y paquetes.
I.5 Redes centralizadas y redes distribuidas. Redes LAN y WAN.

## II. COMPONENTES DE LAS REDES

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:

El alumno analizará funcionalmente los diferentes elementos que constituyen las redes de computadoras, dividiéndolas para su estudio en software y hardware.

CONTENIDO:

II.1 Elementos de hardware; medios físicos de transmisión, interfaces (EIA-RS-232-D, EIA-RS-449, V.24, V.35 y X.21); modems, multiplexores, concentradores, ensamblador desensamblador de paquetes (PAD), procesadores de comunicaciones (front end processor), nodos.
II.2 Elementos de software; características y funciones del sistema operativo (programas para el manejo de comunicaciones, programas para configuración de puertos, programas para la administración de la red).
II.3 Modelos principales de arquitectura de redes: Modelo ISO-OSI, SNA, identificación y funciones de las capas.

## III. PROCEDIMIENTOS PARA CONTROL DE ENLACE Y TRANSFERENCIA DE DATOS

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:

El alumno explicará soluciones a los problemas de secuenciamiento y sincronización en la transmisión de datos, y la integridad de la información transmitida.

CONTENIDO:

III.1 Protocolos: orientados a bit, orientados a carácter; detección y corrección de errores. Códigos convolucionales y no convolucionales. Necesidad de los protocolos. TCP/IP. Clasificación en base a funciones.



FALLA DE ORIGEN

III.2 Comunicación síncrona binaria (BISYNC): Control de la transferencia de datos. Chequeo y recuperación de errores. Codificación de la información. Transparencia de la información. Utilización de la línea. Sincronización Transparencia respecto al medio de comunicación. Procedimiento de inicialización.
III.3 Control de enlace de datos síncrono (SDLC): Control de la transferencia de datos. Chequeo y recuperación de errores. Codificación de la información. Transparencia de la información. Utilización de línea. Sincronización. Transparencia respecto al medio de comunicación. Procedimiento de inicialización.
III.4 Control de enlace de datos de alto nivel (HDLC): Control de la transferencia de datos. Chequeo y recuperación de errores. Codificación de la información. Transparencia respecto al medio de comunicación. Procedimiento de inicialización. Diferencia entre SDLC y HLDC.
III.5 Norma X.25 y manejo de protocolo HDLC.

## IV. ASIGNACIÓN DE CAPACIDADES EN LOS ENLACES

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:

El alumno explicará la asignación de capacidad en los enlaces de una red y las posibles formas de resolverlos para que puedan enfrentarse a casos prácticos: convencionales y no convencionales.

CONTENIDO:

IV.1 Asignación por raíz cuadrada: costo proporcional lineal a la capacidad. Minimización del tiempo de retraso promedio de los mensajes.
IV.2 Asignación por igualdad: minimización del mayor tiempo de retraso esperado en la red.
IV.3 Asignación proporcional. Asignación de capacidades proporcional al flujo en el enlace.
IV.4 Aplicaciones a casos reales: Redes distribuidas. Redes centralizadas.

## V. NODOS O CONMUTADORES DE PAQUETES

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:
El alumno explicará las técnicas que le permitan integrar conmutadores para manejar paquetes en una red.

CONTENIDO:

V.1 Análisis del tipo de información, de la cantidad y tipo de los enlaces y del tamaño del paquete, para determinar parámetros significativos tales como el tamaño del buffer, el número de retransmisiones, la dimensión de las ventanas, la capacidad del nodo (throughput), etcétera.
V.2 Ensamblador-desensamblador de paquetes para manejo de norma X.25.
V.3 Ensamblador-desensamblador de paquetes para manejo de protocolo SDLC.
V.4 Ensamblador-desensamblador de paquetes para manejo de terminales asíncronas (protocolo BSC).

## VI. REDES Y PROCEDIMIENTOS

ANTECEDENTES:

Comunicaciones Digitales

OBJETIVO:

El alumno explicará los tipos de redes y sus características principales.

CONTENIDO:

VI.1 Procedimientos de acceso al canal de datos: exploración (polling), transferencia de estafetas (token-ring) y contención de portadora (CSMA, carrier sense nultiple access).
VI.2 Redes de Area Local.

## VII. SEGURIDAD EN REDES

ANTECEDENTES:

Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:

El alumno analizará los principales riesgos que existen al compartir recursos dentro de una red pública y explicará las herramientas existentes para prevenir, detectar o corregir tales riesgos.

CONTENIDO:

VII.1 Riesgos y amenazas en una red informática: definición de riesgo, amenaza y control, vulnerabilidades de un sistema informático en ambiente distribuido.
VII.2 Riesgos y amenazas en una conexión a red pública: vulnerabilidades de Internet.
VII.3 Firewalls: definición, tipos y construcción.
VII.5 Criptografía: Definición, técnicas criptográficas.
VII.4 Mecanismos de protección: Mecanismos generales de protección a la información, mecanismos particulares de protección a la información.

TESIS CON
FALLA DE ORIGEN

## 2. Incorporar la asignatura de "Seguridad en Internet, herramientas y soluciones", con carácter optativo.

**Ventajas**

- El alumno debe conocer sobre los temas de seguridad en redes para aprobar la asignatura.
- El profesor cuenta con libertad de cátedra, pero está obligado a cubrir los temas previstos en el temario.
- Se promueve entre los estudiantes de la Facultad de Ingeniería, incorporados a la carrera de Ingeniería en Computación, una cultura de seguridad a través del estudio detallado de los temas que establecen los principios de la seguridad en redes.

**Desventajas**

- Únicamente los alumnos interesados cursarán esta materia.
- Aún cuando gran cantidad de alumnos se interesen en la materia, el número de alumnos estará restringido por la capacidad de los grupos asignados para el ciclo escolar.

**Programa de la Asignatura: SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES**

Número de créditos: 8

Carrera: ING. EN COMPUTACIÓN

Semestre: 10

Duración del curso:

Semanas: 16
Horas: 64

Horas a la semana::

Teoría: 4
Prácticas: 0

Obligatoria: NO

**Objetivo del curso.**

El alumno conocerá y aplicará los mecanismos y herramientas utilizadas para salvaguardar la información de un ambiente distribuido y público, específicamente Internet.

**Temas**

| Número | Nombre | Horas |
|---|---|---|
| I. | CONCEPTOS BÁSICOS | 9 |
| II. | INTERNET | 9 |
| III. | REDES Y SISTEMAS OPERATIVOS SEGUROS | 20 |
| IV. | CRIPTOGRAFIA | 6 |
| V. | SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES. | 20 |
| | TOTAL | 64 |

**Antecedentes, objetivos y contenidos de los temas.**

I. CONCEPTOS BÁSICOS

ANTECEDENTES:

Redes de Computadoras

OBJETIVO:

El alumno explicará las funciones de una red de computadoras, sus estructuras principales y las posibles formas de enviar información.

