# SEGURIDAD DE LA INFORMACIÓN

## Precaución después de robo de $34,000 a un banco

Sábado 14 de Julio del 2001

"Un doctor de Melbourne, Australia, ha recomendado a los clientes del banco que tengan cuidado con sus cuentas de cheques. El dijo que le robaron $34,000 de su cuenta y tarjetas de crédito en el Commonwealth Bank of Australia. El banco le ha asegurado a sus clientes que sus cuentas están seguras porque si son robadas o sometidas a fraude electrónico, los montos serán reembolsados.

Pero el vocero del banco, Bryan Fitzgerald, dijo que no puede asegurar que otros clientes no hayan sido víctimas de fraude.

El anterior presidente de la Asociación Médica Australiana, Gerald Segal, ha criticado la respuesta del banco después de que descubrió que le fue retirado dinero de su cuenta en montos de $2000 sin su consentimiento."

theage.com.au, 2001

## Reportada grave falla de seguridad en Hotmail

"En una grave transgresión de seguridad, millones de cuentas de Hotmail han quedado expuestas en la Web. En potencialmente una de las más grandes exposiciones de correo electrónico jamás vista, un sitio Web podría tener a las personas accediendo millones de cuentas privadas."

ZDNN Staff, Agosto 30, 1999

## La gran mentira sobre la privacidad

"¿Ha visto a uno de esos abogados de la televisión hábilmente inventar una gran mentira para su cliente culpable? Lo mismo está sucediendo con la gran mentira acerca de privacidad en Internet. La mentira es que los mecanismos de privacidad están funcionando. La verdad es que usted es más vulnerable que antes. Y a menos que emprendamos acciones para defendernos nosotros mismos – pronto – nuestra información privada estará expuesta para cualquiera que desee obtenerla. Sí, alguien puede acusarme de ser demasiado cínico, demasiado impaciente. Yo no soy el único. Justo ayer, el Centro de Información para la Privacidad Electrónica (EPIC) presentó una querella contra la Comisión Federal de Comercio (FTC). Esta es la agencia del gobierno encargada de monitorear la privacidad en Internet. EPIC desea conocer si la FTC es realmente capaz de responder a las demandas de privacidad – o si deben tomarse acciones más agresivas para proteger a los consumidores en línea."

Jesse Berst, Editorial Director, ZDNet AnchorDesk, Octubre 13, 1999

# 1. Introducción

El concepto de comercio por Internet está principalmente relacionado con anunciar, comprar y vender productos y servicios con el objetivo básico de reducir costos e incrementar los beneficios. En años anteriores, el uso comercial de la red estaba bastante restringido. Sin embargo, hoy en día muchas políticas de restricción han sido eliminadas y las compañías pueden utilizar Internet para resolver variados problemas.

Para algunas empresas, el comercio por Internet es sinónimo de tomar órdenes de compra utilizando tarjetas de crédito de clientes que compran utilizando catálogos electrónicos. Para otras, el comercio significa interactuar electrónicamente con los clientes y proveedores como una forma alternativa al intercambio electrónico de documentos utilizando líneas de comunicación privadas. Este uso de Internet es conocido como Redes Privadas Virtuales ("Virtual Private Network - VPN"). Un tercer uso del comercio por Internet es la autenticación digital.

La WWW, el nombre popular de Internet, ha afectado significativamente cómo se llevan a cabo los negocios. Hasta hace poco, las promociones de un producto o servicio se realizaban por medios escritos, televisión o radio. Más aún, el comercio entre compañías o personas se efectuaba involucrando teléfonos, gente, departamentos, facturas y el correo postal. Ahora, las organizaciones incluyen direcciones electrónicas (correo y sitios Web[1]) en sus anuncios y promociones para expandir sus posibilidades comerciales. La red también está siendo utilizada para eliminar el costoso papeleo y la sobrecarga de trabajo de los métodos manuales.

La publicidad y el mercadeo mediante sitios Web es la principal razón para que muchas compañías usen Internet. Las empresas crean sus propias páginas electrónicas para anunciar y mercadear sus productos y explicar al público cuáles bienes o servicios proporcionan.

El comercio electrónico ha revolucionado la forma en que los consumidores alrededor del mundo están adquiriendo bienes y servicios. Sin importar si usted está buscando un artículo difícil de conseguir, o necesita hacer una entrega a un amigo que se encuentra geográficamente lejos, las compras "en línea" le permiten localizar los productos en una forma sencilla y por lo general amigable. Con este concepto, no hay que movilizarse de tienda en tienda, buscar parqueo para el vehículo o hacer fila en las cajas.

[1] Otro seudónimo para Internet. En este documento utilizaremos indistintamente los términos WWW y Web para referirnos a la red genérica Internet.

La selección del producto, facilidad de acceso, oportunidad y conveniencia, hacen del comercio electrónico una forma adecuada de llevar a cabo las compras sin salir de la casa o la oficina. Debido a estas razones es que las compras electrónicas se han convertido en una de las actividades más populares de Internet. El rápido crecimiento del comercio electrónico o "e-commerce" ha cambiado la forma en que los bienes y servicios se compran y se venden. Los consumidores han obtenido una forma ágil y conveniente de comprar globalmente, y los proveedores han adquirido medios más efectivos y menos costosos de ampliar su base de clientes.

Realizar negocios por Internet presenta algunas ventajas y desventajas. Entre las ventajas podemos citar:

- Un aspecto positivo es la relativa poca inversión económica que representa crear un sitio Web. Los bajos costos permiten a las compañías pequeñas competir de igual a igual con las grandes empresas. Por supuesto que la inversión realizada estará en proporción directa al tipo de producto ofrecido, el mercado meta y los objetivos de calidad, ventas y servicio que pretenden lograrse.
- Los sitios Web también ofrecen la posibilidad de expansión geográfica. Más aún, el ahorro de costos ayudan a mejorar el servicio y reducir el tiempo de respuesta.
- No es muy costoso crear interfaces Web para clientes o anuncios. Los bajos costos de la publicidad permiten a las pequeñas compañías competir de "igual a igual" con las empresas más grandes.
- Internet también ofrece posibilidades a los negocios locales para expandir su base de clientes en el ámbito internacional. Alrededor de dos mil millones de órdenes de compra han sido colocadas este año en Internet, que representan mundialmente un monto cercano a los $95 mil millones.

Desdichadamente, existen varias desventajas relacionadas con el comercio por Internet que son muy significativas. Entre estas desventajas destacan:

- Es difícil distinguir a una empresa y sus productos de otras similares.
- Las reglamentaciones concernientes a impuestos, importación/exportación, etc. pueden ser muy restrictivas.
- Los clientes potenciales pueden experimentar dificultades localizando una determinada compañía por la gran variedad existente de éstas.

En Internet, los conceptos de comercio y seguridad están estrechamente relacionados. La necesidad de contar con procesos de comercio mediante esta red de carácter mundial es sin duda muy fuerte en la comunidad de negocios. La Web le ha abierto las puertas a muchas compañías para realizar transacciones comerciales a escala global. Desafortunadamente, esto también ha incrementado la aparición de negocios engañosos y clientes inescrupulosos. La confianza del consumidor en la seguridad de la red es actualmente baja, aún cuando, por ejemplo el fraude de crédito por Internet es estadísticamente bajo.

Una vez que la seguridad, y por ende la integridad y la privacidad, estén garantizadas, las personas y las empresas confiarán más y se producirá un nivel mayor de transacciones sobre la red.

El potencial del comercio electrónico es una de las principales razones que están contribuyendo al rápido crecimiento de Internet como un medio de comunicación y negocios. Como en cualquier actividad comercial, es importante considerar las implicaciones de seguridad en la forma de hacer negocios, especialmente para obtener el grado preciso de satisfacción de todas las partes involucradas en las actividades emprendidas.

La necesidad de contar con un adecuado nivel de seguridad es crítica para que los proveedores de bienes y servicios, junto con sus posibles consumidores, puedan confiar unos en otros. Los primeros requieren la garantía de que sus mercancías serán pagadas, mientras que los segundos esperan que lo adquirido por ellos sea entregado bajo las condiciones originalmente pactadas. Hay sin duda, negocios y usuarios inescrupulosos que se dedican a llevar a cabo actividades ilegales, disminuyendo la confianza en los procesos de compra/venta. Es en este sentido que el tema de la seguridad adquiere una dimensión particular y esencial para el campo del comercio electrónico.

Conforme la necesidad por los aspectos de seguridad en Internet se incrementa, nuevos mecanismos y protocolos están siendo desarrollados permanentemente. Sin embargo, un sistema de seguridad siempre estará en función de la organización que controla el sistema. Por lo tanto, si la red Internet se vuelve o no más segura dependerá de los vendedores de tecnología y de las empresas que adquieran ésta. Las personas son quienes tienen la responsabilidad de decidir qué, cómo y cuánto confiar. De esta forma, la seguridad no es tanto un problema técnico sino de personas, derivando su fortaleza del entendimiento y aceptación que éstas tengan del término confianza.

# 2. Comercio electrónico[2]

La seguridad en la Web y el comercio electrónico están estrechamente unidos, ya que el crecimiento de este último depende en gran medida de la confiabilidad de la red. Una investigación de la firma consultora Forrester [TIWANA 1999] establece que para el año 2002:

- $327 mil millones en negocios serán realizados por Internet
- $10 mil millones de tiquetes de viaje se venderán por la WWW
- $2 mil millones en ventas de música se producirán en la red

El comercio electrónico se presenta como una clave para encontrar nuevas fuentes de ingreso, extenderse a otros mercados fuera de las fronteras geográficas, reducir costos y crear estrategias de negocios emergentes y no tradicionales. Pero los riesgos que encara esta clase de comercio se han convertido en su principal detractor, permitiendo que la infraestructura creada sea susceptible a abusos, fallos, fraude o interrupción. Debido a lo anterior, es que cualquier compañía que participe (o esté pensando en hacerlo) de transacciones comerciales digitales o intercambio de dinero electrónico, debería dar prioridad a los aspectos de seguridad.

## 2.1 Naturaleza del comercio por Internet[3]

"Establecer buenas relaciones con los clientes y socios comerciales es la clave para la creación de un negocio exitoso".

El advenimiento del comercio electrónico provee a las empresas una mayor oportunidad para usar Internet y construir relaciones más estrechas con sus clientes y socios. Esto es porque Internet es un buen canal de comunicación -es rápido, razonablemente confiable, bajo en costo y ampliamente accesible.

Los negocios de todos tamaños están listos para ganar a través del desarrollo de una estrategia de comercio exitosa en línea. Las empresas con las soluciones comerciales mejor adaptadas a las demandas de la Era Digital obtendrán una ventaja competitiva.

Internet también puede promover colaboración y una relación más cercana entre las empresas. Por ejemplo los proveedores y compradores pueden utilizar Internet para

[2] Para un mayor nivel de detalle relacionado con los temas de comercio electrónico y mercados electrónicos, se recomienda la lectura del Informe del Club de Investigación Tecnológica "Comercio Electrónico" elaborado por el Dr. Roberto Sasso en Marzo de 1997.

[3] El siguiente apartado se transcribe tal y como aparece publicado en el sitio Web de la empresa Microsoft Corporation bajo el título **"Comercio y el Sistema Nervioso Digital".** Representa un buen resumen del concepto de comercio electrónico.

trabajar de cerca en proyectos conjuntos tales como encontrar el éxito de la promoción de un producto en tiempo real. O los detallistas pueden visitar el sitio Web de un proveedor para chequear en el momento la disponibilidad de un producto y pedir una orden.

La visión de comercio de Microsoft es que cada compañía utilice Internet para crear relaciones más fuertes con sus clientes y socios. Microsoft provee la tecnología, el alcance de mercado y las asociaciones con los proveedores de soluciones que le permita a las compañías construir soluciones comerciales exitosas como parte de su sistema nervioso digital. Estas soluciones generalmente caen a uno de los cuatro tipos de procesos empresariales:

1. **Mercadotecnia directa, ventas y servicios.** Esto incluye el desarrollo de marca, ventas directas y servicio al cliente para relaciones de empresa-empresa al igual que empresa-cliente. Creando visibilidad del sitio, enfocando esfuerzos a clientes interesados, generando prospectos de venta a través de una rica experiencia en las compras, y proveyendo un servicio de respuesta al cliente y el soporte crítico para la mercadotecnia directa, ventas y servicio en línea. Otras consideraciones importantes son las autorizaciones y pagos seguros de las tarjetas de crédito, cálculo de los impuestos automatizado, cumplimiento flexible y una integración con los sistemas existentes de “back end” tales como inventarios, facturación y distribución.

2. **Servicios financieros e informáticos.** Facturación en línea, servicios de inversión, banca en su casa, distribución de productos digitales y de contenido, caen en esta categoría. Aunque las empresas no confíen en Internet para el mercadeo, ventas y servicios, ellos y sus clientes pueden beneficiarse considerablemente por facturar y por el pago de éstos. La persona promedio recibe 12 recibos al mes por correo de vendedores, compañías de tarjetas de crédito y por utilidades. La mayoría de estas compañías están empezando a darse cuenta de los beneficios de vender sus facturas a través de Internet como "e-bills"[4]. Los servicios aquí pueden incluir la entrega de información y medios digitales. Tal distribución a través de Internet requiere de un soporte especial para la retención de los derechos de propiedad intelectual, también conocido como el manejo de los derechos digitales.

3. **Compras corporativas.** Internet puede ayudar a automatizar procesos manuales para la mayoría de las compañías, haciendo que las compras sean de una aplicación de “autoservicio” para los vendedores y una aplicación de intercambio para los proveedores. Generalmente esto involucra que las compras sean de bajo costo, bienes "indirectos" de alto volumen, reparaciones y operaciones. Estos bienes incluyen productos de oficina, productos de limpieza y partes de repuesto. Los beneficios de las compras corporativas en línea incluyen costos administrativos más bajos, mejoramiento en respuesta y reducción en inventarios de los bienes y las partes de repuesto.

4. **Cadena de valor.** Esto abarca establecer vínculos directos con los socios comerciales ya sea "hacia arriba" a los proveedores o "hacia abajo" a los distribuidores y

[4] Facturas Electrónicas (nota de los autores).

vendedores. Internet virtualmente elimina la necesidad y el costo de redes privadas, abriendo de esta manera las comunicaciones de empresa-empresa y el comercio de las compañías de cualquier tamaño. El comercio en Internet conjunta las relaciones entre las empresas para crear una cadena de valor dinámica que reduce los requerimientos de inventario, recorta los ciclos de cobranza de facturas, y hace que los negocios sean más abiertos hacia a sus clientes.

### 2.1.1 Retos en la implantación del comercio electrónico

Es fácil describir el comercio electrónico y los resultados de los beneficios por su implantación. No es tan fácil desarrollar y llevar a cabo los sistemas de comercio electrónico.

### 2.1.2 Costo

El comercio electrónico requiere de sistemas sofisticados distribuidos y basados en tecnología nueva que pueda tocar el alma de los procesos de negocio de una empresa. Como lo es con la mayoría de los sistemas empresariales, el sistema de comercio electrónico requiere de una inversión significativa en hardware, software, contratación y capacitación. Los negocios necesitan una solución comprensiva que sea fácil de usar y pueda entablar un desarrollo que tenga una buena relación costo-eficiencia.

### 2.1.3 Valor

Los negocios quieren saber que sus inversiones en los sistemas de comercio producirán un retorno en sus inversiones. Estos despliegan sistemas de comercio electrónico para poder alcanzar los objetivos de los negocios tales como la generación de prospectos, proceso automatizado de negocios y reducción de costos. Quieren asegurarse que se cumplan estos objetivos. Las empresas también necesitan soluciones flexibles para que fácilmente puedan adaptar un sistema que cumpla con las condiciones cambiantes de los negocios.

### 2.1.4 Seguridad

Porque Internet provee un acceso casi universal, los activos de la compañía deben ser protegidos del mal uso, ya sea accidental o maliciosamente. Al mismo tiempo, esa protección no debe de comprometer el uso de un sitio o su desempeño ni tampoco hacer su desarrollo muy complejo. Hay un punto adicional de seguridad ya que los sistemas de comercio electrónico permiten la recolección y el uso de información sensible acerca de los clientes individuales, las empresas también necesitan proteger la privacidad de sus clientes.

### 2.1.5 Sistemas existentes

Las empresas necesitan poder montar una funcionalidad de las aplicaciones existentes en los sistemas de comercio electrónico. La mayoría de las empresas nuevas al comercio electrónico usan la información tecnológica para conducir los negocios en ambientes de

No-Internet en mercados existentes, manejo de órdenes, facturación, inventarios, distribución y sistemas de servicio al cliente. Internet representa una alternativa y una manera complementaria en la forma de hacer negocios. Es imperativo que los sistemas de comercio por Internet integren a los sistemas existentes de una manera en que eviten duplicar funciones y que mantengan su uso, funcionalidad y confiabilidad.

### 2.1.6 Interoperabilidad

La interoperabilidad significa aquí el enlace de las aplicaciones de socios comerciales para poder intercambiar documentos de negocios. Estos sistemas deben trabajar en conjunto para lograr cumplir los objetivos de los negocios. Por ejemplo, la aplicación del manejo de pedidos de un socio comercial debe interoperar con las aplicaciones de los inventarios para sus proveedores. Interoperar entre negocios reduce costos y mejora el desempeño. Permite la implantación de cadenas de valor más dinámicas".

## 2.2 Modalidades del comercio electrónico

"Los sistemas de pago digitales son una forma de dar dinero a alguien sin tener simultáneamente que entregar oro, monedas, billetes o cualquier otro ítem tangible. Es la transferencia del valor sin necesidad de transferir también los objetos físicos. Es la capacidad de hacer un pago en bits en lugar de átomos" [GARFINKEL 1997].

Los pagos digitales no representan un concepto nuevo. El dinero electrónico ha sido intercambiado entre empresas desde los años 60 mediante la transferencia de fondos. Más recientemente, los clientes han dispuesto de cajeros automáticos para obtener dinero. Y las tarjetas de cargos (créditos y débitos), en uno u otro formato han sido usadas desde hace más de 80 años.

Las modalidades de pago digital son muy diversas. En este apartado mencionaremos aquellas que gozan de mayor popularidad en el ámbito comercial y que se sustentan en una infraestructura de redes computacionales para su operación, de las cuales Internet representa, cada día más, la plataforma en uso por excelencia.