CONTENIDO:

I.1 Definición y objetivo de una red de computadoras.
I.2 Componentes de una red de computadoras.
I.3 Clasificación de las redes de computadoras: por su topología, extensión, conexión y tipo.
I.4 Modelo OSI.
I.5 Modelo TCP/IP.
I.6 Modelo Internet.
I.7 Técnicas de conmutación.

II. INTERNET

ANTECEDENTES:

Redes de Computadoras

OBJETIVO:

Que el alumno conozca y entienda las vulnerabilidades de los servicios ofrecidos por Internet.

CONTENIDO:

II.1 Historia.
II.2 Definición.
II.3 Servicios ofrecidos por Internet.
II.4 Tendencias de Internet y sus servicios.

II.5 Vulnerabilidades.

III. REDES Y SISTEMAS OPERATIVOS SEGUROS

ANTECEDENTES:

Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:

Que el alumno establezca las estrategias y planes de seguridad que detecten, eviten o en su defecto corrijan los riesgos en un centro de cómputo.

CONTENIDO:

III.1 Amenazas a la seguridad.
III.2 Seguridad externa.
III.3 Seguridad interna.
III.4 Planes de seguridad.
III.5 Evaluación de sistemas seguros.

IV. CRIPTOGRAFIA

ANTECEDENTES:

Programación Estructurada y Características de Lenguaje
Estructuras de Datos

OBJETIVO:

Conocer y aplicar las técnicas criptográficas existentes.

CONTENIDO:

IV.1 Definición de criptografía.
IV.2 Técnicas criptográficas.
IV.3 Herramientas existentes.

V. CONCEPTOS BÁSICOS

ANTECEDENTES:

Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:

Conocer las herramientas existentes para establecer mecanismos de seguridad en una conexión a Internet..

CONTENIDO:

V.1 Políticas de seguridad entre una red privada e Internet.
V.2 Servicios de protección de datos y su transferencia.
V.3 Mecanismos para proveer servicios de protección.
V.4 Cultura de Seguridad.

## 3. Incorporar la asignatura "Seguridad en Internet, herramientas y soluciones", con carácter obligatorio.

**Ventajas**

- El alumno debe conocer sobre los temas de seguridad en redes para aprobar la asignatura.
- El profesor cuenta con libertad de cátedra, pero está obligado a cubrir los temas previstos en el temario.
- Se promueve entre los estudiantes de la Facultad de Ingeniería, incorporados a la carrera de Ingeniería en Computación, una cultura de seguridad a través del estudio detallado de los temas que establecen los principios de la seguridad en redes y del conocimiento de hábitos y conductas mínimos indispensables al participar en un modelo de seguridad.
- Los alumnos de la carrera de Ingeniera en Computación contarían con conocimientos suficientes para iniciar y fomentar una cultura de seguridad, en materia de informática, en las áreas de trabajo a las que se incorporen una vez que finalicen sus estudios.
- La Universidad Nacional Autónoma de México (UNAM), a través de su Facultad de Ingeniería, estará en condiciones de preparar profesionales en las áreas de cómputo, telecomunicaciones y sistemas especializados en el área de seguridad en informática, manteniendo la vanguardia en educación de nivel superior.
- El campo de trabajo para los egresados de la carrera en Ingeniería en Computación se incrementaría, como se ha mencionado, existe una demanda de profesionales expertos en seguridad y va en aumento.

**Desventajas**

- Ninguna

**Programa de la Asignatura: SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES**

Número de créditos: 8

Carrera: ING. EN COMPUTACIÓN

Semestre: 10
Duración del curso:

Semanas: 16
Horas: 64

Horas a la semana::

Teoría: 4
Prácticas: 0

Obligatoria: SI

**Objetivo del curso.**

El alumno conocerá y aplicará los mecanismos y herramientas utilizadas para salvaguardar la información de un ambiente distribuido y público, específicamente Internet.

**Temas**

| Número | Nombre | Horas |
|---|---|---|
| I. | CONCEPTOS BÁSICOS | 9 |
| II. | INTERNET | 9 |
| III. | REDES Y SISTEMAS OPERATIVOS SEGUROS | 20 |
| IV. | CRIPTOGRAFIA | 6 |
| V. | SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES. | 20 |
| | TOTAL | 64 |

**Antecedentes, objetivos y contenidos de los temas.**

I. CONCEPTOS BÁSICOS

ANTECEDENTES:

Redes de Computadoras

OBJETIVO:

El alumno explicará las funciones de una red de computadoras, sus estructuras principales y las posibles formas de enviar información.

CONTENIDO:

I.1 Definición y objetivo de una red de computadoras.
I.2 Componentes de una red de computadoras.
I.3 Clasificación de las redes de computadoras: por su topología, extensión, conexión y tipo.
I.4 Modelo OSI.
I.5 Modelo TCP/IP.
I.6 Modelo Internet.
I.7 Técnicas de conmutación.

II. INTERNET

ANTECEDENTES:

Redes de Computadoras

OBJETIVO:

Que el alumno conozca y entienda las vulnerabilidades de los servicios ofrecidos por Internet.

CONTENIDO:

II.1 Historia.
II.2 Definición.
II.3 Servicios ofrecidos por Internet.
II.4 Tendencias de Internet y sus servicios.
II.5 Vulnerabilidades.

III. REDES Y SISTEMAS OPERATIVOS SEGUROS

ANTECEDENTES:

Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:

Que el alumno establezca las estrategias y planes de seguridad que detecten, eviten o en su defecto corrijan los riesgos en un centro de cómputo.

CONTENIDO:

III.1 Amenazas a la seguridad.
III.2 Seguridad externa.
III.3 Seguridad interna.
III.4 Planes de seguridad.
III.5 Evaluación de sistemas seguros.

IV. CRIPTOGRAFIA

ANTECEDENTES:

Programación Estructurada y Características de Lenguaje
Estructuras de Datos

OBJETIVO:

Conocer y aplicar las técnicas criptográficas existentes.

CONTENIDO:

IV.1 Definición de criptografía.
IV.2 Técnicas criptográficas.
IV.3 Herramientas existentes.

V. CONCEPTOS BÁSICOS

ANTECEDENTES:

Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:

Conocer las herramientas existentes para establecer mecanismos de seguridad en una conexión a Internet.

CONTENIDO:

V.1 Políticas de seguridad entre una red privada e Internet.
V.2 Servicios de protección de datos y su transferencia.
V.3 Mecanismos para proveer servicios de protección.
V.4 Cultura de Seguridad.