### 2.2.1 Tarjetas de crédito

Debido a que muchos comerciantes ya poseían mecanismos para manejar transacciones de cargo a tarjetas vía teléfono, éstas fueron la escogencia obvia para los primeros sistemas de pago basados en Internet. Sin embargo, las tarjetas de crédito presentan un problema: el número es esencialmente una palabra de paso de carácter permanente que puede usarse de manera continua para cargar pagos a la cuenta del poseedor de dicha tarjeta. Por esta razón, los números de tarjetas deben ser protegidos de la "escucha indiscreta". Actualmente, hay tres formas de realizar esta clase de transacciones en la Web:

1. **"Fuera de línea"** ("Offline"). Después de que la orden es colocada en la red, el cliente llama al comerciante y le indica telefónicamente el número de su tarjeta de crédito. Este método no es muy seguro porque las líneas de teléfono pueden ser "escuchadas" o las centrales interferidas.
2. **"En línea" sin encripción**[5]. El cliente envía el número de tarjeta de crédito por correo electrónico o lo digita en la página HTML que aparece en su computadora. Aunque aparenta ser el método más inseguro, son realmente pocos los casos documentados de fraude con tarjetas de crédito.
3. **"En línea" con encripción**. La transacción es encriptada (por el programa navegador o por el sistema de correo electrónico) antes de ser enviada al comerciante.

Aunque las tarjetas de crédito son el medio por excelencia de pago, otras modalidades están adquiriendo mayor relevancia ya que poseen menores costos por transacción, anonimato y un mercado más amplio (una gran cantidad de personas no son elegibles para obtener una tarjeta de crédito). Estas otras modalidades[6] caen en una de las siguientes categorías:

1. **Anónima**. No es posible para un comerciante o una entidad bancaria conocer la identidad del cliente si éste decide ocultar su información personal.
2. **Privada**. Aunque el comerciante no conoce la identidad del cliente, puede averiguarla si se pone de acuerdo con la organización que opera el sistema de pago.
3. **Con identificación**. Los sistemas de pago pueden identificar al cliente en todos los casos. Los cheques son un ejemplo de esta categoría.

### 2.2.2 Efectivo digital ("DigiCash" o "E-Cash")

Es un mecanismo de pago electrónico desarrollado por David Chaum, y está basado en un sistema de fichas ("tokens") digitales conocidas como *monedas digitales*. Cada moneda es creada por el cliente y firmada digitalmente por una casa de monedas que puede ser operada por un banco o un gobierno. Los clientes pueden entonces intercambiar monedas entre ellos o con la casa de monedas.

### 2.2.3 PIN virtual ("Virtual PIN")

En 1994, la empresa First Virtual Holdings (FVH) introdujo el sistema PIN Virtual para hacer cargos a tarjetas de crédito por Internet. Este sistema no requiere de ningún software especial para que un cliente pueda realizar sus compras. En vez de esto, los pagos son autorizados por correo electrónico. No se emplea ningún modelo de encripción. Más bien, la seguridad recae en la dificultad de interceptar los mensajes de correo electrónico, en mantener los datos de las tarjetas de crédito fuera de Internet y en disponer de un período

[5] Usamos "encripción" por "cifrado", dada la popularidad del primer término
[6] Una buena descripción de estas modalidades se encuentra en [GARFINKEL1997].

de 60 días para revertir una transacción. Los mensajes intercambiados entre el comerciante y FVH utilizan como mecanismo de autenticación las firmas digitales.

### 2.2.4 Efectivo cibernético o monedas cibernéticas ("CyberCash/CyberCoin")

Este sistema está fundamentado en la tecnología de encripción de llave pública que utilizan normalmente las transacciones de tarjetas de crédito por la WWW. El cliente utiliza Cibermonedas que son emitidas por el servidor de Ciberefectivo, el cual funciona como una tarjeta de débito. Las tarjetas de crédito sirven para abrir cuentas donde se depositarán las cibermonedas que serán acreditadas a dichas tarjetas. El uso de esquemas criptográficos mejora la seguridad de las transacciones.

### 2.2.5 Tarjetas inteligentes ("Smart Cards")

Las tarjetas inteligentes se parecen a las tarjetas de crédito excepto que almacenan información en microprocesadores o memorias en vez de bandas magnéticas. Otras características incluyen:

- Almacenan mucho más información por la tecnología que utilizan.
- Pueden ser protegidas por palabras claves ("passwords").
- Son capaces de utilizar algoritmos de encripción como el RSA para generar pares de llaves del tipo pública/privada, donde la llave pública puede ser libremente leída, no así la llave privada. De esta forma, para desencriptar un mensaje, la tarjeta debe estar físicamente en poder del dueño.

El uso de tarjetas inteligentes es cada vez mayor, y es quizá la tecnología que a futuro tiene mayor proyección mundial.

### 2.2.6 Mondex

Aunque no es un sistema de pago basado en Internet, Mondex constituye uno de los sistemas de pago digital de más amplia difusión en el ámbito mundial. Es un sistema cerrado que utiliza tarjetas inteligentes del tamaño de una tarjeta de crédito, y un protocolo secreto. La tarjeta es cargada con efectivo por medio de un dispositivo ATM[7] especial, y descargada con máquinas telefónicas de tecnología propietaria. La seguridad de este sistema descansa exclusivamente en el secreto de su tecnología.

[7] ATM es la abreviatura de *Automatic Teller Machine* o cajero automático.

## 2.3 Características deseables del dinero electrónico

Para que pueda ser ampliamente aceptado y utilizado de la misma forma que el papel moneda, el dinero electrónico debe reunir al menos las siguientes características [TIWANA 1999]:

- **Seguridad**. El sistema debe ser a prueba de fraudes, o al menos reducir significativamente los ataques por intrusión para revelar su información.
- **Costos reducidos por transacción**.
- **Escalabilidad y confiabilidad**. La implantación debe permitir mejoras futuras y sufrir la menor cantidad de "caídas" posible.
- **Independencia del "plástico"**. El sistema debe poder ser usado por quien tenga el dinero para pagar los ítems que esté comprando.
- **Utilización con cualquier cliente o servidor Web**. No debe estar limitado a un producto específico de software o versión del protocolo HTTP.
- **Independencia del hardware**. Ningún dispositivo especial debería ser requerido para obtener acceso o utilizar el dinero.
- **Privacidad y anonimato limitado**. Algún nivel de anonimato debe ser provisto para intercambiar el dinero.

Por otra parte, la seguridad de las transacciones electrónicas solo puede garantizar si:

- Las transacciones son inaccesibles para toda persona excepto para el comprador y el vendedor (principio de privacidad).
- La información no puede ser alterada durante su transmisión (principio de integridad).
- El vendedor está seguro de que la transacción es emitida por el verdadero comprador (principio de autenticación).
- El comprador está seguro que el vendedor es genuino (condición de no-falsificación).
- El comprador no puede desconocer su transacción si realmente la generó (condición de no-rechazo o no-repudiación).

# 3. Internet: la red de redes[8]

La comprensión del funcionamiento moderno de los sistemas de comercio electrónico obliga necesariamente a desarrollar el tema de Internet. Aunque no todas las transacciones comerciales realizadas electrónicamente emplean Internet como plataforma de comunicación y transferencia de información, la denominada Red de Redes, o la WWW, es sin lugar a dudas el punto de referencia actual y futuro para el ámbito de los negocios, sean éstos de la naturaleza que sean. Por esta sola razón, no podemos llevar a cabo el transitar por el campo de la seguridad en el comercio electrónico si no brindamos antes un panorama general de la red, sus componentes y funcionamiento. Este es el énfasis del presente capítulo y la base de los siguientes.

## 3.1 Breve historia de Internet[9]

Internet ha existido por aproximadamente 30 años y se define como una red de sistemas computacionales interconectados alrededor del mundo. Estos sistemas operan mediante protocolos de comunicación comunes a través de los cuales se comparte información. Sus inicios se remontan a 1969 con el nombre de ARPANET, un proyecto del Departamento de Defensa de los Estados Unidos diseñado para proporcionar comunicaciones confiables entre el sector militar y sus contratistas de defensa. Posteriormente, la academia extendió su uso a nivel mundial.

La World Wide Web (WWW) es un conjunto de programas y protocolos de Internet que presenta la organización de la información como documentos en formato hipertexto y tiene dos funciones principales:

- Lectura no lineal de documentos
- Acceso a los recursos de Internet

Es un sistema cliente – servidor y administra dos tipos de documentos: textos e índices. Se "navega" con algún programa explorador como por ejemplo: Netscape, MS Internet Explorer, y otros más.

La WWW fue desarrollada en 1989 por Timothy Berners-Lee del Laboratorio Europeo para la Física de Partículas (CERN) como un protocolo de comunicación común para permitir que los sistemas de cómputo y los usuarios pudieran intercambiar información. Poco tiempo después, en 1992, fue creada una interfaz gráfica de usuario conocida como MOSAIC, que puso a disposición del público en general la WWW. Hoy en día, el

[8] Una buena aproximación al tema puede encontrarse en [NAIK 1998].
[9] El anexo "Los desarrollos previos a la Internet", resume los principales acontecimientos en el marco de las redes de computadoras, que condujeron a la aparición de ARPANET primero y de Internet posteriormente.

Consorcio World Wide Web (W3C) administra los estándares correspondientes a Internet, la cual es visitada diariamente por millones de personas y su presencia ha creado la oportunidad de establecer negocios y comercializar bienes y servicios.

A inicios de 1995, Internet tenía una cobertura mundial de 15,000 redes y más de 30 millones de computadoras, en más de 180 países. Originalmente, Internet se desarrolló en un ambiente UNIX, pero ahora sus servicios pueden encontrarse en los más diversos ambientes como:

- Microcomputadoras PC-compatibles, Macintosh, etc.
- Sistemas Operativos UNIX, VMS, OS, etc.
- Mini y supercomputadoras.

El siguiente cuadro muestra la evolución histórica de Internet en cuanto a número de computadoras conectadas en diferentes períodos:

| **Año** | **Número de computadoras conectadas** |
|---|---|
| 1970 | 4 |
| 1975 | 73 |
| 1980 | 205 |
| 1985 | 5816 |
| 1990 | 80000 |
| 1995 | 30000000 |
| 2000 | +70000000 (estimado) |

Cada día se conectan más de 1,000 nuevos computadoras a Internet. Más de 20 millones de mensajes viajan por Internet cada semana. Mensualmente, la cantidad de datos que se transmite por Internet se incrementa en un 14%. Se pueden acceder más de 7 millones de servidores Web y más de 100 millones de documentos en pocos segundos usando un dispositivo tan simple como un “ratón”.

## 3.2 Necesidad de protección en Internet

*"Internet es un fenómeno increíble y poderoso que une a la gente y a las organizaciones, y promueve el intercambio de información alrededor del mundo, 24 horas al día. Pero Internet también tiene sus amenazas y peligros. Todos, desde un simple usuario hasta una agencia del gobierno, universidades o grandes corporaciones, se encuentran en riesgo. Los Hackers y los Crackers allá afuera escogen como objetivo a la gente en sus diferentes niveles para robarles información e ingresar ilegalmente en sus sitios, invadiendo la privacidad y quebrantando la confidencialidad y la integridad."*

Marcus Gonçalves

*Noviembre 2 de 1988, 9:00 p.m., Estados Unidos*

Varias organizaciones informan que están teniendo problemas con sus computadoras, las cuales sufren caídas constantes. La evaluación posterior de la situación indicó que un programa de origen desconocido logró infiltrase en los sistemas computacionales, reproduciéndose a sí mismo indefinidamente, consumiendo los recursos computacionales y anulando las operaciones de comunicación en las redes de informáticas. El saldo: 6,000 computadoras deshabilitadas unas cuantas horas después de reportado el hecho, y miles más en la misma situación al día siguiente, incluyendo compañías industriales y comerciales, universidades, centros de investigación e instituciones de servicios públicos.

*Marzo de 1998, Estados Unidos*

Dos adolescentes irrumpieron en una de las redes del Pentágono después de varios intentos que revelaron un plan sistemático y bien organizado. Esto ocurrió 4 años después de que dos *hackers* violentaron la seguridad de las redes del Laboratorio de la Fuerza Aérea en Syracuse, Nueva York, donde se desarrollan algunos de los proyectos más importantes del Departamento de los Estados Unidos en materia de armamento.

*Agosto 13 de 1994, San José, Costa Rica*

Estafan 12 millones de colones a un puesto de bolsa. De acuerdo a la noticia publicada ese día por el periódico La Nación: "Un empleado que sirvió de informante y unas notas enviadas por fax, fueron los instrumentos para estafar por ¢12,5 millones a un puesto de bolsa".

Los casos anteriores representan apenas una mínima muestra de las amenazas y ataques de naturaleza humana y electrónica combinada que suceden diariamente alrededor del mundo. Las dos razones fundamentales que permitieron la ejecución de estos hechos delictivos fueron:

- Defectos de diseño y errores ("bugs") de programación en el software utilizado en las redes computacionales.
- Ausencia total o parcial de políticas de seguridad efectivas tanto en el ámbito técnico (equipos y programas) como administrativo (personas y procedimientos).

Pocas son las personas que realmente se preocupan por conocer la existencia de las amenazas latentes a su **privacidad**. Los ataques a ésta tienen orígenes muy diversos, desde compañías privadas, hasta empresas públicas e individuos. La vigilancia personal por gente ordinaria es más común de lo que uno pudiera pensar. En cuanto a los sistemas computacionales, la disponibilidad, el manejo y el intercambio de información relativa a las personas es prácticamente incontrolable, lo que las deja en un estado casi total de indefensión. El no escuchar a menudo por los medios de comunicación la ocurrencia de casos de violación de la privacidad no significa que estas situaciones no se produzcan. Recordemos que aunque alguien (persona u organización) descubra que su cuenta de correo electrónico o sistema computacional ha sido violentada, el público rara vez llega a enterarse de tales hechos. Después de todo, nadie desea ser el blanco de este tipo de publicidad.

Para conseguir un préstamo, obtener la licencia de conducir, ser admitido en un hospital o simplemente utilizar la tarjeta de crédito para realizar nuestras compras del hogar, los individuos tienen que llenar (o firmar) documentos en los cuales adjunta información personal. Muy poca de esta información se mantiene en forma **confidencial**. La mayoría por el contrario, es reprocesada y hasta vendida a una amplia variedad de compañías, dentro y fuera de los países. En una red como Internet, la manipulación de datos personales es constante. Gran parte de los sitios Web que brindan productos o servicios, ya sea gratuitos o que cobren por ellos, solicitan información personal mínima al usuario Esta información viaja por múltiples centros de comunicación alrededor del mundo, desde el punto de origen hasta el lugar de destino. Por lo tanto, estos datos están sujetos a ser "escuchados", copiados y hasta manipulados sin conocimiento y aprobación del dueño de la información. Entonces se vuelve crítico utilizar herramientas para mantener la confidencialidad de dicha información.

La **integridad** es otra de las características de la información que en el entorno de una red telemática es imprescindible garantizar. Ciertas transacciones, como las de tipo bancario, requieren no solo que se mantenga la confidencialidad de los datos sino también que se respete la integridad de los mismos, es decir, que se garantice que la información original no fue modificada. El mantener la integridad en Internet no es una tarea fácil. Varios son los elementos que pueden tener incidencia en la alteración de la información:

- Problemas de los dispositivos físicos como computadoras, módems, tarjetas de red calidad de las líneas de transmisión, etc.
- Problemas de software como errores en el sistema operativo, los programas de comunicación, las aplicaciones de usuario final (navegadores, transferencia de archivos y otros).
- Problemas humanos como *hackers* malintencionados y los *crackers*.

La red Internet está siendo expuesta cada día más a los **fraudes[10] electrónicos**. Entre los casos más comunes en esta categoría se encuentran la intervención de transacciones con tarjetas de crédito, el espionaje industrial, y la introducción de "código malicioso" en las estaciones de trabajo y servidores para robar información o causar su modificación o destrucción no autorizada.

A manera de resumen, las amenazas en Internet pueden presentarse en dos niveles:

- **Nivel de red**: ataques al hardware y el software.
- **Nivel de transacción**: ataques a la capacidad de intercambiar mensajes (correo electrónico), archivos (con protocolos como el FTP) e información en sus diferentes formatos.

Adicionalmente, los riesgos inherentes a Internet imponen cuatro áreas prioritarias de protección de la información:

- **Protección de documentos** que pueden ser manipulados por individuos no autorizados comprometiendo su confidencialidad e integridad.
- **Protección de transacciones** que pueden ser interceptadas mientras que los usuarios remotos envían información a un servidor Web.
- **Protección de información personal** como códigos de usuario, palabras claves, número de tarjeta de crédito, etc.
- **Protección contra los efectos colaterales de los errores de programación** en las aplicaciones y sistemas de Internet.

## 3.3 Conceptos principales

Para obtener una clara comprensión de los componentes de seguridad involucrados en el comercio electrónico utilizando como plataforma tecnológica la red Internet, es necesario definir un conjunto de conceptos y una terminología básica acerca de los elementos sustantivos del entorno Web. Aunque la cantidad y variedad de éstos es significativa, nos centraremos en aquellos que participan directamente o como factores complementarios en la determinación de los niveles de seguridad presentes en Internet. Para cada término definido se presenta su traducción (que se ha intentado hacer lo más literal posible respetando la idea detrás del concepto) y el nombre original (en idioma inglés) de acuerdo con la literatura computacional estándar.

[10] De acuerdo al Gran Diccionario Enciclopédico SALVAT de 1989, el término fraude significa: "Acción encaminada a eludir cualquier disposición legal, sea fiscal, penal o civil, siempre que con ello se produzca perjuicio contra el Estado o contra terceros".

### 3.3.1 Servidores y clientes Web

Un *Servidor Web* (o sitio Web) es un sistema computacional en el que residen las páginas Web, los programas de administración de estas páginas y el software para recibir y responder solicitudes para manejo de archivos HTML. Un Cliente Web es, en contraste, cualquier computadora que realice solicitudes a un servidor Web para recibir estas páginas en formato HTML.

### 3.3.2 Localizadores uniformes de recursos ("Uniform Resource Locators" - URL's)

Un Localizador Uniforme de Recursos es una dirección para un recurso de la red. Es similar a un nombre de archivo pero incluye también el nombre del servidor, información acerca del protocolo de red que utiliza el recurso así como parámetros específicos y datos del nombre del usuario. Las páginas Web utilizan los URL's para enlazar otras páginas. Un ejemplo común de URL podría representarse de la siguiente manera:

http://www.cit.co.cr

Los esquemas de URL más populares se presentan a continuación:

| URL | Significado |
|---|---|
| http | Protocolo de Transferencia de Hipertexto |
| https | Protocolo de Transferencia de Hipertexto encriptado sobre el protocolo de seguridad SSL |
| ftp | Protocolo de Transferencia de Archivos |
| news | Noticias de la red Usenet |
| telnet | Sesión interactiva de Telnet |
| file | Nombres de archivos locales |
| mailto | Dirección de correo electrónico |

### 3.3.3 Protocolo de Transferencia de Hipertexto ("HyperText Transfer Protocol"–HTTP)

El HTTP es el método principal que utilizan los protocolos Web para transferir datos entre un servidor y un cliente. Es un protocolo cliente/servidor que dispone de pocas instrucciones y funciones y es muy eficiente para la entrada y salida de información.

Maneja direcciones URL y se utiliza en ambientes gráficos multitexto y multimedios. Existen clientes HTTP ("Web Browsers"), servidores HTTP ("Web Servers") y servidores proxy[11]/gateway[12] HTTP que actúan como servidores ante un cliente y como cliente ante otro servidor para resolver direcciones que provienen de otras redes. El formato de las instrucciones no contiene ninguna información vinculada con la sesión de transferencia de los datos como por ejemplo: el identificador de la sesión, el usuario, etc.

### 3.3.4 Lenguaje de Señalización de Hipertexto ("HyperText Markup Language"–HTML)

En la WWW, la información es representada como un conjunto de páginas Web escritas en el Lenguaje de Señalización de Hipertexto o HTML. Las páginas, que representan enlaces dinámicos hacia otros objetos como bases de datos y otras páginas Web, están usualmente almacenadas en los servidores Web y son solicitadas y recibidas utilizando mensajes con el formato del protocolo HTTP.

### 3.3.5 Extensiones MIME ("Multipurpose Internet Mail Extensions" – MIME)

Antes de la aparición del formato MIME, Internet estaba restringida a transportar únicamente datos ASCII, es decir, los datos eran transportados como bytes, pero el bit más significativo tenía que ser un cero. La especificación de formato MIME resuelve esta deficiencia permitiendo el transporte de datos binarios (cualquier combinación de unos y ceros en los ocho bits).

Una variante del MIME, el S/MIME define un protocolo para agregar seguridad a los mensajes electrónicos, proporcionando privacidad al encriptar dichos mensajes y autenticación con la inclusión de firmas digitales (este tema será tratado con mayor profundidad posteriormente). La encripción que utiliza el S/MIME está basada en el cifrado simétrico[13] y la clave de encripción emplea un algoritmo de llave pública.

En los últimos años, los programas navegadores han incrementado su capacidad para leer información que ha sido añadida[14] a los documentos HTML. El navegador utiliza el encabezado del mensaje HTTP para averiguar el tipo de información que debe entender. Aún cuando estos navegadores no están diseñados para comprender más allá del formato HTML y unos cuantos formatos de archivos de imágenes (por ejemplo: BMP, GIF, TIFF, JPG y algunos otros), aceptan todas las formas posibles de documentos (hojas electrónicas,

[11] Representante
[12] Vía de acceso o compuerta
[13] S/MIME recomienda el uso del algoritmo RC2 en modo de cifrado con encadenamiento de bloques y llaves de encripción de 40 bits. Una versión separada de S/MIME para los Estados Unidos utiliza como algoritmo de encripción el DES (ya prácticamente en desuso) o el Triple DES.
[14] En el lenguaje computacional y especialmente en el de correo electrónico, esta información en forma de archivos se conoce como "Attachments".

archivos de sonido, vídeo, etc.) desde el servidor Web. Cuando detecta un formato no reconocido, el navegador busca en la base de datos MIME para localizar una Aplicación de Ayuda MIME ("MIME Helper Application") que sí pueda comprender y procesar el formato específico.

### 3.3.6 Galletas HTTP ("HTTP Cookies")

Debido a que el protocolo HTTP no mantiene información dependiente de la transacción o sesión de trabajo del usuario, los programas navegadores tratan las instrucciones como mensajes de solo lectura. Sin embargo, poco tiempo después de la generalización en el uso de Internet, muchas personas y empresas observaron la posibilidad de guardar información de las sesiones en los clientes Web para ser recuperada más adelante. Por ejemplo, los proveedores de bienes y servicios deseaban dar a sus clientes un número de referencia para ayudarlos a asociar varias transacciones HTTP de compra (o consulta) con un solo identificador de tal forma que en el futuro se pudiera hacer alusión a este identificador sin tener que suministrar nuevamente toda la información por parte del cliente. También los anunciantes en la red buscaban la forma de dar seguimiento a los lugares visitados por los usuarios para crear bases de datos demográficas y personalizar los sitios Web con contenido dinámico para aumentar su base de clientes.

Para cumplir con los anteriores objetivos, la empresa Netscape propuso e implementó las denominadas *Galletas HTTP* (o simplemente *Galletas*), concebidas como pequeñas cantidades de datos que el servidor Web guarda y puede recuperar posteriormente del sistema cliente. Las galletas funcionan como el juego popular de la tinta invisible: un objeto es marcado con una fórmula especial de "tinta" que solo es visible bajo ciertas condiciones (por ejemplo, con el calentamiento del objeto). En Internet, la marca se coloca en el computadora del cliente y el poseedor del secreto para hacerla aparecer es el que mediante el uso de un servidor Web colocó la información.

Las galletas son usadas normalmente por las interfases CGI y código de programación en el lado del servidor, y son administradas por aplicaciones de navegación llamadas Agentes de Usuario HTTP ("HTTPUser Agents"). Los navegadores almacenan los datos en una base de datos o en uno o más archivos. Algunos más sofisticados le permiten al usuario rechazar las galletas o eliminar galletas previamente guardadas en sus computadoras.

Desde el punto de vista de la seguridad (y como se podrá observar más adelante) las galletas pueden representar un riesgo potencial de exposición de la información porque contienen en algún grado, de datos del cliente.

### 3.3.7 Códigos Adicionables ("Plug-Ins")

En sus inicios, los navegadores Web solamente podían extender sus capacidades por medio de aplicaciones de ayuda del tipo MIME, que eran procesos independientes. La empresa Netscape desarrolló entonces el concepto de Código Adicionable o simplemente "Plug-Ins" para extender estas capacidades en una forma integrada. La interfaz del "Plug-In" fue diseñada para incorporar de una forma más transparente, aplicaciones que soporten tipos de datos no reconocidos intrínsecamente por el programa navegador y para hacer a estas aplicaciones más independientes de la plataforma de hardware y software en que se ejecutan con el objetivo de facilitar su migración a otros ambientes.

Cuando el navegador encuentra un tipo de datos MIME que no comprende, verifica si existe algún "Plug-In" que soporte el formato específico, y si lo localiza emite una instrucción para ejecutarlo. Estos "Plug-Ins" son código API que le permiten al navegador intercambiar información y compartir recursos del sistema. Por su naturaleza de código ejecutable, un "Plug-In" puede representar un riesgo para la seguridad de un sistema computacional ya sea por contener código malicioso (o ser blanco de él, como los Caballos de Troya) o porque si no está correctamente diseñado puede convertirse en una eventual Puerta Trasera.

### 3.3.8 Interfaz de Compuerta[15] Común ("Common Gateway Interface" – CGI)

Además de transmitir archivos, un servidor Web puede ejecutar programas en respuesta a una solicitud de entrada. Estos programas son invocados empleando la Interfaz de Compuerta Común o CGI que permite la conectividad entre servidores HTTP y otras formas de datos no-HTTP. El servidor HTTP ejecuta un proceso CGI que es a menudo una aplicación local ("stand-alone"). Una aplicación CGI es iniciada por un cliente HTTP especificando un URL que apunta a ésta. Entonces, el servidor HTTP ejecuta esta aplicación CGI y retorna el resultado al cliente HTTP. Este esquema no representa una técnica muy eficiente porque requiere que un programa separado se inicie cada vez que se recibe una solicitud de entrada Otros métodos alternativos como el Netscape API[16] (NAPI) permiten que el mismo servidor Web responda a las solicitudes.

[15] Compuerta es la traducción que se ha dado en este documento al término en inglés Gateway. Una compuerta es por lo general, un computador especializado en administrar distintos protocolos de comunicación para permitir el enlace de redes heterogéneas.

[16] Abreviatura del término " Application Programming Interfaces" o Interfaces para la Programación de Aplicaciones, que son bibliotecas de funciones utilizadas para escribir aplicaciones de redes y comunicaciones

### 3.3.9 Aplicaciones Java ("Java Applets[17]")

Las aplicaciones Java son pequeños programas independientes de la plataforma de hardware y sistema operativo, que se ejecutan dentro del contexto de un documento HTML en un navegador. Estos programas, que se almacenan en los servidores Web y son enviados[18] al cliente empleando el protocolo HTTP, agregan información dinámica como audio, vídeo, acceso a hojas electrónicas, bases de datos y otros más. Java es un lenguaje orientado a objetos, basado en C++. En vez de compilar a un código nativo, el código Java es traducido a códigos de byte y ejecutados por una Máquina Virtual Java ("Java Virtual Machine" – JVM). El lenguaje Java tiene un conjunto de API's que son transportables a una variedad de plataformas de hardware y sistemas operativos, proporcionan una funcionalidad básica (manejo de ventanas, administración de memoria, entrada/salida, etc.) y se encuentran agrupados en paquetes. Los "applets" son aplicaciones especiales de estas funciones API, que no pueden existir por sí mismas, requiriendo ser invocadas por otra aplicación para poder ejecutarse.

### 3.3.10 Controles ActiveX ("ActiveX Controls")

Desarrollada por Microsoft Corporation, la tecnología ActiveX proporciona una interfaz amigable en ambientes Web y un conjunto muy amplio de funciones cliente/servidor. A diferencia del Java, los controles ActiveX no requieren un lenguaje de programación específico, pudiendo ser implementados en Visual C++, Visual Basic, Java, y otros más.
Los controles ActiveX están basados en el Modelo Objeto-Componente de Microsoft ("Component Object Model" – COM) e intenta sustituir a la tecnología OLE (por "Object Linking and Embedding").

[17] Los Applets son programas de tamaño reducido utilizados por los navegadores en un ambiente Web.Típicamente escritos en el lenguaje de programación Java desarrollado por Sun Microsystems, los applets (sin traducción literal) incrementan las capacidades de navegación con texto mejorado, gráficos y animaciones. Desde el punto de vista de seguridad son muy importantes porque Java puede fluir a través de una pared de fuego sin mayores contratiempos a menos que se tomen las debidas precauciones para prevenirlo. [ANONYMOUS 1998]
[18] El término en inglés en este caso es "download".

## 3.4 Funcionamiento de la red Internet: conjunto de protocolos TCP/IP[19]

Desde hace muchos años, una organización gubernamental estadounidense, la Agencia de Proyectos de Investigación Avanzada o ARPA por sus siglas en inglés[20], ha venido realizando investigaciones en el campo de las redes de comunicación telemática. La tecnología ARP incluye un conjunto de estándares de red que definen los detalles de cómo deben comunicarse las computadoras, así como el grupo de reglas[21] para interconectar redes y para controlar el enrutamiento del tráfico de información. El TCP/IP es la asociación de varios protocolos (pero principalmente dos: El Protocolo de Control de Transmisión o TCP y el Protocolo Internet o IP), independientes del hardware y el software de implantación, para facilitar la interconexión de redes dentro o fuera de las organizaciones, y forma la base de lo que se conoce como la red de redes: Internet. Por su gran éxito, Internet ha demostrado la viabilidad de la tecnología TCP/IP y muestra cómo puede incorporar una amplia variedad de tecnologías subyacentes de red.

El TCP/IP permite a los desarrolladores y fabricantes de aplicaciones y dispositivos para redes computacionales, aislarse de los detalles de bajo nivel de la comunicación de información, lo que presenta ventajas como:

- No es necesario recordar muchos detalles de la configuración del hardware involucrado.
- Las aplicaciones no se encuentran restringidas a una sola arquitectura de computadora, o a un solo tipo de hardware de red.
- Las aplicaciones son más portátiles ("portables") entre sistemas operativos heterogéneos, ampliando las posibilidades de conexión de equipos de muy variada naturaleza.

Las características que diferencian al TCP/IP de otros tipos de red se pueden resumir en:

- Independencia de la tecnología de red.
- Interconexión universal. El TCP/IP facilita la comunicación entre cualquier par de computadoras conectadas a la red. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red, y cada paquete de mensajes (datagrama) lleva en su interior las direcciones de su fuente y destino. Mientras tanto, las computadoras intermedias de conmutación, utilizan la dirección destino para la toma de decisiones de enrutamiento.

[19] Una porción de este apartado es extraída de la sección "1.2 El TCP/IP de Internet" de [COMER 1996 ]. Se recomienda la lectura de este libro porque brinda un excelente tratamiento del conjunto de protocolos que conforman el TCP/IP.
[20] ARPA se inició como una agencia de investigación para proyectos de defensa hasta mediados de la década del 60.
[21] Formatos de mensajes, descripción de cómo un sistema computacional debe responder cuando recibe un mensaje, manejo de errores o condiciones anormales, etc.

- Acuses de recibo punto-a-punto. El acuse de recibo de la información se da entre la fuente y el destino únicamente (aún cuando las dos computadoras no estén conectadas a la misma red física) y no entre máquinas sucesivas a lo largo del camino.
- Estándares de protocolo de aplicación. El TCP/IP incluye servicios básicos de nivel de transporte y de aplicación como correo electrónico, transferencia de archivos y acceso remoto.

Las siguientes figuras ilustran el funcionamiento y principales componentes de los sistemas computacionales que interactúan en Internet.[22]. En la Figura 1 se pueden apreciar los componentes constitutivos de un sistema computacional en Internet: usuarios, computadoras (hardware y software), líneas de comunicación, dispositivos de transmisión de información (hardware y software) y proveedores de servicios (personas, hardware y software). Cada uno de estos componentes incorpora un elemento de seguridad específico a la red total. Por esta razón, cuando se habla de seguridad en el ámbito del comercio electrónico, irremediablemente deben tomarse en cuenta todos estos factores.

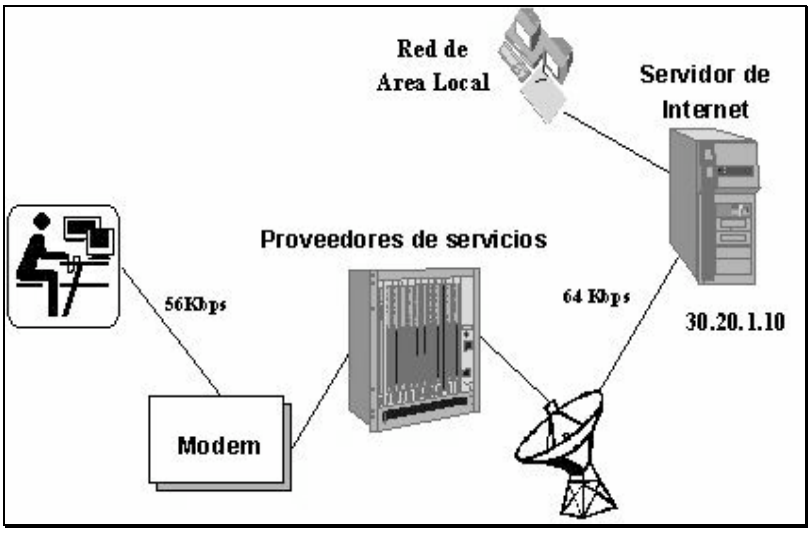


Fig.1. Componentes básicos de una red Internet

Una computadora puede estar conectada directamente a Internet (conexión dedicada) o puede también conectarse esporádicamente por medio de una sesión remota (a través de un módem y una línea telefónica).

[22] Estas figuras son importantes para entender más adelante, las posibles amenazas y ataques a que pueden verse sometidos los usuarios en una red como Internet.

En la Figura 2, se pueden apreciar los componentes físicos y lógicos que permiten la comunicación de la información, a saber: enrutadores, protocolos de comunicación (como por ejemplo, TCP/IP, SLIP/PPP, etc.), módems, centrales telefónicas y servidores de comunicación.

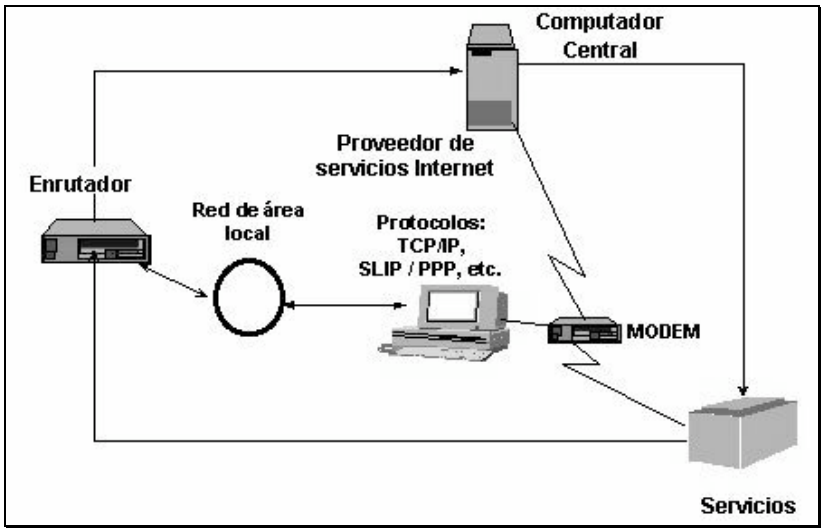


Fig. 2. Componentes físicos de comunicación

En la Figura 3 se muestran los diferentes tipos de enlaces de comunicación y conexión a Internet como por ejemplo los enlaces telefónicos, radiales o satelitales, y los protocolos de comunicación y conversión representados por la "nube de Internet".