**Estructura jerárquica de conocimientos para la asignatura de Seguridad en Internet.**

Como parte de las actividades de análisis previas a la elaboración de este trabajo de tesis y como complemento a la propuesta del temario para la asignatura de Seguridad en Internet, fue necesario identificar la estructura de temas a investigar así como determinar el orden y la profundidad con que cada uno de ellos debe ser tratado. El objetivo específico es, como primera etapa, permitir adquirir los conocimientos suficientes para atender un problema de seguridad y sentar las bases para especializarse a futuro, si así se desea.

A continuación, se presenta la estructura conceptual de conocimientos que determinamos para la materia de Seguridad en Internet, Herramientas y Soluciones, así como el detalle específico de tiempos dedicados a cada tema.

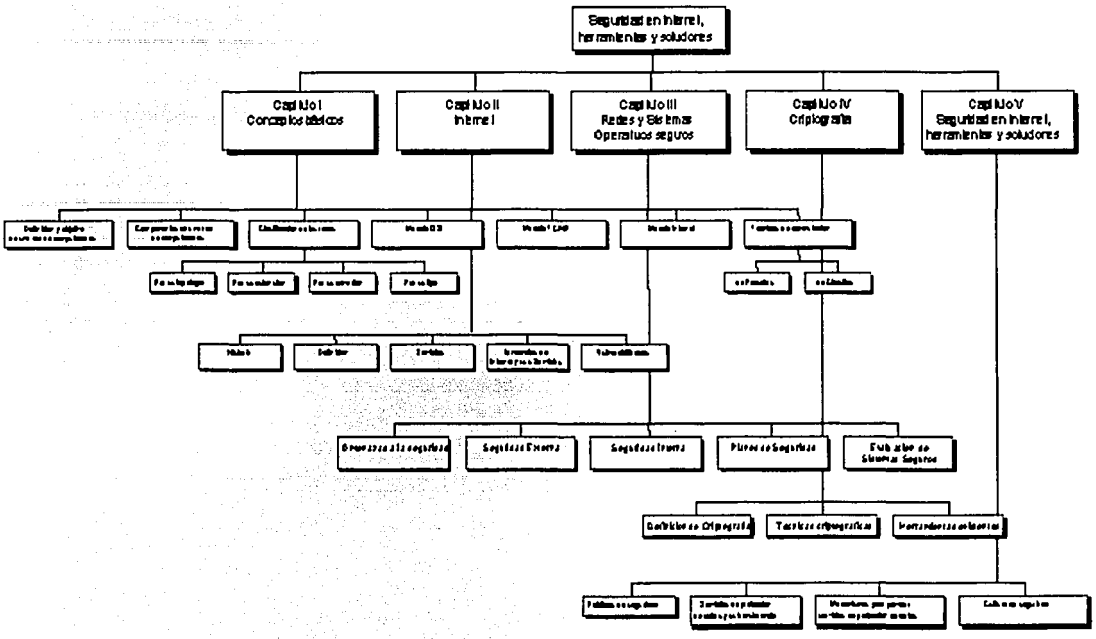


Fig. 5.1 Árbol conceptual de la asignatura

| Capítulo I. Conceptos Básicos | |
|---|---|
| Tema | Horas propuestas |
| Definición y objetivo de una red de computadoras | .5 |
| Componentes de una red de computadoras | 1 |
| Clasificación de las redes de computadoras: por su topología, extensión, conexión y tipo | .5 |
| Modelo OSI | 1.5 |
| Modelo TCP/IP | 1.5 |
| Modelo Internet | 2 |
| Técnicas de conmutación | 2 |
| Número total de horas: | 9 |

| Capítulo II. Internet | |
|---|---|
| Tema | Horas propuestas |
| Historia | 1 |
| Definición | 1 |
| Servicios ofrecidos por Internet | 3 |
| Tendencias de Internet y sus servicios | 1 |
| Vulnerabilidades | 3 |
| Número total de horas: | 9 |



TESIS CON
FALLA DE ORIGEN

| Capítulo III. Redes y Sistemas Operativos seguros | |
|---|---|
| Tema | Horas propuestas |
| Amenazas a la seguridad | 3 |
| Seguridad externa | 3 |
| Seguridad interna | 4 |
| Planes de seguridad | 6 |
| Evaluación de sistemas seguros | 4 |
| Número total de horas: | 20 |

| Capítulo IV. Criptografía | |
|---|---|
| Tema | Horas propuestas |
| Definición de criptografía | 1 |
| Técnicas criptográficas | 3 |
| Herramientas existentes | 2 |
| Número total de horas: | 6 |

| Capítulo V. Seguridad en Internet, herramientas y soluciones. | |
|---|---|
| Tema | Horas propuestas |
| Políticas de seguridad entre una red privada e Internet | 4 |
| Servicios de protección de datos y su transferencia | 6 |
| Mecanismos para proveer servicios de protección | 8 |
| Cultura de Seguridad | 2 |
| Número total de horas: | 20 |
| Total de horas: | 64 |

5.2 Tabla de análisis de tiempos para la asignatura Seguridad en Internet, herramientas y soluciones.

Como parte de los resultados que obtuvimos en el desarrollo de esta tesis, estamos convencidos de que la incorporación de la materia de Seguridad en Internet, en la carrera de Ingeniería en Computación, es sólo uno de tantos pasos que pueden y deben darse con la intención de crear y promover una cultura de seguridad en informática dentro de la Facultad de Ingeniería.

Como segunda fase, en continuación a este trabajo, es factible implantar una página de Internet dedicada a la seguridad en informática, creada y alimentada por estudiantes de la Facultad de Ingeniería, dedicados a la investigación y desarrollo, observando los siguientes principios:

**Servicios**

Capacitación virtual sobre seguridad informática.

Base de conocimientos sobre riesgos y esquemas de control.

Centro de información sobre herramientas existentes en materia de seguridad.

Taller sobre implantación de soluciones.

Mesa de ayuda.

Foros de discusión.

Vínculos con otras universidades u organismos dedicados a la seguridad.

**Productos**

Diseño de arquitecturas de hardware o software dedicados a la seguridad mediante convocatorias a concurso.

Trabajos de investigación mediante cooperación con otras entidades.

Desarrollo de infraestructura de seguridad para empresas mediante patrocinio.

Elaboración de publicaciones electrónicas sobre seguridad.

Arquitectura de firma electrónica y conexiones seguras.