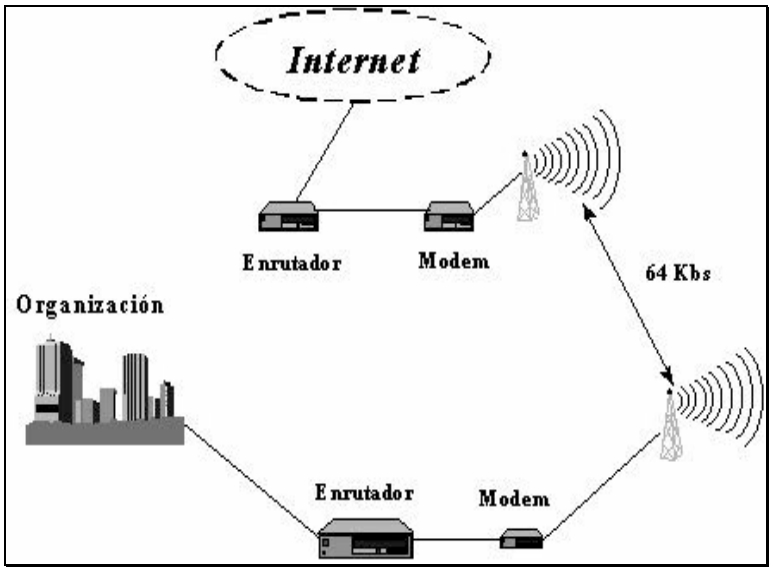


Fig. 3. Enlaces de comunicación

Es posible identificar las computadoras en Internet vía nombres simbólicos, en lugar de números. El Sistema de Nombres de Dominios (“*Domain Name System”)*, es un sistema para asignar y administrar nombres por dominios[23] y subdominios, por ejemplo:

- library.wustl.edu
- administra.cic.itcr.ac.cr

Así, para contactar a Pedro Pérez en este último dominio, vía su dirección electrónica se utilizaría: pperez@administra.cic.uned.ac.cr.

Algunos dominios de uso común son:

- com: organizaciones comerciales
- edu: organizaciones educativas (universidades, escuelas secundarias, etc).
- gov: organizaciones gubernamentales
- mil: organizaciones militares
- net: recursos de la red
- {cr, uk, fr, ...}: dominios por país

Cada dispositivo en Internet debe tener una dirección distintiva de forma tal que la información enviada a éste pueda ser correctamente entregada. Este esquema de direccionamiento es controlado por el protocolo IP. Las direcciones IP consisten de dos partes: la porción de red y la porción del equipo anfitrión (“host”). La primera parte es utilizada para describir la red donde reside el anfitrión, mientras que la segunda se requiere para identificar a un anfitrión particular. Para asegurar que las direcciones de red son únicas, una agencia central es la responsable por asignarlas, la Autoridad Internet de Números Asignados (IANA). Esta organización establece los procedimientos y tiene el control sobre los números asignados. Sin embargo, cuando una institución se une a Internet, puede obtener direcciones de red desde el Centro de Información de la Red Internet (INTERNIC).

Los identificadores de anfitrión se clasifican en representaciones sucesivas de bajo nivel conocidas como nombres, direcciones y rutas. El nombre identifica lo que el dispositivo es, una dirección indica dónde está y la ruta define cómo llegar hasta ahí. Las direcciones IP pueden expresarse de diferentes maneras, pero la más común es la notación decimal con puntos, donde cada número está separado por uno de ellos, por ejemplo: 196.193.200.158.

Existen cuatro clases de direcciones principales: A, B, C y D. Las tres primeras se usan para identificar los dispositivos que comparten una red común. La clase D o de multidifusión (“multicast”) sirve para reconocer un conjunto de dispositivos que comparten un mismo protocolo. Sin importar la clase, cada dirección consiste de 32 bits (4 bytes u

[23] Un dominio es una jerarquía de nombres. Sintácticamente, un nombre de dominio consiste de una secuencia de nombres (o etiquetas) separadas por puntos [COMER 1996].

octetos). Cada anfitrión posee una dirección IP específica que le permite a otros anfitriones comunicarse con él. Dependiendo de la clase de red, pueden existir desde 253 hasta millones de anfitriones en la red. Como no es práctico definir una red con miles o millones de anfitriones, la porción de dirección del anfitrión se separa en redes adicionales conocidas como *subredes*, usando máscaras de red.

Las direcciones IP pueden ser difíciles de recordar, por lo que a cada dispositivo se le asigna un nombre de anfitrión ("hostname"). Para que el TCP/IP trabaje correctamente este nombre debe ser traducido a su correspondiente dirección IP. Esto puede lograrse de varias formas, incluyendo un archivo de nombres ("hostnames") o recurriendo al Servicio de Nombres de Dominio ("Domain Name Service" – DNS).

## 3.5 Servicios en Internet

Internet dispone en la actualidad de una muy amplia variedad de servicios ofrecidos por muchas compañías, los cuales tienen su fundamento en el conjunto de protocolos TCP/IP. Entre los servicios más frecuentemente encontrados en Internet podemos citar:

- Noticias y grupos de discusión
- Compras en línea
- Comunicación directa entre dos o más personas ("chat")
- Búsqueda de software, archivos (texto, imágenes, video, etc.), bases de datos, y otros
- Correo electrónico
- Conexión remota a otras computadoras
- Acceso remoto interactivo a Sistemas de Información (texto, imágenes, hipermedios, bases de datos especializadas)
- Transferencia de Archivos (FTP)

Por la importancia que revisten hoy en día para la masificación en el uso y aceptación de Internet a escala mundial (y por ende para la seguridad de la información transmitida), revisaremos brevemente dos de los servicios de mayor difusión en la red: el correo electrónico y la transferencia de archivos.

## 3.6 Mensajería electrónica o correo electrónico ("Electronic Mail" – Email)

El servicio de correo electrónico es la aplicación más popular de intercambio de mensajes en Internet. Tuvo sus orígenes en sistemas propietarios de minicomputadoras y "mainframes", y su comercialización masiva inició con el advenimiento de las redes de área

local (LAN's). Las primeras implantaciones se caracterizaban por su falta de adherencia a protocolos de comunicación estándares.

En la implantación del correo electrónico, un servidor de archivos actúa como servidor de correo. Los clientes intercambian mensajes que pasan a través del servidor (o de varios servidores intermedios) el cual los almacena primero y los retransmite posteriormente a sus respectivos destinos (esquema de "store and forward") en atención a una operación de lectura (llamada a un procedimiento remoto o RPC) de parte de dichos clientes.

Existen tres modalidades de operación del correo electrónico:

- **Modelo "fuera de línea"** ("Offline"). El cliente se conecta de vez en cuando al servidor y recupera sus mensajes. Una vez transferidos éstos, son eliminados del servidor. El procesamiento posterior de estos mensajes tiene lugar en el cliente y el servidor no tiene conocimiento de esto.
- **Modelo "en línea" ("Online").** El cliente establece una sesión con el servidor y todo el procesamiento de los mensajes ocurre durante esta sesión en el servidor, con instrucciones del cliente. Un ejemplo muy común de este esquema son las "conversaciones personales" o "chats".
- **Modelo con desconexión ("Disconnected").** Este esquema es un híbrido de los dos anteriores. El cliente se conecta al servidor, recupera sus mensajes y los procesa "fuera de línea". En algún momento, el cliente se reconecta y envía al servidor los cambios realizados a los mensajes. Aunque el servidor es el depositario principal de la información, el cliente actúa como un almacén temporal.

Las aplicaciones de correo electrónico pueden utilizar varios protocolos para el transporte de los mensajes. Los más comunes son:

- **Protocolo de Oficina de Correo** ("PostOffice Protocol" – POP). Es un protocolo aplicable al modelo "fuera de línea" y actualmente se encuentra en su tercera revisión (POP3). Un cliente POP no puede recuperar selectivamente sus mensajes sino que está limitado a solicitarlos todos o ninguno.

- **Protocolo de Trasnferencia de Correo Simple** ("Simple Mail Transfer Protocol" – SMTP). Es un protocolo para la transferencia de mensajes de correo electrónico entre un cliente y un servidor o entre dos servidores. Sigue un esquema de solicitud-respuesta, se ubica en una capa superior del Protocolo TCP y está diseñado para transferir en forma eficiente múltiples mensajes a un cliente o a múltiples clientes.

- **Protocolo para el Acceso de Mensajes en Internet** ("Internet Message Access Protocol" – IMAC). Con este protocolo el cliente puede recuperar mensajes en forma selectiva o parte de éstos. Su uso es muy recomendable cuando se emplean líneas telefónicas con bajas velocidades de transmisión.

## 3.7 Protocolo de Transferencia de Archivos ("File Transfer Protocol" – FTP)

La transferencia de archivos se presenta con mucha frecuencia en las aplicaciones TCP/IP con tráficos significativos de red. Antes de la aparición del TCP/IP, existían protocolos de transferencia de archivos para ARPANET que evolucionaron hasta llegar al estándar actual conocido como FTP. La Figura 4 muestra el modelo de proceso FTP.

En una función de transferencia se tienen que tomar en cuenta los detalles de autorización, el nombre y la representación entre máquinas heterogéneas. El FTP incluye estas características además de [COMER 1996]:

- Acceso interactivo. La interfaz del FTP permite a los usuarios actuar de una manera interactiva con los servidores remotos.
- Especificación de formato (representación). El FTP permite al usuario especificar el tipo y formato de los datos almacenados
- Control de autenticación. El FTP exige a los usuarios que se autoricen a sí mismos enviando un nombre de conexión y una clave de acceso al servidor antes de solicitar la transferencia de archivos. El servidor rechaza el acceso a los usuarios que no puedan suministrar ambos parámetros.

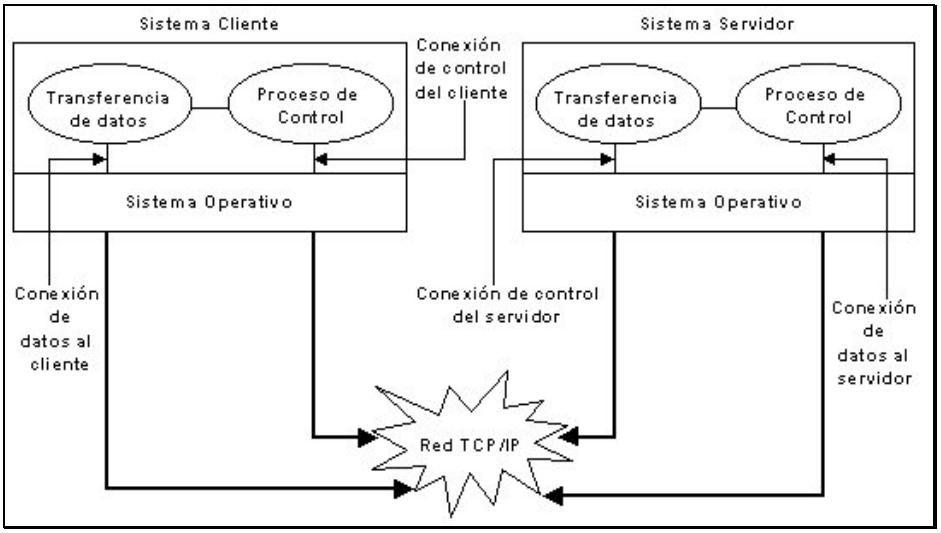


**Fig. 4. Modelo de procesamiento del FTP [COMER 1996]**

## 3.8 Elementos comunes susceptibles de ataques en Internet

Dentro de la amplia variedad de componentes y servicios que ofrece la WWW, algunos de ellos se presentan como los objetivos predilectos de ataque por parte de los denominados **cibercriminales** (*Hackers*[24] malintencionados o *Crackers*[25]) [Hernández 1998].

### 3.8.1 Protocolo de Transferencia de Correo Simple ("Simple Mail Transfer Protocol" - SMTP)

Este protocolo incluye la instrucción "MAIL FROM" que muestra la dirección de retorno del mensaje No hay forma de confirmar si la dirección de retorno visualizada por dicha instrucción es genuina. Esto permite a un usuario enviar un mensaje de correo electrónico en forma anónima, adjuntando "código malicioso" y sin dejar rastro de su procedencia.

### 3.8.2 Protocolo de Control de Transmisión/Protocolo de Internet ("Transmission Control Protocol/Internet Protocol" - TCP/IP)

Este es el protocolo de transmisión de Internet. Los *hackers* maliciosos o los *crackers* pueden visualizar la información contenida en los paquetes de comunicación del TCP/IP que detallan tanto la dirección origen como la de destino de los mensajes. Esto les permite enviar información haciendo aparentar que proviene de un sistema autorizado.

### 3.8.3 Servidor de Nombres de Dominio ("Domain Name Server" – DNS)

El sistema DNS es una función básica en las comunicaciones en Internet. Los servidores DNS son bases de datos distribuidas que transforman nombres de sistemas computacionales (por ejemplo usuarios) en direcciones IP. Este tipo de sistema es vulnerable debido a que los *hackers* malintencionados o los *crackers* pueden localizar las direcciones IP de los sistemas conectados al servidor DNS.

### 3.8.4 Protocolo de Transferencia de Archivos ("File Transfer Protocol" – FTP)

FTP es un brinda un servicio muy valioso en Internet. Usando FTP, un usuario puede obtener software de dominio público, documentos, imágenes y archivos multimedios, lo cual representa un peligro potencial muy grande si no se conoce bien el contenido de este software o su procedencia real.

[24] " Hacker: Persona interesada en sistemas operativos, seguridad computacional e Internet. También, un programador o un individuo que se gana la vida programando". [ANONYMOUS 1998]

[25] " Cracker: Alguien que con intenciones maliciosas, ilegalmente quebranta la seguridad de un sistema computacional. Alguien que quebranta los esquemas de registro y protección de un software comercial". [ANONYMOUS 1998]

### 3.8.5 “Finger”

Es un programa utilitario de UNIX que permite a un usuario localizar información de otros usuarios en Internet. Desde una perspectiva de seguridad, es importante proteger correctamente la información, especialmente teniendo en cuenta que una de las formas predilectas de los *hackers* maliciosos y los *crackers* para introducirse en los sistemas es la recuperación de información de los usuarios. Por tanto, es indispensable restringir la cantidad de información que un “cibercriminal” potencial pueda recolectar a través de un servicio “Finger”.

### 3.8.6 Servicio de Terminal Virtual “Telnet”

Este es un servicio que entrega al usuario un acceso directo a computadoras que están conectadas a Internet. Por ejemplo, los catálogos, librerías e informes del tiempo pueden accederse directamente desde una sesión Telnet. El riesgo de seguridad existe ya que las conexiones vienen desde una red y pueden interconectarse con otras directamente, por lo que se hace necesario autenticarlas.

# 4. Seguridad en el comercio electrónico e Internet

Con el afán de entender mejor el concepto de seguridad, podríamos analizar la siguiente definición:

> *"Acción de proteger a una persona, animal o en general cualquier cosa contra determinados riesgos"* [HADF 1997].

La seguridad lleva implícitos una serie de costos de oportunidad, lo cual debe balancearse tanto con su utilización y el costo asociado de implementarla. De hecho, la seguridad es inversamente proporcional a la utilización y el costo, porque conforme un sistema se vuelve más seguro, también se hace más restrictivo y difícil de utilizar. Por lo tanto, el costo de administrar y mantener un sistema puede subir significativamente. Alcanzar un nivel apropiado de seguridad para un sistema es un balance delicado entre la protección necesaria y costo.

Las amenazas a los sistemas de información y la batalla para protegerlos son similares a una guerra de guerrillas. La guerrilla usa tácticas ocultas para minar y sabotear los sistemas instaurados. El enemigo es usualmente desconocido y se preocupa de cubrir su rastro para poder atacar de nuevo sin problemas. En algunos casos, la guerrilla obtiene información necesaria para acceder a los sistemas de los propios empleados de confianza de una institución. En algunos casos, el guerrillero es uno de estos empleados [SHELDON 1997].

En general, al tratar de establecer un apropiado nivel de seguridad es necesario tener en cuenta tres importantes factores:

- El tipo de amenaza a que se está expuesto
- El valor de lo que se está protegiendo
- El objetivo que se persigue con las medidas de seguridad

Las amenazas provienen del tipo de situaciones a que se pueden ver expuestos regularmente las cosas que serán objeto de la seguridad. El valor de lo que se está protegiendo influye en la determinación de la medida a escoger, por cuanto debe prevalecer un criterio de costo/beneficio. Por regla general, no resulta lógico establecer una medida de seguridad que sobrepase el valor del bien resguardado. El objetivo que se persigue determina de alguna forma el grado de intensidad o de profundidad con que se desea que actúe la medida de seguridad que se va a adoptar. Por ejemplo, no es lo mismo querer adoptar una medida de detección, en cuyo caso basta con percatarse del intento de llevar a cabo una acción no deseada, que desear adoptar una medida de carácter correctivo, con la cual, una vez detectada la situación indeseable, la medida deba llevar la situación a su estado original antes del ataque.

## 4.1 Seguridad en la WWW

En una red de comunicaciones como es el caso de Internet, la información puede verse enfrentada con amenazas que pertenecen a una de las siguientes categorías:

- **Ataques pasivos**. En un ataque pasivo el intruso simplemente monitorea el tráfico de información tratando de capturar datos sensibles. Tales ataques pueden basarse en la red ("escuchando" los enlaces de comunicación) o basarse en los sistemas (reemplazando un componente del sistema por un Caballo de Troya que capture la información requerida). Los ataques pasivos son los más difíciles de detectar. En general, uno debería suponer que siempre habrá alguien monitoreando la información que se transmite por Internet.

- **Ataques activos**. En estos casos, el atacante trata de vencer las defensas. Se pueden mencionar los siguientes tipos de ataques activos:

    - *Intentos de obtener acceso al sistema*: en donde el atacante intenta explotar las debilidades de seguridad para ganar acceso y control sobre un cliente o el servidor del sistema.
    - *Engaño ("spoofing"):* en donde el atacante se hace pasar por un sistema confiable para persuadir a que le envíen información sensible.
    - *Ataques criptográficos*: en donde el atacante intenta quebrantar la contraseña, o descifrar algunos de los datos (generalmente por medio del método de fuerza bruta).

- **Ataques de negación de la prestación del servicio**. Al atacante no le importa tanto intentar conocer información secreta sino más bien evitar los procesos sobre ésta, ya sea redireccionando el tráfico o incrementándolo con información inútil.

En el caso de la seguridad en la Web, los objetivos de seguridad más comunes son:

- **Control de Acceso**: asegurar que la persona o computadora en el otro extremo de la comunicación está debidamente autorizado para ejecutar las acciones que solicita realizar.
- **Autenticación**: asegurar que el recurso (humano o máquina) en el otro extremo de la sesión es realmente quien dice ser.
- **Integridad**: asegurar que la información que se recibe es la misma que se envió.
- **No Rechazo** ("No Repudiación"): asegurar que al producirse una transacción se pueda probar posteriormente que ésta efectivamente se produjo. Es decir, que tanto el emisor como el receptor acepten que el intercambio tuvo lugar.
- **Privacidad**: asegurar que la información sensible no es visible para intrusos, lo que se alcanza generalmente utilizando encripción.

Adicionalmente, la Web tiene algunas vulnerabilidades:

- Cuando un usuario selecciona un enlace ("link"), el sistema al que se está conectando es determinado por lo que se haya definido en el documento almacenado en el servidor. Si el servidor ha sido infiltrado, un intruso ("hacker") podría redireccionar al usuario hacia su propio servidor.
- Los programas CGI frecuentemente se escriben para implementar un requerimiento específico. Si el diseño o la programación no son sometidos a un estricto control de calidad, estos programas podrían contener errores ("pulgas"), explotables por un intruso.
- Los documentos HTML pueden incluir datos de diferentes tipos (gráficos, sonido, animación, etc.). En el programa navegador ("browser"), cada uno de estos tipos de datos está asociado con un programa de presentación, llamado visualizador. Estos programas son de por sí grandes y complejos, lo que implica que ellos podrían contener errores. Adicionalmente, algunos de estos formatos de archivos contienen capacidades de programación (un buen ejemplo de ello es el formato PostScript) que los hacen vulnerables a la modificación de su código por parte de un virus. Un intruso podría usar estas características para ejecutar sus propios programas o para instalar, modificar o destruir datos en las computadoras de los clientes.

## 4.2 Seguridad en los servidores

La efectividad de las medidas de protección en los servidores Web es el punto crítico para una organización. Las empresas colocan generalmente servidores de este tipo para distribuir información en Internet, aunque no es común que deseen ofrecer un acceso irrestricto a la misma. Sin embargo, y a pesar de que puede existir una conciencia clara de la necesidad de proteger la información, la mayor parte de las compañías fallan en brindar seguridad a sus sistemas de cómputo debido a que:

- Fracasan en establecer una política de seguridad y piensan que este tema es de naturaleza eminentemente técnica (por lo que le corresponde al Departamento de Sistemas de Información, la responsabilidad de velar por ella).
- Utilizan texto llano (no cifrado) y palabras claves ("passwords") que nunca expiran, en redes de cualquier tipo (de área local, de área ancha, Internet, etc.)
- No invierten en herramientas de seguridad o en la obtención de correcciones ("parches") a los programas de seguridad.
- Tienen malas prácticas de monitoreo de actividades relacionadas con la seguridad de la información (si es que éstas existen)
- No se ejercitan en el concepto de contingencias, es decir, no planifican contra desastres.

El reto en la protección de los servidores se encuentra en mantener los sitios Web seguros proporcionando comunicaciones seguras y colaboración para identificar y legitimar usuarios. En este sentido los requerimientos más importantes son:

- Necesidad de identificar y autenticar usuarios para garantizarles el acceso a la información y los servicios relacionados.
- Proteger los sistemas con efectivos mecanismos de control de acceso para evitar la incursión de los llamados cibercriminales.
- Asegurar a las empresas que pueden implementar canales de comunicación privados a prueba de intrusos (como las VPN's) y extender las redes corporativas hacia la Internet para llevar a cabo transacciones comerciales y financieras.
- Auditar y monitorear la aplicación de las políticas de seguridad establecidas.

## 4.3 Seguridad en los clientes

El ámbito de la seguridad de los clientes en Internet es bastante complejo por la diversidad de procesos y aplicaciones que pueden ejecutarse. Sin embargo, hay algunas áreas que representan los eslabones de seguridad críticos. Estas áreas incluyen:

**1.** Programas navegadores. Un navegador es:

- Una interfaz de búsqueda y despliegue de información.
- El primer punto de contacto entre un usuario y el universo cibernético.
- La puerta de acceso visual a los datos que fluyen por la red.

Una buena porción de los ataques a la seguridad informática se producen en los navegadores debido a las acciones que realizan los usuarios. Para no comprometer esta seguridad, los navegadores deben incorporar como mínimo, los siguientes aspectos en su diseño e implantación:

a. Utilización de mecanismos de encripción y protocolos de transmisión seguros como el SSL.
b. Empleo de encripción, firmas y certificados digitales con el objetivo de asegurar la integridad y autenticidad de la información.
c. Control estricto sobre los módulos Java, especialmente con los "applets" y los "scripts" (archivos de procedimientos de ejecución secuencial).

> **Recomendación**: Una buena política de control es utilizar únicamente módulos de procedencia conocida y preferiblemente certificados.

d. Control estricto sobre los módulos ActiveX. Su caso es similar a los módulos Java.

e. Control sobre la aceptación de galletas ("cookies"). Los navegadores más importantes en la actualidad tienen opciones para alertar o deshabilitar las galletas.
f. Definición de una política de seguridad en el uso y manejo del correo electrónico. Este servicio es el preferido de los cibercriminales para depositar virus (y todas sus variantes) en las computadoras de los usuarios.

**Recomendación**: Utilizar protocolos de seguridad para correo electrónico como el PEM, el PGP y el S/MIME

**2.** Certificados de Sitio. Un certificado de sitio permite a un servidor Web identificarse como un proveedor de servicios autorizado. Debido a que el nombre de un servidor es único e inalterable, los certificados deben incluir dicho nombre. Si un programa navegador en el cliente detecta una discrepancia entre este nombre y el incluido en el certificado emite una alerta al usuario.

**3.** Autoridades Certificadoras. Los navegadores tienen listas preinstaladas de empresas que emiten certificados para identificar y autenticar los sitios Web

**4.** Java y "Scripts" de Java. Java presenta cuatro aspectos de riesgo para las aplicaciones Internet, bajo ciertas condiciones:

- La capacidad de ejecutar arbitrariamente instrucciones utilizando un archivo binario y la creación de "applets".
- Los "applets" que ejecutan en un mismo navegador pueden interferir entre ellos. Entonces, un "applet" malicioso podría provocar un malfuncionamiento de los otros, provocando que ciertas operaciones del usuario sean rechazadas.
- Los "applets" pueden arbitrariamente establecer conexiones remotas con cualquier dispositivo en Internet (¡incluyendo máquinas de intrusos!).
- El administrador de seguridad puede ser obviado, permitiendo la ejecución de código malicioso.

JavaScript es un lenguaje de programación desarrollado por Netscape para hacer de las animaciones y otras formas de interacción más fáciles de usar. Los programas JavaScript residen en archivos HTML que tienen la capacidad de girar instrucciones al programa navegador. Debido a que una porción del lenguaje reside dentro del navegador, tiene potencialmente acceso a la información que éste maneja, violentando la privacidad de la información. Por esta misma razón, y al igual que los "applets" un programa JavaScript malicioso podría interferir con la ejecución de otros módulos provocando un rechazo de servicio.

5. Controles ActiveX. La tecnología ActiveX posee quizás la más grave amenaza a la seguridad en Internet que se haya detectado. Mediante un "applet" ActiveX es posible descargar un virus en una computadora, o bien esta aplicación podría grabar información sensible de una compañía y después enviarla a un competidor. Los controles ActiveX ofrecen un terreno muy fértil para los creadores de virus y los

*hackers*. En febrero de 1997, en un programa de la televisión alemana con cobertura nacional, miembros del Chaos Computer Club, mostraron un control ActiveX capaz de transferir dinero de una cuenta de un banco a otro sin necesidad de tener un número de identificación personal ("Personal Identification Number" – PIN) para autenticar la transacción. La tecnología ActiveX es completamente insegura porque permite que cualquier código binario contenido en los "applets" sea ejecutado o que otro tipo de código (por ejemplo un virus) se le adjunte.

## 4.4 Seguridad interna y seguridad física

Por lo general, al hablar de problemas de seguridad se piensa únicamente en que los ataques pueden provenir del exterior. Sin embargo, es necesario echar un vistazo a los aspectos internos, de forma tal que se tenga un mayor panorama de las posibles causas que pueden atentar contra la seguridad.

Según el documento Maximun Security [ANONYMOUS 1998], en estudios realizados recientemente se indica que más del 50% de las empresas que poseen un servidor de Internet han experimentado ataques remotos. La cifra, aunque impresionante, no revela que un número mucho mayor de empresas han sido objeto de ataques provocados por su propio personal. Solo por citar un ejemplo, un programador de una empresa médica, molesto porque fue despedido, podría antes de abandonar la empresa ejecutar una programa que destruya el trabajo de facturación de los servicios prestados en los últimos meses. La empresa víctima de este ataque puede no contar con respaldos actualizados (o no contar del todo con ellos), lo que le provocaría pérdidas económicas muy significativas y decenas de horas-hombre en trabajo. Y aunque parezca increíble, casos como estos ocurren diariamente.

Los ataques internos son más generalizados que los ataques remotos por varias razones:

- Atacar una red desde adentro es mucho más fácil. De hecho, los usuarios autorizados tienen acceso a información que no está disponible para los usuarios remotos. Por ejemplo, consideremos la tarea de crear una lista de todos los usuarios de la red. Para un usuario remoto lograr ingresar a los sistemas automatizados de la compañía para apropiarse de la información, puede resultar sumamente difícil. Por el contrario, para un usuario interno esta es una tarea mucho más sencilla.
- El personal interno tiene acceso a más herramientas computacionales directamente relacionadas con la plataforma de equipos y programas existentes en la organización que los usuarios remotos, como por ejemplo, compiladores o intérpretes de lenguajes de programación. Con estas herramientas un usuario interno podría intentar quebrantar exitosamente el sistema de seguridad.
- Algunos usuarios internos gozan de ciertos niveles de confianza o privilegios que les facilita el acceso a la información sensible de la empresa.

En procura de asegurar apropiados niveles de seguridad interna se podrían emprender acciones tendientes a:

- Establecer en forma clara y por escrito, políticas en torno a este tema[26] (definición de funciones y responsabilidades), y hacer que el personal las respete.
- Restringir el acceso a ciertos dispositivos críticos (como los módems, servidores de datos y comunicaciones, etc.) para que sean utilizados exclusivamente por aquellas personas que realmente lo requieren
- Instalar medidas de protección de naturaleza física, como cerraduras, sistemas de vigilancia por vídeo y otros, para aquellos dispositivos que procesen información crítica para el negocio.

Algunas veces el hardware puede representar un riesgo de seguridad interna. Considérese la utilización de módems dentro de la empresa. Acaso la empresa ha evaluado realmente si todos los empleados requieren acceso al exterior, pues se estaría brindando la oportunidad a todos ellos de extraer información de la empresa, enviarla hacia fuera sin que necesariamente se genere un registro de la transmisión. De esta forma se podría estar divulgando información sensible de la empresa, y detectar e identificar quién es la persona que lo está haciendo resultaría sumamente difícil, sobre todo si el número de personas con acceso a módems es considerable.

Otro aspecto a considerar sería lo referente a la seguridad física como el acceso a dispositivos, directorios y archivos. El solo hecho de que el personal interno tenga acceso a las estaciones de trabajo supone un riesgo muy alto para la confidencialidad e integridad de la información, pues ellos podrían agregar componentes como discos fijos, disquetes u otros dispositivos internos y respaldar en ellos información de naturaleza clasificada, o remover estos dispositivos para obtener también la información deseada. Debido al tamaño actual de estos componentes, es fácil ocultarlos en lugares como maletines, cajas y hasta debajo de la ropa de una persona, sin que se detecte en forma evidente su presencia.

Algunas veces las fallas en la seguridad interna se deben a la falta de una valoración de este tema. Para poder llevar a cabo tal valoración se requiere una persona que sea especialista en el asunto. De hecho en algunas organizaciones existe el puesto de oficial de seguridad o nombre similar, para representar a aquella persona que es responsable por realizar la valoración de las amenazas, sugerir las mejores medidas de control y ponerlas en práctica, intentando mantenerlas lo más actualizadas y vigentes que le resulte posible.

[26] Lo ideal sería que éstas formen parte de los correspondientes contratos de trabajo. Muchas organizaciones carecen de tales políticas y otras creen que es inútil implementarlas porque el personal siempre hará hasta lo imposible por ignorarlas. Si bien es cierto que las políticas no evitan que el personal ande indagando entre la información de la empresa, el hecho de que estén por escrito faculta a la empresa a que en caso de que un funcionario sea sorprendido haciendo algo indebido, se le pueda despedir y acusar formalmente ante una instancia judicial (si las circunstancias lo ameritan), para lo cual se tendría documentación útil en un proceso de esta naturaleza.

En vista de que para algunas organizaciones puede resultar algo difícil controlar la seguridad de la información entre sus empleados, se puede acudir a programas especializados llamados rastreadores de seguridad interna ("*internal security scanners"*), tales como SATAN, Asmodeous, Network Security Scanners y Nessus, por citar algunos productos existentes en el mercado, que mantienen una vigilancia permanente de los procesos de manipulación e intercambio de información en un sistema computacional.

Con respecto de Internet, es necesario ejercer un control estricto de su uso, pues ello puede acarrear, además de fugas de información como las ya comentadas, un despilfarro del tiempo de trabajo, como podría ser el producto de que los empleados estén accesando sitios con material pornográfico, o realizando labores que no tengan una relación directa con los fines de la empresa.

## 4.5 Particionadores-Irruptores y Agrietadores - Resquebrajadores ("Hackers" y "Crackers")

En el argot informático se utilizan estos dos conceptos sin que necesariamente la gente conozca realmente su significado. Un *hacker* es una persona que está intensamente interesada en trabajar y conocer a fondo algunos sistemas operativos. En la mayoría de los casos los *hackers* son programadores. Como tales, los *hackers* obtienen conocimientos muy avanzados de los sistemas operativos y lenguajes de programación. Ellos pueden descubrir deficiencias en estos sistemas y las causas. Una conducta muy típica de los *hackers* es buscar constantemente mayor conocimiento, lo que los lleva a compartir libremente el conocimiento adquirido y nunca intentan dañar datos de forma intencional.

En el "*New Hacker's Dictionary*" (escrito por un *hacker*), se ofrecen seis definiciones sobre el concepto de *hacker*:

- Persona que disfruta de explorar los detalles de los sistemas programables y de cómo exceder sus capacidades, en oposición a muchos usuarios quienes prefieren aprender solo lo mínimo necesario.
- Aquél que programa entusiastamente (aún obsesivamente).
- Persona buena para programar rápidamente.
- Experto en un lenguaje o sistema operativo en particular, como por ejemplo un *hacker* en Unix.
- Persona que disfruta de los retos intelectuales, de vencer o evitar limitaciones.
- Intruso malicioso que trata de descubrir información sensible para curiosear.

Por su parte, los *cracker* son personas que quebrantan o violentan la integridad de los sistemas computacionales remotos con intenciones maliciosas. Un *cracker* una vez que ha obtenido un acceso no autorizado, destruye datos vitales, niega el acceso legítimo a los servicios de los usuarios, o básicamente causa problemas a sus víctimas. Este grupo se identifica muy fácilmente debido a que sus acciones son siempre mal intencionadas.

## 4.6 Confidencialidad e integridad

La mayoría de datos que viajan por Internet no gozan de tratamiento confidencial. Los mensajes electrónicos frecuentemente se ven como tarjetas postales y cualquiera que las reciba puede leerlas. En Internet un mensaje es procesado por muchas redes y dispositivos que intervienen en el trayecto de la fuente hasta el destino. Cualquiera que tenga acceso a ellos, esté autorizado o no, está en capacidad de observar su contenido. La falta de privacidad existe no solo en los correos electrónicos, sino también en la mayoría de datos transferidos por medio de protocolos como el FTP y el HTTP.

Según datos de 1994, estos dos protocolos procesaron aproximadamente la mitad de los bytes transferidos por Internet. Apenas unos pocos paquetes de mensajes que atraviesan diariamente la red son enviados en una forma segura que garantiza su confidencialidad.

A pesar de que se puede argumentar que la mayoría de los datos de Internet no necesitan ser privados, también se puede razonar que al menos algunos de ellos sí deberían serlo. Afortunadamente existen soluciones disponibles. Los datos sensibles pueden ser encriptados en un formato ininteligible antes de transitar por la red, y desencriptados después de que se reciben. La criptografía ofrece una mayor privacidad que el sobre de papel en el cual viaja una tarjeta postal debido a que solo el destinatario puede "abrir" (desencriptar) el mensaje.

Dos condiciones mínimas relacionadas con la información deben cumplirse en la WWW para hacer de la red un medio confiable y efectivo en los servicios que puede brindar: la **integridad** y la **confidencialidad**.

La integridad se refiere a la condición actual de algunos datos al compararlos con su estado "puro" u original. Un mensaje o archivo que transita por Internet está en riesgo de ser modificado o eliminado a lo largo de su trayecto físico. Un mensaje que sufre alguna de estas dos acciones pierde entonces su integridad.

La confidencialidad tiene como objetivo proteger la información contra la divulgación o revelación a cualquiera que no esté autorizado para tenerla.

## 4.7 Técnicas de seguridad[27]

Aunque las amenazas en Internet existen en una cantidad y variedad muy significativa, la red no va a desaparecer por este motivo. Hay muchas formas de defenderse de los ataques que se presenten, aunque ninguna de éstas es, por sí sola, perfecta. El único método efectivo para garantizar que la información almacenada en un sistema computacional se encuentra segura, es mantener éste desconectado de todas las redes, protegerlo en un cuarto vigilado y no permitir que nadie lo acceda. La utilidad en este caso de dicho sistema es altamente limitada. Por lo tanto, se vuelve imprescindible definir estrategias de defensa que se encuentren soportadas por técnicas de seguridad cuya implantación incluirá tanto elementos técnicos (hardware y software) como administrativos (políticas, definición de funciones y asignación de responsabilidades para el personal, etc.).

En este apartado se describirán las técnicas de seguridad más comúnmente encontradas en Internet y que rigen todos los aspectos del comercio electrónico, a saber: la encripción, los certificados y las firmas digitales, la identificación y autenticación, los sistemas de llave pública y los controles de acceso. Los conceptos serán desarrollados independientemente de sus posibles implantaciones de hardware o software, que en todo caso representarían productos específicos de algunos fabricantes y que por lo general incluyen solo parcialmente las especificaciones teóricas. Los elementos administrativos se detallarán más adelante en el capítulo concerniente a las políticas y estrategias de seguridad en Internet.