La selección de construir una página Web dedicada a la seguridad, como segunda fase, no es fortuita, por el contrario, la interacción con la red y el aprovechamiento de sus recursos es el clima propicio para constituir un foro público de conocimiento y difusión de cultura sobre seguridad.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

Programa de Asignatura

INGENIERÍA MECANICA ELÉCTRICA — División

COMPUTACIÓN — Departamento

Fecha de aprobación del

| | | | | | |
|---|---|---|---|---|---|
| Programa de la Asignatura: | SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES | | | | |
| Clave: | | Número de Créditos: | 06 | Carrera: | Ingeniería en Computación |
| Duración del Curso: | Semanas: | 16 | | | |
| | Horas: | 64.0 | Semestre: | | 10° |
| Horas a la semana: | Teoría: | 4.0 | Obligatoria: | | X |
| | Prácticas: | 0.0 | Optativa: | | |

OBJETIVO DEL CURSO

El alumno conocerá y aplicará los mecanismos y herramientas utilizadas para salvaguardar la información de un ambiente distribuido y público, específicamente Internet.

TEMAS

| Núm. | Nombre | Horas |
|---|---|---|
| I. | CONCEPTOS BÁSICOS | 9.0 |
| II. | INTERNET | 9.0 |
| III. | REDES Y SISTEMAS OPERATIVOS SEGUROS | 20.0 |
| IV. | CRIPTOGRAFIA | 6.0 |
| V. | SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES | 20.0 |
| | | 64.0 |

TESIS CON
FALLA DE ORIGEN

ASIGNATURA: SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES

ANTECEDENTES, OBJETIVOS Y CONTENIDOS DE LOS TEMAS

I. CONCEPTOS BÁSICOS.

ANTECEDENTES: Redes de Computadoras

OBJETIVO:
El alumno explicará las funciones de una red de computadoras, sus estructuras principales y las posibles formas de enviar información.

CONTENIDO:
- I.1 Definición y objetivo de una red de computadoras.
- I.2 Componentes de una red de computadoras.
- I.3 Clasificación de las redes de computadoras: por su topología, extensión, conexión y tipo.
- I.4 Modelo OSI.
- I.5 Modelo TCP/IP.
- I.6 Modelo Internet.
- I.7 Técnicas de conmutación.

II. INTERNET.

ANTECEDENTES: Redes de Computadoras

OBJETIVO:
Que el alumno conozca y entienda las vulnerabilidades de los servicios ofrecidos por Internet.

CONTENIDO:
- II.1 Historia.
- II.2 Definición.
- II.3 Servicios ofrecidos por Internet
- II.4 Tendencias de Internet y sus servicios.
- II.5 Vulnerabilidades

III REDES Y SISTEMAS OPERATIVOS SEGUROS.

ANTECEDENTES: Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:
Que el alumno establezca las estrategias y planes de seguridad que detecten, eviten o en su defecto corrijan los riesgos en un centro de cómputo.

CONTENIDO:
- III.1 Amenazas a la seguridad.
- III.2 Seguridad externa.
- III.3 Seguridad interna.
- III.4 Planes de seguridad.
- III.5 Evaluación de sistemas seguros.

IV. CRIPTOGRAFIA.

ANTECEDENTES: Programación Estructurada y Características de Lenguaje
Estructuras de Datos

OBJETIVO:
Conocer y aplicar las técnicas criptográficas existentes.

CONTENIDO:
- IV.1 Definición de criptografía.
- IV.2 Técnicas criptográficas.
- IV.3 Herramientas existentes.

ASIGNATURA: SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES

**TECNICAS DE ENSEÑANZA:**

| | |
|---|---|
| Exposición oral | (X) |
| Exposición audiovisual | (X) |
| Ejercicios dentro de clase | ( ) |
| Ejercicios fuera del aula | ( ) |
| Seminarios | ( ) |
| Lecturas obligatorias | (X) |
| Trabajos de investigación | (X) |
| Prácticas de taller o laboratorio | ( ) |
| Prácticas de campo | ( ) |
| Otras: | |

**ELEMENTOS DE EVALUACIÓN:**

| | |
|---|---|
| Exámenes parciales | (X) |
| Exámenes finales | (X) |
| Trabajos y tareas fuera del aula | (X) |
| Participación en clase | ( ) |
| Asistencia a prácticas | ( ) |
| Otros: | |

**ANTECEDENTES**

| Asignatura | Clave |
|---|---|
| ESTRUCTURAS DE DATOS | 0190 |
| ORGANIZACIÓN Y ADMINISTRACIÓN DE CENTROS DE CÓMPUTO | 0613 |
| PROGRAMACIÓN ESTRUCTURADA Y CARACTERÍSTICAS DE LENGUAJE | 0075 |
| REDES DE COMPUTADORAS | 0780 |
| SISTEMAS OPERATIVOS | 0640 |

**CONSECUENTES**

| Asignatura | Clave |
|---|---|
| Ninguna | |

ASIGNATURA: SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES

**ANTECEDENTES, OBJETIVOS Y CONTENIDOS DE LOS TEMAS**

V. SEGURIDAD EN INTERNET, HERRAMIENTAS Y SOLUCIONES.

ANTECEDENTES: Redes de Computadoras
Sistemas Operativos
Organización y Administración de Centros de Cómputo

OBJETIVO:
Conocer las herramientas existentes para establecer mecanismos de seguridad en una conexión a Internet.

CONTENIDO:
V.1 Políticas de seguridad entre una red privada e Internet.
V.2 Servicios de protección de datos y su transferencia.
V.3 Mecanismos para proveer servicios de protección.
V.4 Cultura de Seguridad.

TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN

# CONCLUSIONES

Cuando una organización requiere compartir datos, sistemas o recursos físicos, es tiempo de implantar una red de computadoras; para hacerlo se deberán cubrir dos aspectos básicos:

- Adquisición de los componentes
- Creación de las políticas de seguridad

**Adquisición de los componentes**

Para adquirir los componentes físicos, tal como servidores, equipos personales, impresoras y ruteadores, entre otros, se determinaran los siguientes aspectos:

- Número de usuarios actuales.
- Número máximo de usuarios que podrán conectarse a la red.
- Necesidad de conexión externa.
- Necesidad de la utilización de los servicios de Internet.
- Aplicaciones con las que se desea convivir.
- Presupuesto.

Una vez establecida esta información, se definirá el tipo de red, conexión, sistema operativo de red, sistema operativo de los clientes y número de servidores.

**Creación de las políticas de seguridad**

Una vez que existe el proyecto de red o que se realizó la implementación de ésta, es necesario que de acuerdo a las políticas y necesidades de la organización se determine un esquema de seguridad informática, basándose en los sistemas operativos seleccionados. Cabe señalar que las políticas de seguridad deben evolucionar constantemente conforme cambien los sistemas o las políticas internas.