### 4.7.1 Criptografía

La criptografía o "arte de enviar mensajes en clave secreta" es considerada actualmente como la técnica de seguridad más efectiva y económica para proteger la información. Aunque se implementa por lo general en software, también existen dispositivos especializados ("chips", tarjetas y hasta computadoras) para llevarla a cabo. La encripción es un método de escritura donde el texto en claro ("plain text"), es transformado en texto cifrado (algunas veces llamado cifra o criptograma) utilizando una llave criptográfica de transformación (conocida como clave) que puede ser de naturaleza pública (conocida por una o más personas) o privada (utilizada únicamente por las personas que desean intercambiar información). De la misma forma, al proceso inverso de transformar texto cifrado en texto en claro se le conoce como descifrado o desencripción. La Figura 5 muestra ambos procesos.

[27] Un tratamiento detallado de este tema puede encontrarse en [GÁMEZ 1995].

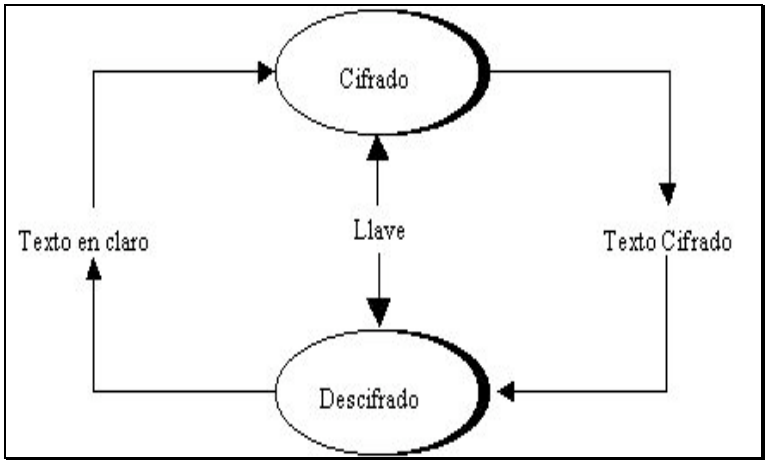


Fig. 5. Modelo de Encripción/desencripción

Existen tres tipos básicos de encripción: las **transposiciones,** las **sustituciones** y los **productos**. Las transposiciones reorganizan los bits o caracteres de los datos, cambiando su ubicación. Las sustituciones reemplazan bits, caracteres o bloques de caracteres por elementos sustitutos. La encripción de productos es un híbrido de los dos primeros tipos, donde los caracteres sufren simultáneamente sustituciones y transposiciones. La Figura 6 muestra los tres modos de encripción.


**Fig. 6. Tipos básicos de encripción**

Como ejemplo podríamos tener un tipo simple de ciframiento por sustitución desplazando cada una de las letras del alfabeto que se utilice, un número "*k*" de posiciones hacia adelante (en estos casos el ciclo se cierra cuando al llegar a la Z se pasa nuevamente a la A), en donde "*k*" es la llave de encripción. A este método se le conoce como el método de César, debido a que Julio César (Siglo I antes de Cristo) lo utilizó con un valor de $k = 3$.

En aplicaciones computacionales, la transposición es usualmente combinada con la sustitución. Por ejemplo, uno de los algoritmos de encripción más conocidos y empleados, el *DES* ("Data Encryption Standard"), encripta bloques de 64 bits (cada vez), usando una combinación de transposición y sustitución.

*Criptoanálisis* es la ciencia y estudio de los métodos para violentar (o quebrantar) los ciframientos. Un mensaje cifrado es violentado (o quebrantado), si es posible determinar el texto en claro o la llave a partir del texto cifrado, o determinar la llave para parejas de texto en claro-texto cifrado. Existen tres métodos básicos de ataque:

- El que se basa solo en el texto cifrado,
- El que se apoya en porciones conocidas de texto en claro, y
- El que se fundamenta en texto en claro escogido.

Hasta hace poco todos los criptosistemas eran de una sola llave, por lo que los mismos son usualmente considerados como sistemas convencionales (o clásicos).

En los criptosistemas asimétricos o de dos llaves, las llaves de cifrado y descifrado difieren una de la otra en el sentido de que, al menos una llave no es factible computacionalmente de ser determinada a partir de la otra. Entonces una de las dos articipacióne $E_K$ o $D_K$, puede ser revelada sin poner en peligro a la otra.

En 1997, el Instituto Nacional de articipac y Tecnología de los Estados Unidos ("*National Institute of Standards and Technology" – NIST*), hizo un llamado a la comunidad científica con el objeto de buscar un sustituto del DES, estándar que se ha utilizado en ese país en materia criptográfica por espacio de 25 años aproximadamente. De acuerdo a Bruce Schneier, en esa oportunidad se contó con la participación de 15 candidatos, entre ellos la empresa costarricense TecApro. Se estima que el proceso de selección puede tomar varios años.

### 4.7.2 Firmas digitales

Las firmas manuscritas en los documentos se han usado desde hace mucho tiempo como una prueba de que el firmante es el autor de éstos, o al menos, que está de acuerdo con el contenido. Sin embargo, ¿qué es lo que hace que las firmas mantengan esa condición de confianza?. Existen cinco razones por las cuales una firma manuscrita goza de toda la credibilidad del caso:

- La firma no puede ser falsificada. La firma es la prueba de que el firmante (o signatario) conscientemente firmó el documento.
- La firma es auténtica. La firma constituye un elemento convincente para el que recibe el documento, de que el signatario conscientemente lo firmó.
- La firma no se puede reutilizar. La firma se constituye en parte del documento, de modo que nadie puede desplazar la firma a otro documento.
- El documento firmado es inalterable. Después de que el documento es firmado, éste no puede ser alterado.
- La firma no puede ser rechazada. La firma y el documento son pruebas físicas (elementos tangibles). El signatario no puede posteriormente decir que no firmó el documento, pues se tiene como prueba el documento en el que se observa la firma.

En la realidad, ninguna de estas condiciones acerca de las firmas es completamente cierta. Las firmas pueden ser falsificadas, pueden ser tomadas de una pieza de papel y puestas en otro y los documentos pueden ser alterados después de ser firmados.

En computación, el esquema equivalente a la firma manuscrita (pero que garantiza mayor integridad y seguridad que aquellas) se conoce como **firma digital**, la cual se define como una porción de datos (bits) enviados con un mensaje codificado que especifica de manera única al emisor y verifica que el mensaje no haya sido alterado durante la transmisión. El concepto de una firma digital se muestra en la Figura 7.

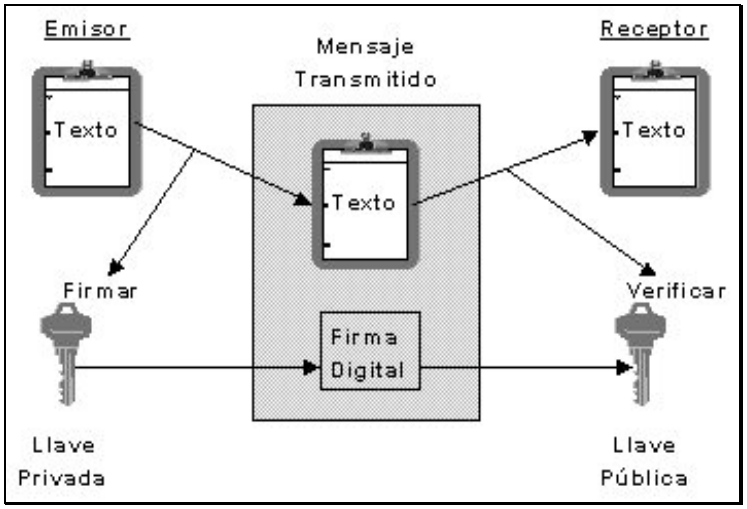


**Fig. 7. Firma digital [TIWANA 1999]**

Las firmas digitales permiten tanto la verificación de la integridad de un mensaje como la implantación del mecanismo de no-rechazo. Es decir, las firmas pueden ser utilizadas legalmente para resolver disputas entre las partes en una transacción, en caso de que una de ellas trate de negar que participó en la operación.

Existen varios algoritmos de firmas digitales, los cuales son todos de la categoría de llave pública. Algunas veces al proceso de firmar se le llama **encripción con llave pública**, mientras que al proceso de verificación se le conoce como **desencripción con llave pública**.

### 4.7.3 Control de acceso

Un mecanismo de control de acceso establece la interfaz entre un eventual usuario y un sistema, y se compone de tres etapas o procesos, por medio de los cuales un usuario debidamente autorizado obtiene los permisos que le han sido concedidos de previo para ejecutar acciones específicas sobre los diferentes objetos del sistema. Estas etapas son: identificación, autenticación y autorización[WEBE 88]. .

### 4.7.4 Proceso de identificación

Es el proceso por el cual el mecanismo de control de acceso le solicita al usuario algún tipo de información que sirva para determinar su identidad, ello con el objeto de conocer quién es el usuario que está intentando ingresar al sistema. Con esta información el mecanismo debe determinar si en sus registros existe algún usuario que esté habilitado y activo, que corresponda con la información suministrada. Dicha información se conoce con diferentes nombres como por ejemplo, código de usuario ("*username"*), número de cuenta ("*account"*) y nombre de conexión ("*login name"*). En la Figura 8 se aprecia el proceso de identificación.

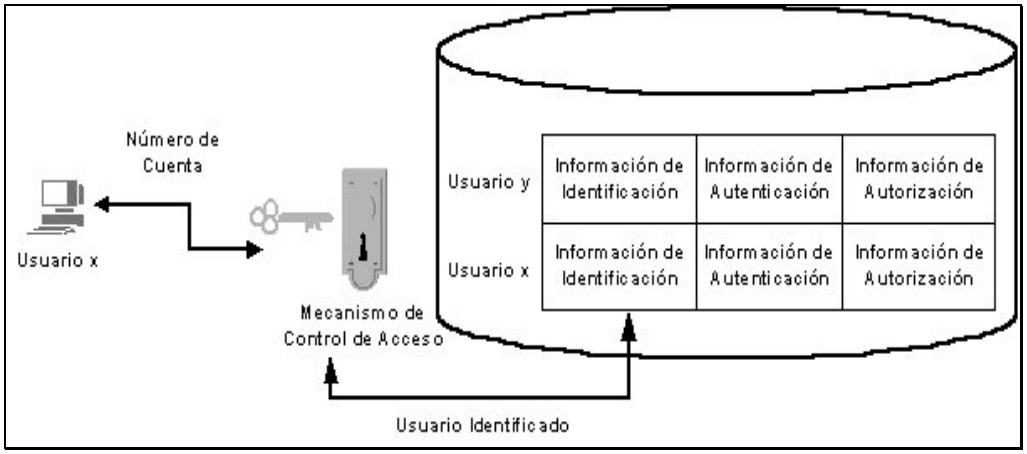


**Fig. 8. Proceso de identificación [WEBE 88]**

Una vez que el mecanismo de control de acceso ha captado la información de identificación se procede con la segunda etapa o proceso.

### 4.7.5 Proceso de autenticación

Puesto que en muchos casos la información que se utiliza para identificar un usuario puede ser pública, el mecanismo de control de acceso necesita autenticar a los usuarios. El proceso de autenticación consiste en demostrar al mecanismo de control de acceso que el usuario que se está identificando es legítimo, por cuanto la información de identificación no es suficiente para asegurar que el usuario que está intentando ingresar al sistema sea quien dice ser. El proceso de autenticación se puede apreciar en la Figura 9.

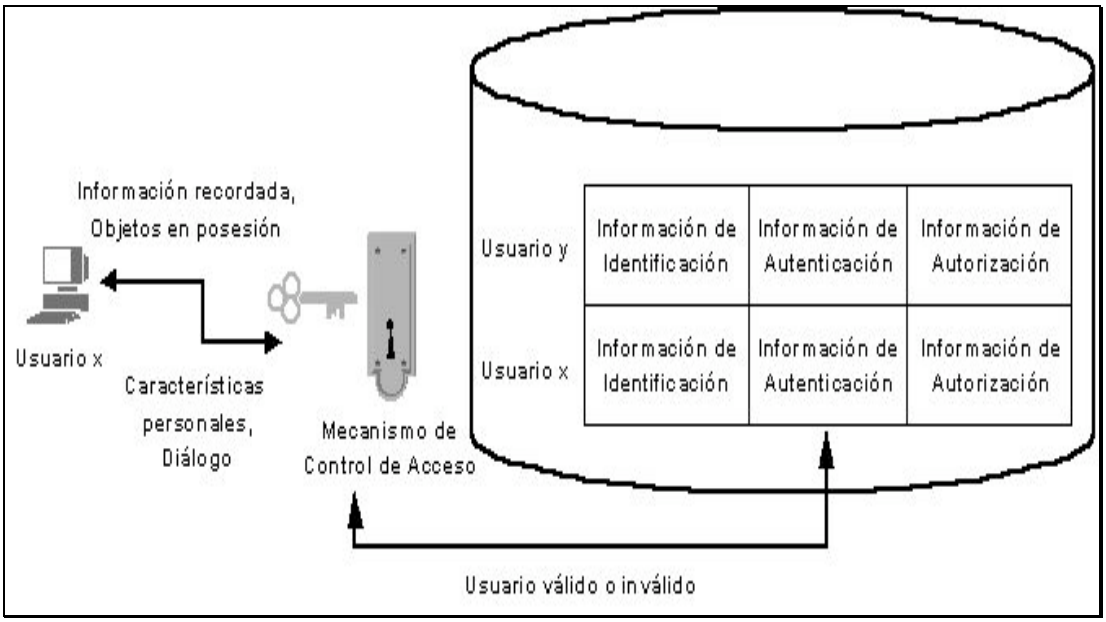


**Fig. 9. Proceso de autenticación [WEBE 88]**

Para ser autenticado, el usuario debe ingresar cierta información que le resulte privada o exclusiva, es decir, que no sea del dominio público del resto de posibles usuarios. En este sentido, existen diferentes técnicas de autenticación:

- **Por posesión**: el usuario debe presentar ante el mecanismo de control de acceso algún objeto, el que con el solo hecho de su presentación haga suponer que únicamente el

usuario correspondiente es quien lo posee. Ejemplo de ello son llaves, tarjetas con banda magnética, tarjetas con microchip, por citar los que se usan más comúnmente.

- **Por conocimiento**: en este caso, el usuario debe suministrar cierta información que él retiene en su mente, y que es de suponer que solamente el usuario involucrado en el proceso de ingreso la conoce. Ejemplos de este tipo de técnica son las contraseñas (palabras de paso o *passwords*) y los PIN (*Personal Identification Number*).
- **Características biométricas**: otro método para autenticar usuarios es valerse de ciertos atributos físicos que en teoría no son tan fáciles de imitar o suplantar. En este caso constituyen ejemplos utilizados, la impresión de las huellas dactilares, el contorno de la mano, el patrón de la voz, reconocimiento de la retina o el iris, y hasta la firma manuscrita.
- **Diálogo**: esta técnica consiste en que el mecanismo de control de acceso sostiene un diálogo con el usuario, en el cual el sistema le hace algunas preguntas y el usuario las debe responder correctamente, en el entendido de que el verdadero usuario suministró las respuestas correctas a la hora de registrarse inicialmente en el sistema. En estos casos, al usuario que está ingresando se le plantean solo algunas de las preguntas, las cuales deben ser respondidas adecuadamente; para ello se parte del supuesto de que solamente el verdadero usuario conoce todas las respuestas correctas.

A pesar de todo, por sí sola ninguna de estas técnicas es suficiente para asegurar totalmente la autenticidad de un eventual usuario, razón por lo cual se recomienda que para aumentar la efectividad del proceso se combinen una o varias de ellas.

En caso de que la combinación (información de identificación/información de autenticación) suministrada no corresponda con la de alguno de los usuarios registrados en el mecanismo de control de acceso, éste produce un mensaje advirtiéndole al usuario que el intento de ingresar al sistema fue fallido, y que trate de nuevo. En algunas implantaciones de mecanismos de control de acceso, luego de un número preestablecido de intentos fallidos se pueden generar diversas acciones, tales como el reporte en una bitácora acerca de la situación fallida, o bien, desactivando por un cierto tiempo la computadora desde donde se estuvieron haciendo los intentos de ingreso. Esto último corresponde a una medida extrema, la cual posiblemente puede obedecer a que existieron sospechas en cuanto a que se estuviera intentando ganar acceso, por parte de una persona extraña, a la cuenta de un usuario, sin su consentimiento.

### 4.7.6 Proceso de autorización

En caso de que resulten satisfactorias las acciones de identificación y autenticación emprendidas por un usuario, éste será reconocido como válido por el mecanismo de control de acceso, y sólo le permitirá ejecutar aquellas acciones para las cuales fue previamente autorizado. Al conjunto de acciones o privilegios que un usuario tiene derecho sobre los diferentes objetos o recursos del sistema se le conoce con el nombre de perfil ("*profile"*) o rol. En la Figura 10 se muestra en qué consiste el proceso de autorización.

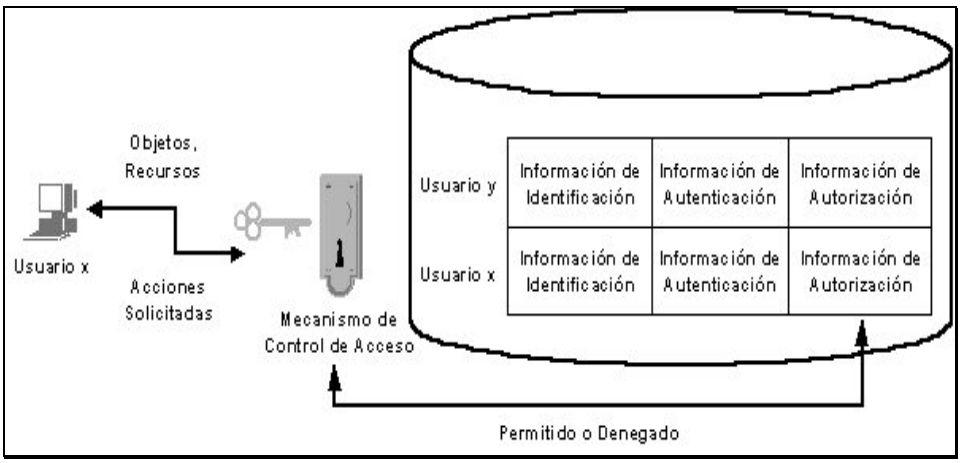


**Fig. 10. Proceso de autorización [WEBE 88]**

En resumen, no basta el solo hecho de ingresar satisfactoriamente a un sistema, pues si no se cuenta con los permisos o privilegios suficientes es poco lo que un intruso puede hacer con los objetos definidos dentro del mismo. De hecho, antes de ejecutarse cada una de las acciones que emprenda un usuario auténtico de un sistema, se debe validar contra su correspondiente perfil si cuenta con los derechos suficientes para poderla llevar a cabo. Si los permisos establecidos no lo permiten, el mecanismo de control de acceso debe denegar la realización de la acción solicitada.