A continuación se muestran los pasos a seguir:

| |
|---|
| Análisis de Riesgos |
| Diseño de las políticas para prevenir, detectar y corregir los riesgos detectados |
| Implementación de las políticas de seguridad |

## Análisis de riesgos

Se define del valor de la información y su sensibilidad, para posibilitar la identificación de los riesgos y amenazas del sistema. Esta identificación debe abarcar las siguientes áreas:

- Seguridad informática física
- Seguridad de la red
- Seguridad de los datos

Los riesgos deben analizarse sobre cada uno de los siguientes componentes de la red:

| Grupo | Componente de red |
|---|---|
| Activos Cuantificables | Personas<br>Edificios<br>Muebles<br>Aire Acondicionado<br>Calefacción<br>Electricidad<br>Sistemas de control de incendios |
| Hardware | Computadoras<br>Equipo periférico<br>Equipo de comunicación<br>Ruteadores<br>Puentes de enlace<br>Concentradores<br>Cableado |
| Software | Sistemas operativos de clientes y servidores<br>Aplicaciones<br>Protocolos de comunicación |
| Datos | Información contenida en discos duros, diskettes, CD-ROMs y cintas |
| Conexiones de red | Ethernet<br>TCP/IP<br>NFS(*Network File System*, Sistema de Archivos de Red) |

Las amenazas más comunes son:

| Elemento de red | Amenaza |
|---|---|
| Sistemas operativos de red | Acceso no autorizado<br>Modificación, consulta o eliminación no autorizada<br>Negación de un servicio |
| Modems | Robo de información<br>Acceso de personas no autorizadas<br>Introducción de software peligroso<br>Modificación, consulta y eliminación de información |
| Estaciones de trabajo | Revelación de contraseñas<br>Acceso f'isico sin autorización<br>Modificación, consulta o eliminación no autorizada |
| Enrutadores, puentes de enlace y concentradores | Modificación de la configuración resultando en la negación de servicio y/o acceso a recursos |

Establecidos los riesgos involucrados en el sistema, se establece su peligrosidad y se determina para cuales debe implementarse un esquema de seguridad y de que nivel.

## Diseño de las políticas

Establecer las herramientas y mecanismos necesarios para contrarrestar los riesgos determinados en el análisis.

| Elemento de red | Amenaza | Contramedida |
|---|---|---|
| Sistemas operativos de red | Acceso no autorizado<br>Modificación, consulta o eliminación no autorizada<br>Negación de un servicio | Instalación de un sistema operativo de red seguro<br>Gestión de contraseñas<br>Servicios de Identificación<br>Servicios de Autenticación<br>Asignación de recursos |
| Modems | Robo de información<br>Acceso de personas no autorizadas<br>Introducción de software peligroso<br>Modificación, consulta o eliminación de información | Prohibición conexión por modem centralizado y call-back<br>Firewalls<br>Servicios de Identificación<br>Servicios de Autenticación<br>Encriptación de datos |

| Elemento de red | Amenaza | Contramedida |
|---|---|---|
| Estaciones de trabajo | Revelación de contraseñas<br>Acceso f'isico sin autorización<br>Modificación, consulta o eliminación no autorizada | Limitar el acceso a las instalaciones<br>Seguridad externa<br>Alarmas en los cables para detectar intrusos<br>Uso de fibra óptica<br>Encriptación de datos<br>Gestión de contraseñas |
| Servicios de archivos de red | Robo o destrucción<br>Acceso no autorizado<br>Modificación, consulta o eliminación no autorizada | Control de acceso físico<br>Servicios de Identificación<br>Servicios de Autenticación<br>Asignación de recursos |
| Enrutadores, puentes de enlace y concentradores | Modificación de la configuración resultando en la negación de servicio y/o acceso a recursos | Gestión de claves<br>Acceso restringido a dispositivos |

## Implementación de las políticas de seguridad

Instituir los mecanismos y herramientas de seguridad interna, externa y en Internet conforme a los requerimientos.

Especificar los planes y pruebas de contingencia para la recuperación de desastres.

Diseminar entre todo el personal de la empresa conocimiento y formación en seguridad informática, creando así una cultura en seguridad.

Administrar y coordinar la seguridad en informática.

### Propuesta del Tema de Seguridad en Redes

Cuando iniciamos el proceso de selección del tema para trabajo de tesis, buscamos entre diferentes opciones sin encontrar complacencia. Sin embargo, el mismo proceso de búsqueda a través de medios electrónicos de comunicación e información, nos llevo a detenernos al recapacitar y tomar conciencia de que, al paso del tiempo, el uso de Internet es más cotidiano e inconsciente provocando una dependencia a sus servicios y haciendo casi imperceptible el hecho de que, a la par de esa cotidianeidad, caminan riesgos que envuelven o vulneran nuestra seguridad.

En esa pausa, concebimos la idea que cristalizamos como tema de tesis y finaliza con esta conclusión sobre nuestra propuesta, para la cual, requerimos retomar nuestros cuestionamientos iniciales:

**¿Seguridad en Internet?**
**¿Riesgos?**
**¿Herramientas de protección?**
**¿Soluciones de seguridad?**

De lo anterior, podemos desprender que, en forma general, sabemos muy poco acerca del futuro de las telecomunicaciones y de los servicios a los que vamos a tener acceso a través de las redes públicas y privadas, pero es claro que los riesgos han evolucionado y seguirán incrementándose estableciendo el reto por garantizar la seguridad de la información y de las comunicaciones pero más allá, está gestándose una nueva sociedad que se interrelaciona electrónicamente, crece desmedidamente, sin principios claros de respeto, impersonal en muchos de sus casos. Sólo la educación y cultura en estos temas, permitirán el sano desarrollo de esa sociedad electrónica.

Después de lo revisado e investigado consideramos prudente que la Facultad de Ingeniería perteneciente a la Universidad Nacional Autónoma de México (UNAM), en complemento a las actividades que ésta última ya viene cubriendo en materia de seguridad informática, debe incorporar en el plan de estudios de la carrera de Ingeniería en Computación ese mismo tema, ya sea modificando el temario de la materia de Redes de Computadoras o incorporando una materia obligatoria denominada Seguridad en Internet, Herramientas y Soluciones esta última la mejor y más completa de nuestras propuestas.

Los beneficios ya han sido mencionados en el capítulo correspondiente, pero debemos resaltar que prepararnos en materia de seguridad informática es el primer paso para construir y fomentar una cultura que en ese mismo sentido será indispensable para convivir e interactuar en un futuro próximo.

Finalmente, el presente trabajo de tesis pretende ser una guía de consulta en lo relativo a seguridad en Internet, las herramientas disponibles y la implantación de soluciones a los requerimientos de seguridad, dirigida principalmente al estudiante de la Facultad de Ingeniería y a aquellos que como nosotros se interesen en este tema.

TESIS CON
FALLA DE ORIGEN

# ANEXO 1
# CRIPTOGRAFIA

A lo largo de la historia de la humanidad, se han conocido diferentes casos en los que se hizo necesario proteger la información o comunicación; es decir, proteger el contenido de mensajes enviados para que solo pudieran ser leídos por la persona o personas a las que iban dirigidos. Las técnicas empleadas han sido muy variadas dependiendo de cada cultura o sociedad que estudiemos.

En la actualidad, la importancia que la información tiene para las organizaciones y empresas así como la variedad de canales de comunicación electrónica, han fomentado el uso de técnicas de ocultamiento de información para la protección y seguridad de la misma. El riesgo en el almacenamiento de la información se encuentra estrechamente relacionado con el robo de datos o el acceso no autorizado, mientras que en la transmisión el principal riesgo reside en la intervención del canal de comunicación.

La palabra criptología proviene de la palabra griega *Kryto* y *logos* que significa estudio de lo oculto, donde una de sus ramas es la criptografía, la cual, se ocupa específicamente de las técnicas, métodos y procedimientos para la ocultación de mensajes.

La criptografía se define como el método que transforma un texto legible en otro ilegible, el cual sólo puede ser leído aplicando inversamente el mismo proceso de transformación. En este sentido, la protección de la información se logra variando la forma del texto.

La criptografía se basa en los siguientes pasos:

- El emisor genera un mensaje.
- El contenido del mensaje es tratado mediante un cifrador que, con la ayuda de una clave, crea un texto oculto.
- El texto cifrado llega al receptor a través de un medio de comunicación.
- El receptor utiliza un descifrador, el cual utiliza otra clave para obtener el texto original y el receptor obtiene el mensaje original.

Se llama cifrado a la transformación del texto original (llamado también texto inicial o texto claro), esta transformación lo convierte en texto cifrado o criptograma. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado. Cada una de estas transformaciones está determinada por un parámetro llamado clave. El conjunto de sus posibles valores se denomina espacio de claves K. La familia de transformaciones criptográficas se llama sistema de cifrado y matemáticamente se representa como T={Tk/k K}.

Para cada transformación criptográfica Tk se definen las imágenes de cada una de las palabras de n letras, es decir, el sistema criptográfico se puede describir como T = {Tk^n:1 <= n < i }, siendo Tk^n(x)=y, donde "y" es la palabra cifrada que corresponde a la palabra original "x".

Para evitar ambigüedades, se hacen las siguientes suposiciones:

- Tk^n es una función biyectiva.
- Se usa el mismo alfabeto para ambos textos, original y cifrado.
- Se define el cifrado con todas las posibles palabras, independientemente si existen o no.
- Cada n-palabra se cifra en una n-palabra, teniéndose así que el cifrado no cambia la longitud del texto original.

Adicionalmente, se recomienda que, en el caso de procesamiento digital, se hagan las siguientes suposiciones:

- Se trabaja únicamente con alfabeto binario.
- Debe existir el cifrado de todas las palabras posibles.
- Si el cifrado cambiara la longitud del texto, sería necesario usar un nuevo formato para el texto cifrado.

De acuerdo a Auguste Kerchoffs Von Nieuwenhof (1835-1903), uno de los teóricos de la criptografía más reconocidos, en sus tratados especifica que todo sistema criptográfico debe estar compuesto por dos tipos de información:

- Pública, familia de algoritmos que definen el sistema criptográfico.
- Privada, clave o frase de seguridad confidencial que se utiliza en cada cifrado.

Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales, todo dependerá del sistema utilizado, clasificándose de la siguiente forma:

- Sistemas de cifrado simétrico
- Sistemas de cifrado asimétrico
- Sistemas de cifrado híbridos

**Sistemas de cifrado simétrico**

Son aquellos que utilizan una misma clave para cifrar y descifrar un mensaje, a este algoritmo se le conoce también como *criptografía con clave secreta*.

El principal riesgo en este tipo de sistemas es que la fuente del texto sea redundante en el mensaje, para evitar este incidente se sugieren dos métodos básicos: la difusión y la confusión.

La difusión, consiste en anular la redundancia de la fuente en el mensaje cifrado mediante una de las dos formas siguientes:

- Transposición para evitar los criptoanálisis basados en las frecuencias de las n-palabras.
- Dependencia de cada letra del mensaje cifrado con un gran número de letras del texto original.

La confusión, consiste en hacer que la relación entre la clave y el mensaje cifrado sea lo más compleja posible, normalmente, esto se consigue con la técnica de la sustitución.

En conclusión, por sus características, la difusión y la confusión son dos técnicas poco recomendables para implantar un sistema de cifrado.

Los sistemas de cifrado simétrico pueden, a su vez, clasificarse de acuerdo al tipo de operación que realizan:

- Transposición
- Sustitución
- Producto

De igual forma, el cifrado simétrico puede dividirse en dos grandes grupos, según la fuente que genera el texto:

- Fuentes que generan n-palabras.
- Fuentes que generan letras.

**Transposición, sustitución y producto**

La transposición consiste en alterar el orden de los caracteres del texto original de acuerdo a una clave; la sustitución, se refiere a cambiar los caracteres originales por otros; y, el producto, es la aplicación iterativa de encriptación sobre textos.

**Fuentes que generan n-palabras**

Textos formados por n-palabras, donde el cifrado actúa convirtiendo cada n-palabra en una nueva n-palabra, el cual, también es conocido como cifrado por bloques.

El sistema de cifrado por bloques más conocido es el denominado DES (Data Encryption Standard), este sistema se puede catalogar como un cifrado en bloque que es a la vez un cifrado producto de transposiciones y sustituciones.

**Fuentes que generan letras**

Textos formados por letras, donde el cifrado es la combinación de letras con una secuencia cifrante (flujo de bits secretos), aplicando un operador. La secuencia cifrante se produce mediante un generador de bits.

Los sistemas de cifrados de flujo pueden dividirse en cifrados síncronos y asíncronos, según la dependencia entre la función de transición de estados y el espacio de los elementos de entrada.

**Sistemas de cifrado asimétrico**

Estos sistemas son conocidos también como sistemas de cifrado de clave pública y utilizan una combinación de dos claves diferentes, una pública y otra privada de carácter confidencial.

Utilizando la clave pública, es posible codificar información que sólo con la llave privada será posible decodificar. La clave pública puede ser conocida por cualquier usuario que la requiera mientras que, la clave privada, sólo debe ser conocida por el propietario de la información. Esta característica permite que una persona pueda cifrar información utilizando la clave pública de un destinatario en particular, confiando en que éste último será el único que podrá descifrar la información aplicando su clave privada.