### 4.7.7 Certificados digitales

Una razón especial por la que la criptografía es la clave para salvaguardar la información en Internet es su versatilidad. Más allá de garantizar la privacidad y la confidencialidad, la criptografía también puede emplearse para la autenticación, la cual forma la base del control de acceso, los permisos, autorizaciones y el mecanismo de no-rechazo. Y una de las aplicaciones esenciales de la criptografía en el proceso de autenticación son los **certificados digitales**. Un certificado proporciona una manera práctica de utilizar la encripción. Son como huellas digitales virtuales que "dan fe" de la identidad de una persona u organización. El certificado por sí mismo es un conjunto de información a la cual se adjunta una firma digital. La firma es colocada por una Autoridad de Certificación ("Certification Authority" – CA) que es una empresa que goza de la confianza de la comunidad de usuarios certificados. Como mínimo, un certificado digital contiene la siguiente información que puede ser verificada por cualquier entidad:

- El nombre del poseedor del certificado y alguna otra información de identificación

- Una llave pública que puede usarse para verificar la firma digital de un emisor de mensajes
- El nombre del emisor del certificado o CA
- El período de validez del certificado

Alguien que envíe un mensaje electrónico adjunta su certificado para firmar y encriptar dicho mensaje. El receptor de éste primero emplea su propio certificado para verificar que la llave pública del emisor es auténtica, y entonces aplica esta llave para descifrar el mensaje. Además de proporcionar autenticación, los certificados digitales hacen del control de acceso un mecanismo más seguro y fácil de administrar que las palabras de paso ("passwords"), debido a que no se requiere sustituir claves olvidadas o estar recordando a los usuarios que las cambien continuamente. Por último, los certificados son fáciles de conseguir y utilizar, además de ser baratos. Típicamente un certificado puede costar unos $10.

# 5. Seguridad en redes de computadoras: arquitecturas y protocolos de comunicación

¿Qué significa tener *seguridad*? La respuesta a esta pregunta no es sencilla y comprende estimar los beneficios que se esperan obtener producto de la protección y de los costos asociados a ésta. Una "seguridad adecuada" varía de empresa a empresa, y como el objetivo es proteger el flujo y utilización de la información en una organización, el problema se circunscribe al concepto general de **protección de la información**. Desde la introducción comercial de las redes de computadoras en la década del 80, la seguridad ha sido un tema de constante y creciente discusión. Inicialmente, la discusión sobre la seguridad en sistemas de redes computacionales estuvo circunscrita al área de procesamiento de datos. En 1983, con la proyección de la película "War Games" ("Juegos de Guerra"), el tema comenzó a recibir atención mundial.

Tres tendencias principales han contribuido a incrementar los problemas alrededor de la seguridad en las redes: las demandas por conectividad, el fácil acceso a los recursos de las redes y la diseminación (y abaratamiento) del uso de las microcomputadoras. La implantación de sistemas altamente conectivos frustra muchas veces los métodos de seguridad y control existentes. Uno de los objetivos primarios de una red de computadoras es proporcionar un acceso fácil y conveniente a los sistemas informáticos dentro de una empresa, y son estas dos características las que a menudo presentan conflictos con los requerimientos de seguridad.

La protección del procesamiento de información es necesaria debido a que ésta puede ser comprometida por ignorancia, accidente o malicia. El sentido de la seguridad es entonces establecer con certeza que la información no pueda ser obtenida, eliminada o modificada por personal no autorizado. Para lograr la seguridad en una red de computadoras deben existir mecanismos como procedimientos operativos y administrativos, hardware y software, diseñados para detectar y prevenir amenazas de tipo pasivo o activo sobre cualquier componente de un sistema de información. Según [JACKSON 1991], el 75% de las amenazas a la seguridad de la información provienen del personal de las propias empresas, el 20% es de naturaleza física y solamente el 5% tiene su origen en circunstancias externas a la organización. Hoy en día, los mayores costos en que incurren las empresas cada año son el resultado directo de errores humanos, accidentes y omisiones.

El moderno concepto de seguridad de la información incluye cuatro objetivos básicos [FORD 1994]:

- **Confidencialidad**: Asegurar que la información no es revelada por personas no autorizadas
- **Integridad**: Asegurar la consistencia de los datos, previniendo la creación, alteración o destrucción no autorizada

- **Disponibilidad**: Asegurar que los usuarios legítimos obtengan el acceso deseado a la información
- **Uso legítimo**: Asegurar que los recursos para el procesamiento de la información no sean utilizados por personal no autorizado o en formas no autorizadas

## 5.1 Servicios de seguridad en las comunicaciones

En el contexto de las comunicaciones, las principales medidas de seguridad se conocen como servicios de seguridad. Existen cinco de estos servicios:

- **Autenticación**. Garantiza la identidad de alguna entidad. Es el servicio más importante porque los demás dependen en alguna medida de éste. Permite enfrentar los ataques por enmascaramiento
- **Control de Acceso**. Protección contra manipulación y uso no autorizado de los recursos de información. Este servicio representa un medio para forzar la autorización y contribuye a lograr los objetivos de seguridad de confidencialidad, integridad, disponibilidad y uso legítimo.
- **Confidencialidad**. Prevención contra la revelación o exposición no autorizadas. Se subdivide en Servicio de Confidencialidad de Datos (orientado al contenido) y Servicio de Confidencialidad del Tráfico de Información (orientado al flujo de datos).
- **Integridad de los datos**. Prevención contra cambios o eliminaciones de información no autorizadas. La integridad puede protegerse en el ámbito de datos completos, parte de éstos o de aquellos transmitidos por algún canal de comunicación.
- **No-desconocimiento o rechazo**. Permite establecer con certeza la participación de las entidades en un proceso de comunicación de datos, cuando alguna de éstas niegue con posterioridad y en forma falsa que participó en dicho proceso. Es el único servicio que trata de proteger contra usuarios autorizados más que contra entidades desconocidas. El objetivo de este servicio no es únicamente evitar que los participantes intenten engañarse mutuamente, sino también el de reconocer que los sistemas no son perfectos y que pueden ocurrir circunstancias en que dos partes tengan puntos de vista diferentes de lo que realmente sucedió en una comunicación.

## 5.2 Políticas de diseño de seguridad en redes de computadoras

Es importante disponer de una efectiva y bien concebida política de seguridad en una red de computadoras, que permita resguardar la inversión de una empresa en el activo de la información y los recursos relacionados. Por supuesto, una política de esta naturaleza es útil de implementar solo si el valor de la información a proteger excede los costos de las medidas a adoptar. La mayoría de las organizaciones tienen información sensible almacenada en sus redes de computadoras y tarde o temprano tienen que enfrentar el

aspecto de la seguridad. Estos datos deben estar protegidos contra actos de vandalismo de la misma forma que otros activos de la institución.

Sin embargo, cualquier política efectiva debe tener en consideración que los usuarios no deben ser impedidos de llevar a cabo sus tareas de manejo de información, porque de lo contrario buscarán la forma de sobrepasar los controles establecidos, volviendo improductiva la política misma. La política de seguridad ideal en una empresa es aquella cuya competencia no pertenece a un único departamento sino a la organización en general y además es aceptada por todo el personal, el cual está dispuesto a garantizarla en forma permanente.

En una red como Internet, la protección de la información transmitida es crítica, especialmente en ambientes de transacciones electrónicas donde la integridad y la confidencialidad de los datos debe mantenerse al máximo posible para garantizar la confianza en los procesos comerciales. Por este motivo, es muy importante que los participantes de la red (usuarios, clientes y proveedores de bienes y servicios) comprendan, acepten y promuevan el uso permanente de procedimientos y técnicas de seguridad de la información.

Definir una política de seguridad significa desarrollar planes y procedimientos que salvaguarden los recursos de la red contra pérdidas y daños. Una red es un conjunto de componentes interrelacionados, para cada uno de los cuales deben considerarse las necesidades y requerimientos particulares de seguridad. Un enfoque adecuado toma en cuenta los siguientes aspectos:

- ¿Cuáles recursos es necesario proteger?
- ¿Quiénes tendrán la responsabilidad de velar por la seguridad de estos recursos?
- ¿Cuáles son las amenazas más probables de enfrentar?
- ¿Cuáles medidas de protección se pueden considerar para proteger los recursos de una manera oportuna y con una relación beneficio-costo favorable?

Un elemento importante de una política de seguridad en una red de computadoras es asegurar que todas las personas conocen su propia responsabilidad por mantener la protección de la información. Aunque es muy difícil anticipar todas las posibles amenazas que puedan ocurrir, la política definida debe garantizar que para cada tipo de problema que se presente, existe alguien que pueda enfrentarlo de una manera oportuna y responsable. La Figura 11 muestra, a manera de resumen, los niveles de seguridad que deben ser considerados en una política de seguridad.


**Fig. 11. Componentes de una política de seguridad en redes**

## 5.3 Protocolos de seguridad

Los protocolos de seguridad representan las especificaciones de comunicación seguras entre los diferentes componentes de la red para cumplir con los objetivos de identificación, reconocimiento y certificación de los usuarios y el mantenimiento de la integridad y confidencialidad de la información.

### 5.3.1 Protocolo S-HTTP

El Protocolo Seguro de Transferencia de HiperTexto o S-HTTP ("Secure HyperText Transfer Protocol") se ejecuta en un servidor Web e intenta hacer que el protocolo HTTP utilizado para la transferencia de información entre un cliente y un servidor Web realice su operación de una forma más segura y confidencial. El S-HTTP encripta ciertas páginas que fluyen entre el servidor y el cliente. Esta encripción se aplica únicamente sobre páginas que contienen información sensible como por ejemplo el número de la tarjeta de crédito, lo que significa que si alguien está "olfateando" ("sniffing") o escuchando de una forma indiscreta ("eavesdropping"), solo obtendrá datos sin un sentido claro.

Hay sin embargo una restricción con este protocolo. Para que pueda funcionar en el lado del cliente, éste debe poseer un programa navegador que soporte el protocolo. Actualmente, pocos son los programas de esta naturaleza que soportan el S-HTTP como por ejemplo, Internet Explorer, Netscape y SPRY Mosaic.

### 5.3.2 Protocolo SSL

El Protocolo Seguro de Nivel de Ranura o SSL ("Secure Sockets Layer") también se utiliza para transferir información de una manera más segura y confidencial. El SSL trabaja utilizando un puerto (o ranura) seguro para el intercambio de información entre un cliente y un servidor. El puerto por definición de un sistema servidor es el 80. El SSL, por su parte, usa el puerto lógico 443 que controla la forma en que se manejan las comunicaciones. Este protocolo no está restringido a las páginas Web siendo utilizado también por el protocolo de transferencia de archivos FTP.

Del lado del servidor, el SSL se ubica entre el programa navegador y el programa HTTP. Primero, el SSL intercambia información de verificación. Después, toda la información que fluye desde y hacia el puerto es encriptada, desencriptada y validada para garantizar que no haya sido alterada en el trayecto. El protocolo no se utiliza normalmente para transferir todas las páginas sino cuando se requiere enviar información sensible debido a la sobrecarga de procesamiento que involucran los procesos de verificación, encripción, desencripción y validación. Al igual que con el protocolo S-HTTP se necesita un programa navegador que sea compatible con el SSL.

Una variante del SSL es el protocolo para la Seguridad a Nivel de Transporte ("Transport Layer Security" – TLS) adoptado en 1995 por la Fuerza de Tarea de Ingeniería para Internet ("Internet Enginnering Task Force" – IETF). Este protocolo utiliza una función de llave segura HMAC en vez del algoritmo MD5 del SSL.

### 5.3.3 Protocolo de Transacciones Electrónicas Seguras ("Secure Electronic Transaction Protocol" – SET)

SET es un protocolo criptográfico diseñado para enviar números de tarjetas de crédito encriptados por Internet. A diferencia de otros protocolos aún se encuentra bajo desarrollo a cargo de empresas como Visa, Master Card, Microsoft, Netscape, IBM y GTE. Tiene tres componentes básicos: una "cartera" electrónica que reside en la computadora del cliente; un servidor que se ejecuta en el sitio Web del comerciante y el Servidor de Pago SET que se localiza en algún banco. Cuando un cliente realiza alguna compra, el número de su tarjeta de crédito es encriptado y enviado al comerciante. El software de éste firma digitalmente el mensaje de pago y lo reenvía al banco de procesamiento donde el servidor SET desencripta toda la información y aplica el cargo a la tarjeta de crédito.

### 5.3.4 Protocolo de Correo de Privacidad Mejorada ("Privacy Enhanced Mail" – PEM)

El PEM fue desarrollado a mediados de los años 80 por el Grupo de Investigación en Privacidad y Seguridad ("Privacy and Security Research Group") y proporciona varias características de seguridad a las aplicaciones de correo electrónico:

- **Confidencialidad**. Los mensajes solo son legibles para los receptores. La confidencialidad se aplica tanto a los mensajes en ruta como a los que están almacenados.
- **Autenticación**, para garantizar la identidad del emisor.
- **Integridad**. El mensaje recibido es exactamente el que se transmitió.
- **No-rechazo**. El emisor no puede alegar que no envión el mensaje.

Los mensajes PEM están diseñados para utilizar el protocolo SMTP como mecanismo de transporte y el algoritmo criptográfico de ciframiento simétrico DES en modo de Cifrado con Encadenamiento de Bloques ("Cipher Block Chaining" – CBC)[28].

### 5.3.5 Protocolo de Privacidad Adecuada ("Pretty Good Privacy" – PGP)

La especificación del PGP fue escrita por Phil Zimmerman para incorporar la encripción asimétrica o de llave pública y las firmas digitales a los mensajes y archivos de correo electrónico, garantizando la autenticación en los primeros y la privacidad de los segundos. Para cumplir con los propósitos anteriores implementa el algoritmo IDEA ("International Data Encryption Algorithm") en modo de ciframiento de bloques simétricos. EL PGP está disponible para una amplia variedad de plataformas incluyendo Microsoft Windows, DOS, UNIX, Macintosh y VMS.

### 5.3.6 Protocolo de Entubamiento Punto-a-Punto y las Redes Privadas Virtuales ("Virtual Private Networks" – VPN's)

El Protocolo de Entubamiento Punto-a-Punto ("Point-to-Point Tunneling Protocol" – PPTP) es una tecnología de red que permite a un usuario u organización usar Internet como una red privada virtual segura. Este protocolo se integra con los servidores de acceso remoto para llevar a cabo los siguientes procesos:

[28] Para una adecuada comprensión de los modos de encripción se recomienda la lectura de [DENNING 1983].

- Un usuario se conecta a Internet.
- Un programa de VPN en la computadora del usuario reconoce la dirección de la red destino especificada y negocia con el servidor en esta red una sesión encriptada.
- Los paquetes de información encriptada son convertidos a paquetes IP (del protocolo TCP/IP) para enviarlos por un *túnel* o *tubo* a través de la red.
- El servidor VPN negocia la sesión VPN, recibe los paquetes IP y los desencripta.
- La información desencriptada fluye normalmente a otros servidores o usuarios en la red destino.

La seguridad en una VPN requiere dos elementos de seguridad adicionales a los proporcionados normalmente por los mecanismos de seguridad básica en Internet:

- Encripción para asegurar la privacidad y la integridad de la información transmitida.
- Autenticación de dos factores ("Two-factor Authentication") que aporta la identificación y autenticación de usuarios remotos.

### 5.3.7 Servicios de Seguridad en Sistemas de Manejo de Mensajes ("Message Handling System"- MHS)

Los servicios de seguridad para MHS están diseñados para enfrentar distintas amenazas en ambientes de correo electrónico, intercambio electrónico de datos ("Electronic Data Interchange" - EDI), y mensajería de voz. Las categorías de amenazas a las que se opone son:

- **Enmascaramiento**. Suplantación de identidad de un usuario o proceso para obtener acceso no autorizado a funciones críticas de un MHS.
- **Secuenciación de mensajes**. Solicitud de repetición de mensajes.
- **Modificación o destrucción** de información.
- **Rechazo** de procesos o mensajes.
- **Filtración de información** que conduce a la pérdida de confidencialidad y del anonimato.

# 6. Ataques, amenazas y riesgos en Internet[29]

La información es un activo muy valioso... y también muy frágil, fácil de ser mal utilizada y cometer abusos con ella. Para su protección se crearon primero los derechos de autor, las marcas registradas, el secreto comercial y otras leyes similares. Con el ingreso a la era computacional, se definieron nuevos reglamentos para proteger también la propiedad y privacidad de la información. Se desarrollaron medidas de seguridad como las palabras de paso y técnicas como la criptografía para hacer la vida más difícil la labor de los criminales que deseaban adueñarse de la información. Hoy en día contamos con el ciberespacio, un lugar sin presencia física que contiene datos escritos, hablados y electrónicos, sin importar dónde existen o cómo son comunicados. Este nuevo reino ha traído cosas buenas y otras que no lo son tanto.

La seguridad de la información es muy importante para todos los usuarios de computadoras, aunque muchos no quieran reconocerlos, o les asuste hacerlo. Bill Clinton estableció en una forma muy clara, el impacto actual de la información en la vida de las personas y los países:

"Ciertas infraestructuras son tan esenciales que su incapacidad o destrucción podrían tener un impacto debilitante en la defensa o la seguridad económica del país. Esta infraestructura crítica incluye las telecomunicaciones, los sistemas de energía eléctrica, el acarreo y almacenamiento del petróleo y la gasolina, la banca y las finanzas, el transporte, los sistemas de suministro de agua, los servicios de emergencia y la continuidad del gobierno. Las amenazas a estas infraestructuras críticas caen en dos categorías: amenazas físicas a la propiedad tangible y las llamadas ciberamenazas basadas en ataques electrónicos, de radio frecuencia y computacionales, sobre la información o los componentes de comunicación que controlan estas infraestructuras".