Hoy en día, el criptosistema de clave pública más ampliamente utilizado, es el RSA y se basa en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos grandes primos.

### Sistemas de cifrado híbridos

Este tipo de sistemas de cifrado combina tanto los sistemas de clave simétrica como los de clave asimétrica.

Funcionan mediante el cifrado de clave pública y permiten compartir una clave de cifrado simétrico. En cada mensaje la clave simétrica utilizada es diferente, si un intruso pudiera descubrirla, solo sería valida para ese mensaje y no para los restantes. La clave simétrica es cifrada con la clave pública y el mensaje saliente es cifrado con la clave simétrica, acto seguido se utiliza la clave simétrica para descifrar el mensaje.

PGP y GnuPG son sistemas de cifrado híbridos.

### Algoritmos

En los sistemas de cifrado asimétrico se utilizan las siguientes funciones matemáticas para transformar la información:

- Algoritmo Hash: Transforma los datos en un resumen irreversible, es decir, una vez aplicado el algoritmo sobre los datos, es imposible obtenerlos nuevamente a partir del resumen obtenido y a su vez, este resumen sólo puede ser obtenido única y exclusivamente mediante los datos originales.

- Algoritmo de clave pública: función matemática fácil de resolver en un sentido pero difícil de realizar en sentido contrario, a menos que se conozca la clave privada. Las claves son biunívocas, donde a cada clave pública le corresponde una clave privada y viceversa, por lo cual el cifrado generado mediante el uso de una clave pública sólo puede ser descifrado mediante la clave privada correspondiente e inversamente el cifrado mediante clave privada sólo puede ser verificado mediante la clave pública correspondiente.

# ANEXO 2
# GESTIÓN DE CLAVES

La gestión de claves se refiere al conjunto de procedimientos existentes para la administración de claves de usuario. Para crear y mantener una clave de usuario, es necesario observar diferentes etapas:

- Generación
- Distribución
- Almacenamiento
- Tiempo de vida
- Destrucción
- Aplicación de acuerdo con una política de seguridad

La gestión de claves se realiza mediante protocolos.

## Generación de claves

Se deben considerar los siguientes aspectos en la creación de una clave:

- Longitud de la clave. Entre más caracteres se utilicen para una clave mayor será la seguridad de la misma, ya que la combinación de caracteres requeridos será mayor.
- Caracteres utilizables. Se debe permitir el uso de cualquier caracter.
- Elección de la clave. Se deben elegir palabras o combinaciones de estas que no pertenezcan a nuestra vida cotidiana, tal como nombre propio o de familiares y fechas de nacimiento, entre otras.
- Claves aleatorias. Son cadenas de bits aleatorios generados a través de un procedimiento automatizado.
- Frases de paso. Se utilizan frases convenientemente largas convertidas en una clave aleatoria por medio de un algoritmo.

TESIS CC
FALLA DE C ..N

## Distribución de claves

El problema central de todo sistema de gestión de claves es la entrega de claves, esta distribución debe efectuarse previamente a la comunicación.

Existen dos posibilidades para entregar la clave:

- Automática. Se lleva a cabo sobre la misma red de comunicación en donde se está transmitiendo y la transferencia suele iniciarse con la petición de la clave.
- Manual. Es Independiente del canal de comunicación.

La distribución segura de claves sobre un canal inseguro requiere de técnicas criptográficas.

## Almacenamiento de claves

El almacenamiento de claves puede realizarse en tarjetas de banda magnética, en una llave de plástico con un chip ROM o una tarjeta inteligente.

También pueden ser encriptadas y almacenadas en un archivo electrónico.

## Tiempo de vida

Una clave no debe utilizarse por tiempo indefinido.

Para protocolos orientados a conexión, se debe usar la misma clave de sesión durante la duración de la comunicación, siendo descartada al finalizar la comunicación y nunca reutilizada.

Para protocolos no orientados a conexión se debe usar una clave de sesión durante un cierto periodo o para un cierto número de transacciones.

## Destrucción de claves

Las claves que ya no se utilicen deben ser destruidas oportunamente. En función del dispositivo de almacenamiento empleado, deberá buscarse la forma de que se vuelvan irrecuperables.

# ANEXO 3
# NETIQUETTE

Los servicios de Internet y particularmente la utilización de correo electrónico, establecen nuevas condiciones para la comunicación, por lo que es necesario crear reglas de etiqueta que aseguren la personalidad tanto del remitente como del destinatario.

Netiquette es una guía de escritura que los usuarios pueden observar al hacer uso de los servicios de Internet, su objetivo es mantener una comunicación cordial entre usuarios.

Las relaciones interpersonales, aún las establecidas en forma escrita, deben regirse siempre por buenos modales, cortesía, respeto, consideración y tolerancia.

Las reglas de Netiquette son las siguientes:

**Concientizarse**

- La regla de oro de Internet es simple: No hacer a los demás los que no nos gustaría que nos hicieran a nosotros.
- Recordar que al otro lado de nuestra pantalla hay otra persona.
- Escribir como si las dos personas se estuvieran mirando a los ojos.
- No escribir nada que no diríamos frente a frente a la otra persona.
- Nunca mantener el correo abierto o en manos de personas extrañas.
- Mantener la clave de usuario secreta
- Revisar los mensajes de correo electrónico, al menos una vez al día.
- En la medida de lo posible, no enviar información confidencial por este medio.
- Evitar enfrentamientos.

**Tener cuidado al responder**

- Cuando se responde un mensaje se debe mantener especial cuidado en que el destinatario sea la persona a quien deseamos enviar el mensaje, pues la respuesta podría recibirse por personas a las que no deseamos informar; en la medida de lo posible, hay que evitar las listas de distribución.
- Enviar los mensajes personales en privado.

- Se considera de mal gusto reenviar correos personales a listas de distribución.
- Los mensajes deben ser claros y concisos, se recomienda no utilizar más de 80 caracteres al responder.
- El contenido y la ortografía deben mantenerse impecables.
- Cuando se utilicen siglas o abreviaciones, la primera vez que sean escritas, deberá definirse su significado.
- Mantener el "Asunto" del mensaje original, al responder o reenviar un mensaje.

**Forma de responder**

- Contestar los mensajes de correo electrónico a la brevedad.
- No enviar archivos adjuntos extensos, es posible que el destinatario no lo reciba si se produce un error al momento de la transmisión.
- Utilizar el encabezado nombrado "Asunto" como una oración sencilla que describa el tema que se tratará en el mensaje de correo electrónico.
- Incluir la firma digital al final de los mensajes de correo, no mayor a 4 líneas de texto y que incluya el nombre y la dirección de Internet.
- Para el caso de mensajes de correo electrónico con carácter personal, utilizar nemotécnicos, "caritas de expresión", que ayudan a transmitir sentimientos.
- Se debe ser cuidadoso al usar sarcasmo y humor.
- No contestar un mensaje cuando se esté enojado o de mal humor.
- No escribir con letras mayúsculas.

# BIBLIOGRAFÍA


[1] Charles P. Pfleeger
**Security in Computing**
Prentice Hall International, Inc. 1989

[2] Charles Royal P. Fisher
**Seguridad en los Sistemas Informáticos**
Paraninfo, 1988

[3] Mike Hendry
**Practical Computer Network Security**
Artech House, Inc. 1995

[4] D. Parker
**Computer Security Management**
Reston, 1981

[5] Ribagorda, A. Calvo y M.A. Gallardo
**Seguridad en UNIX, sistemas abiertos e Internet**
Paraninfo, 1996

[6] J.L. Morant, A. Ribagorda y J. Sancho
**Seguridad y Protección de la Información**
Ed. Centro de Estudios Ramón Areces, S.A., 1994

[7] DoD (US. Department of Defense)
**Trusted Computer System Evaluation Criteria**
DoD 5.200.28-STD. Diciembre 1985

[8] Antonio Villalón Huerta
**Seguridad en Unix y Redes V. 2.1**
Julio 2002

[9] Rolf Oppliger
**Sistemas de Autentificación para Seguridad en Redes**
Alfaomega Grupo Editor, 1998

[10] Jesús de Marcelo Rodao
**Piratas Cibernéticos**
Alfaomega Grupo Editor

[11] Harry Katzan, Jr
**The Standard Data Encryption Algorithm**
Petrocelli Books, Inc. 1977

[12] Harvey M. Deitel
**Introducción a los Sistemas Operativos**
Addison-Wesley Iberoamericana, 1987

[13] Sánchez Allende Jesús , López Lerida Joaquín
**Redes, Iniciación y Referencia**
Osborne McGraw Hill, 2000

[14] Joel Scambray, Stuart Mc Clure, George Kurtz
**Hackers 2, Secretos y Soluciones para la Seguridad en Redes**
Osborne McGraw Hill

[15] Craig Zacker
**Redes, Manual de Referencia**
McGraw Hill, Osborne Media

[16] José Luis Raya, Elena Raya
**Microsoft Windows 2000 Server**

[17] Tanenbaum, Andrew S.
**Computer Networks**
Prentice Hall, Second Edition

[18] L. Roberts and B. Wessler
**Computer Network Development to Achieve Resource Sharing**
AFIPS Conference Procceding, vol. 36, 1970

[19] L. Pouzin
**Presentation and Major Design aspects of the Cyclades Computer Network**
Procceding 3rd Data Communications Symposium, St Petesburg, Nov. 1973

[20] V. Cerf and R. Kahn
**A Protocol for Packet Network Intercommunication**
IEEE Trans. Communication, vol. COM-22, 1974

[21] Alberto León García e Indra Widjaja
**Redes de Comunicación Conceptos Fundamentales y Arquitecturas Básicas**
McGraw Hill 1ª Edición

## INTERNET


[I 1] http://www.iec.csic.es/criptonomicon/seguridad/
[I 2] http://www.rediris.es/rediris/boletin/35/enfoque2.html
[I 3] http://www.cintel.org.co/ONLINE/rct_online_agosto/
[I 4] http://personal.telefonica.terra.es/web/loseskakeados/seguridad1.htm.htm
[I 5] http://europa.eu.int/information_society/eeurope/news_library/pdf_files/execsum_es.pdf
[I 6] http://download.hispasec.com/hispasec/unixsec.zip
[I 7] http://it.unex.es/sypi/default.htm
[I 8] http://www.iec.csic.es/criptonomicon/seguridad
[I 9] http://www.seguridadenlared.org/es
[I 10] http://agamenon.uniandes.edu.co/revista/articulos/otraopcion.html
[I 11] http://www.microsoft.com/latam
[I 12] http://www.maestrosdelweb.com/actualidad/noticia.asp?id=1811
[I 13] http://maite71.upc.es/~soriano/cripto.htm
[I 14] http://www.rebol.com/docs/core23/rebolcore-13.html
[I 15] http://webs.ono.com/usr016/Agika/index.html
[I 16] http://www.geocities.com/CapeCanaveral/2566/
[I 17] http://www.iies.es/teleco/publicac/publbit/bit109/infoviainternet.htm
[I 18] http://www.itrainonline.org/itrainonline/spanish/networking.shtml
[I 19] http://compnetworking.about.com/cs/networksecurity/
[I 20] http://webs.ono.com/usr016/Agika/3internet/seg_internet.htm
[I 21] http://cvirtual.racsa.co.cr/seguridad.html
[I 22] http://www.iec.csic.es/criptonomicon/seguridad/
[I 23] http://www.start-art.com/vr/libros/seguridad.htm
[I 24] http://www.mixmarketing-online.com/vocabulario.html
[I 25] http://www.windowstimag.com/atrasados/2001/58_nov01/articulos/formacion.asp
[I 26] http://www.monografias.com/cgi-bin/search.cgi?substring=1&bool=and&query=Firewall
[I 27] http://www.lafacu.com/apuntes/informatica/
[I 28] http://compnetworking.about.com/cs/authentication/index.htm
[I 29] http://rinconquevedo.iespana.es/rinconquevedo/Criptografia/redundancia.htm
[I 30] http://compnetworking.about.com/cs/encryption/index.htm
[I 31] http://www.faqs.org/rfcs/rfc1288.html
[I 32] http://www.faqs.org/rfcs/rfc742.html
[I 33] http://www.codeproject.com/internet/cfinger.asp
[I 34] http://www.tldp.org/HOWTO/Firewall-HOWTO.html
[I 35] http://www.vicomsoft.com/knowledge/reference/firewalls1.html
[I 36] http://compnetworking.about.com/cs/firewalls/index.htm
[I 37] http://www.snmp.org/protocol/
[I 38] http://www.dpstele.com/dpsnews/articles/snmp/snmp_intro.html
[I 39] http://visualroute.visualware.com/
[I 40] http://compnetworking.about.com/cs/networktools/
[I 41] http://www.catalyst.com/support/help/cstools3/library/whois/
[I 42] http://www.monografias.com/intoredes
[I 43] http://orbita.starmedia.com/~josiane_rodriguez_suarez/proyecto_redes.html
[I 44] http://www.cesg.gov.uk/site/iacs/itsec/media/intro-guides/criteria.pdf
[I 45] http://niap.nist.gov/cc-scheme/ValidatedProducts.html
[I 46] http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=17
[I 47] http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=15