Aparte de su peligro potencial a la seguridad de una nación, el cibercrimen amenaza a los individuos y a las organizaciones. Lamentablemente, en la mayoría de los casos se realizan solo esfuerzos a medias, que es como cerrar la puerta de la casa con llave pero dejando la ventana abierta para que ingresen los ladrones. Los técnicos en computadoras le indican a los usuarios que creen palabras de paso difíciles de averiguar pero los *hackers* maliciosos continuamente "escuchan" en las redes computacionales empleando poderosas herramientas para deducir estas claves. Y lo peor de todo es que la gran mayoría de personas no están dispuestas a perder el tiempo protegiendo su información, a la espera de nunca ser víctima de los cibercriminales. Es cierto que no existe una fórmula totalmente efectiva para prevenir el crimen, pero no es razón suficiente para no proteger la información en alguna forma si no somos capaces de protegerla completamente.

[29] En [PARKER 1998] el lector encontrará un excelente material acerca del crimen cibernético, mientras que en [ANONYMOUS 1998] se explican detalladamente las principales formas de ataque a la seguridad, incluyendo los virus informáticos.

Los propietarios de la información pueden de manera razonable adoptar medidas reconocidas para el resguardo de los datos, y prácticas para adquirir el nivel adecuado de protección. Y si a final de cuentas no se toma ninguna medida de seguridad, que esta solución provenga de una decisión razonada (como un análisis de riesgo e impacto) y no de la simple negligencia.

La cantidad de medidas que se usen para resguardar la información parece no tener una incidencia muy significativa en si los crímenes son exitosos o no. La clave para una protección efectiva es utilizar los resguardos más adecuados para la naturaleza de la amenaza que se desea enfrentar, y crear las asociaciones entre personas y sistemas en donde la confianza se encuentre balanceada con los mecanismos de defensa impuestos.

La mayoría de las empresas tienen esquemas de protección muy deficientes que facilitan la intrusión de individuos no autorizados a sus sistemas computacionales. ¿Cuántas compañías que poseen "paredes de fuego" para filtrar los paquetes de datos y garantizar que solo ciertos usuarios o procesos acreditados tengan acceso a la información, no tienen funcionarios con computadoras en sus escritorios, conectadas por un lado a la red interna y por el otro a la línea telefónica? En este caso, la "pared de fuego" resultaría en un mecanismo inútil si algún *hacker* malicioso o un *cracker* pueden ingresar a una de estas computadoras marcando el número y la extensión de teléfono de un funcionario y de aquí obtener acceso a la red, sobrepasando las medidas de protección impuestas.

El factor humano es crítico en cualquier organización y no debe ser subestimado. Gengis Kahn logró atravesar la Gran Muralla China utilizando la opción más simple. En vista de que la muralla era muy sólida, profunda y larga, inteligentemente sobornó al guarda que cuidaba la puerta. Por más fuertes que sean los controles técnicos de seguridad implementados, las personas representan los eslabones más débiles de una cadena de la protección.

## 6.1 Identificación de riesgos y componentes por proteger

Toda empresa que se encuentre interesada en implementar adecuados mecanismos de control y protección de la información debería comenzar por identificar los componentes que necesitan ser protegidos. Algunos son obvios, como bases de datos con información corporativa, documentos confidenciales, planes (estratégicos, de contingencia, etc.). Otros componentes son continuamente olvidados, como las personas que actualmente utilizan los sistemas de información. Debe establecerse una lista formal de todos los recursos dentro de la organización que puedan verse potencialmente amenazados o afectados por acciones maliciosas, por ejemplo:

- Software: programas fuentes y ejecutables, sistemas operativos y programas de comunicaciones.
- Datos: bases de datos, respaldos bitácoras de auditoría, etc.

- Personas: usuarios, personal de sistemas de información, clientes, proveedores y administradores.
- Documentación: de programas, manuales técnicos de los equipos, procedimientos administrativos y otros.

Una vez confeccionada la lista debe procederse a realizar un análisis y evaluación de riesgos para los diferentes elementos de la lista, ya sea en forma individual o por grupos funcionales.

El análisis de riesgo brinda algunos beneficios a escala organizacional como [UCI 1997] y [Hernández 1999]:

- Permite mejorar el conocimiento sobre la empresa
- Ayuda a identificar activos y vulnerabilidades potenciales o actuales
- Mejora la base para la toma de decisiones y
- Contribuye a justificar los gastos de seguridad en materia informática

El análisis de riesgo puede hacer uso de métodos cuantitativos o cualitativos, y en general, comprende las siguientes etapas:

- Identificación de activos
- Determinación de vulnerabilidades
- Estimación de la probabilidad de ocurrencia de amenazas
- Cálculo de la pérdida estimada si las amenazas se materializan
- Análisis de contramedidas posibles de adoptar
- Cuantificación del costo de implantación de las medidas de protección (o en su defecto, el ahorro esperado por concepto de implantación de las soluciones de protección)

**Recomendación**: Algunos modelos formales para el análisis de riesgo informático que pueden ser consultados son:

- Metodología para el Análisis y la Administración del Riesgo (CRAMM). Esta metodología es un estándar en el Reino Unido para identificar las medidas de seguridad adecuadas que protejan los sistemas de información encargados de administrar datos sensibles pero no clasificados
- Escenarios en Serie de Amenazas. Los escenarios son una herramienta de administración que identifican amenazas y sus correspondientes contramedidas.
- Metodología para la Valoración del Riesgo de Ocho Etapas. Esta metodología identifica y categoriza las amenazas y vulnerabilidades, y define medidas para enfrentarlas.

## 6.2 Ataques remotos

"Un ataque remoto se puede definir como cualquier ataque iniciado contra una máquina remota. Una máquina remota es cualquier máquina que puede ser contactada por Internet u otra red". [ANONYMOUS 1998]

Un *hacker* malicioso o un *cracker* intenta lograr el acceso a un sistema remoto averiguando cómo se comporta la red, sus posibles puntos débiles, quiénes están conectados a ésta y dónde consiguen el acceso a ella. A pesar de lo que pudiera pensarse, esta información es fácil y rápida de obtener, utilizando únicamente programas utilitarios estándares de red (por ejemplo, la instrucción SLIST de Novell Netware indica los servidores actualmente accesibles en la red).
El intruso inicia su proceso emitiendo una consulta a un servidor, el cual reúne la información disponible. Esta información no es completa y presenta solo posibilidades (posibilidad de que la dirección XXX corresponda a un servidor, posibilidad de que la versión de UNIX que está ejecutando un determinado usuario sea la ZZZ, etc.). También, la mayoría de los sistemas operativos cuentan con instrucciones que permiten al usuario conocer el nombre, versión y fabricante de éstos.

Algunos servicios ofrecidos en Internet proporcionan también gran cantidad de información útil para un ataque, como por ejemplo, el servicio WHOIS del Centro para la Información de Redes ("Network Information Center", en internic.net) que contiene el nombre de los servidores en todos los dominios disponibles en los Estados Unidos excepto los militares, información técnica de cada dominio y sus respectivas direcciones. La existencia de sitios que brindan estos servicios presenta una perspectiva muy interesante. Por un lado, los cibercriminales (o quienes están en proceso de serlo) pueden aprovechar la información disponible para ganar conocimiento de cómo violentar la seguridad de los sistemas computacionales. Por el otro, las organizaciones pueden sacar provecho a la misma para mejorar sus sistemas de seguridad internos.

Hasta aquí, un intruso pudo haber obtenido datos relacionados con el hardware, el sistema operativo, posibles condiciones de seguridad exigidas por la red o las aplicaciones que están en ejecución y la topología de la red. Sin embargo, en manos de un buen conocedor (y los *hackers* y *crackers* lo son) estos datos proporcionan al intruso información invaluable sobre sus objetivos, que utilizarán luego para la creación de programas que exploten estas debilidades como virus, Caballos de Troya y otros similares.

Con intrusos intentando penetrar sus sistemas computacionales, las empresas pueden acudir a diferentes fuentes para identificar y corregir sus vulnerabilidades:

- *Software de escaneo*. Generalmente utilizados como herramientas de auditoría, programas como ISS y SATAN, ayudan a identificar y documentar vulnerabilidades en una red.
- *Sitios Web de crackers*. Estos sitios almacenan gran cantidad de datos sobre deficiencias detectadas en equipos, programas, sistemas operativos y utilitarios.

- *Consultorías*
- *Fuentes de seguridad legítimas*. Son organizaciones, muchas de ellas sin fines de lucro, que mantienen bases de datos extensas sobre temas relacionados con la seguridad en Internet. Algunas de estas instituciones son el Equipo de Repuesta para Emergencias Computacionales ("Computer Emergency Response Team" – CERT), el Banco de Recursos para la Seguridad Computacional ("Computer Security Resource Clearinghouse" – CSRC) y el Centro de Información de Redes del Departamento de Defensa de los Estados Unidos.

## 6.3 Niveles de ataque

Los ataques a un sistema computacional pueden ocurrir a partir del momento en que éste inicia una sesión en Internet. Como cada vez es más frecuente que los servidores de red permanezcan encendidos y conectados a la red las veinticuatro horas, es de esperar los ataques en forma permanente.

Un gran porcentaje de los ataques ocurre en períodos de baja utilización de las redes, especialmente en las noches y las madrugadas (tiempo relativo al sistema objeto del ataque), por varias razones importantes:

1. Disponibilidad de tiempo. Los cibercriminales, en su mayoría, trabajan, asisten a la universidad, o utilizan el resto del día en otras actividades.
2. Velocidad. Cada día que pasa, aumenta el tráfico en la red, por lo que es mejor trabajar en hora donde el transporte de información sea más rápido. Esta situación depende por supuesto, de la ubicación geográfica de las redes.
3. Ocultamiento. Entre más usuarios se encuentren conectados en una red en un momento específico, es mayor la posibilidad de que alguno detecte un comportamiento anormal de la misma, producto de una intrusión. Las computadoras ideales para asegurar el ocultamiento son aquellas que están encendidas pero no muestran ninguna actividad (probablemente porque el usuario no se encuentra cerca de ella). Estos equipos sirven de puente o distractor para un cibercriminal cuya localización física puede ser muy lejana.

**Recomendaciones:**

- Si no va a utilizar una computadora, no deje abierta la sesión. Mejor aún, apague la máquina.
- Utilice programas utilitarios para monitorear la actividad en la red, los servidores o las estaciones de trabajo.
- Revise con especial cuidado las bitácoras de registro de actividad en la porción correspondiente a las horas de la noche y la madrugada.

Hace algunos años, los ataques provenían principalmente de las universidades, puesto que de ahí venía el acceso a Internet. Muchos de los *crackers* eran jóvenes estudiantes que aprovechaban esta disponibilidad para ganar acceso a otras redes. Hoy en día, el panorama es totalmente diferente. Los cibercriminales pueden ingresar ilegalmente a un sistema de cómputo desde la casa, la oficina o un vehículo en movimiento. Un *cracker* típico presenta generalmente las siguientes características:

- Codifica en C, C++ o Perl
- Tiene amplios conocimientos del TCP/IP
- Utiliza Internet más de 50 horas por mes (esta característica la comparten también los adictos al Web)
- Tiene conocimientos técnicos avanzados de varios sistemas operativos
- Tiene o ha tenido un trabajo en que se utilizan las computadoras
- Colecciona hardware y software en diferentes versiones

Los objetivos más comunes de los cibercriminales incluyen:

- Pequeñas redes debido a que, por lo general, los propietarios de estas tienen poca o ninguna experiencia en Internet, los administradores de la red tiene poco conocimiento del TCP/IP y el hardware o el software (o ambos) tienen cierto grado de antigüedad.
- Universidades y empresas con una buena cantidad de poder computacional.
- Oficinas gubernamentales donde se maneja una buena cantidad de información personal y existe poca consciencia del concepto de seguridad informática.

En una red de computadoras se pueden identificar seis niveles de sensibilidad a los ataques, tal como se puede apreciar en la Figura 12.

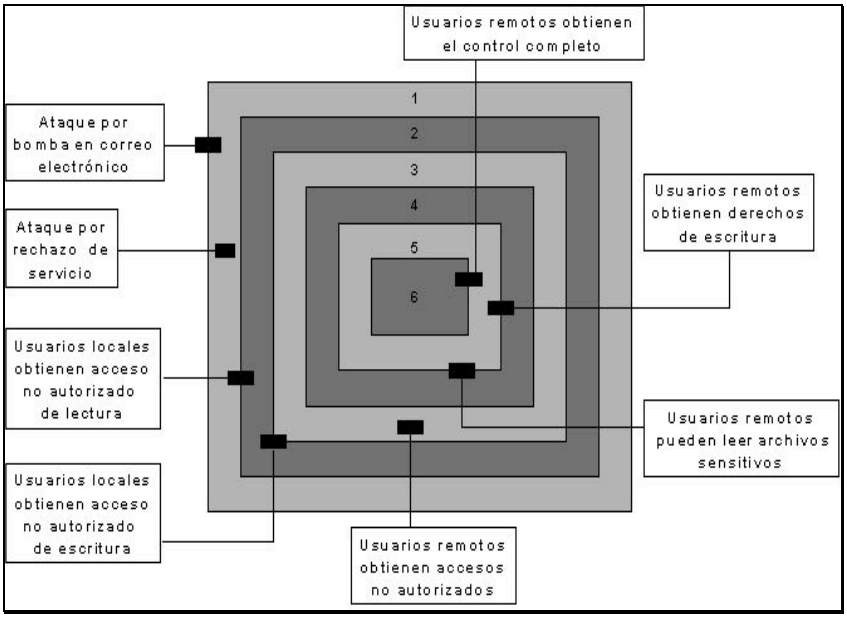


**Fig. 12. Niveles de sensibilidad en una red de computadoras [ANONYMOUS 1998]**

Los ataques de nivel uno son de poca importancia, su propósito es causar molestias e incluyen el rechazo para ejecutar un servicio y el "correo bomba".

Los niveles dos y tres involucran a los usuarios locales de una red los cuales logran obtener derechos de lectura y escritura a los archivos o directorios. Un *cracker* en estos dos niveles puede ser un usuario principiante que desea por curiosidad lograr violentar el sistema de seguridad, o bien un usuario con un plan de ataque detallado y que conoce bien la configuración del sistema.

En el nivel cuatro, un usuario remoto logra tener acceso al sistema para verificar la existencia de archivos o en el mejor de los casos, leerlos.

Los niveles cinco y seis, son los más críticos porque los usuarios remotos adquieren privilegios completos sobre los archivos y directorios. Un ataque en estos niveles es poco probable que ocurra si se han tomado las previsiones del caso para asegurar los niveles dos, tres y cuatro.

Existen programas comerciales y mejoras ("parches") de los sistemas operativos que actúan en los diferentes niveles de sensibilidad para prevenir los ataques mencionados con anterioridad.

### 6.3.1 Ataques por "engaño" ("spoofing")

El "engaño" es una técnica sofisticada donde un dispositivo autentica a otro que falsifica el envío de mensajes desde una fuente autorizada. Para entender más claramente este concepto es necesario comprender otros dos: **Confianza** ("Trust") y **Autenticación**. La confianza es la relación entre dos máquinas que están autorizadas para conectarse una con otra. La autenticación es el proceso que ambos equipos utilizan para identificarse mutuamente. Ambos términos están inversamente relacionados: entre más confianza existe, menores serán los requerimientos de autenticación necesarios.

En términos generales, el proceso de engaño presenta los siguientes pasos:

- El *cracker* conoce que entre dos máquinas X e Y existe una relación de confianza.
- El *cracker* intenta violentar la seguridad de X. Para lograrlo debe presentarse convincentemente como Y.
- Para suplantar a Y, el *cracker* debe falsificar la dirección de origen.

Para que el ataque anterior tenga éxito se requiere:

- El cracker debe identificar sus objetivos
- Debe "anestesiar" al sistema que intenta suplantar
- Debe falsificar la dirección de la máquina suplantada

- Debe conectarse al otro equipo, "enmascarándose" como si fuera el sistema "anestesiado"
- Debe averiguar en forma precisa la secuencia correcta de números de paquete que el otro equipo le solicita

Las configuraciones y servicios más vulnerables a este tipo de ataque son aquellos dispositivos que ejecuten el servicio Sun RPC en UNIX, cualquier servicio de red que utilice autenticación de direcciones IP, el sistema Windows X del MIT (Massachussets Institute of Technology) y el servicio "r" de UNIX.

La forma de impedir este tipo de ataques en una red es mediante el uso de programas utilitarios o de configuración del sistema operativo del equipo de enrutamiento, que rechacen aquellos paquetes que reclaman originarse en una dirección local.

### 6.3.2 Ataques basados en Telnet

Telnet es un servicio de terminal virtual diseñado para permitir a un usuario ingresar a un equipo remoto y ejecutar instrucciones en éste. Este servicio imita una conexión de terminal ASCII entre dos sistemas computacionales separados geográficamente. Una terminal virtual es equivalente a una conexión serial entre dos equipos.

Los problemas de seguridad asociados a Telnet son muchos y muy variados, debido principalmente a errores de programación. El principal problema es que si un *cracker* logra determinar un usuario válido (junto a su palabra clave) puede obtener acceso al archivo de autenticación FTPPASS que contiene los nombres de usuario y palabras de paso almacenados. Aunque las claves están encriptadas, el algoritmo criptográfico utilizado es fácil de vulnerar[30].

Los dos métodos más efectivos para enfrentar este tipo de ataques son la deshabilitación del acceso FTP para las sesiones Telnet, y la sustitución del Telnet tradicional con la versión segura conocida como SSH ("Secure Shell") que permite ejecutar operaciones de transferencia de archivos y sesiones de terminal virtual criptográficamente protegidas.

### 6.3.3 Dispositivos destructores

Los dispositivos destructores son programas que cumplen uno o los dos siguientes objetivos: hostigamiento ("harassment") y destrucción de datos. La mayoría de esta clase de dispositivos no presentan riesgos de seguridad significativos sino molestias. Sin embargo, en ocasiones pueden amenazar la capacidad de funcionamiento de una red. Y aunque los ataques no comprometen la seguridad del sistema sí provoca operaciones

[30] Un programa en BASIC para desencriptar las palabras de paso se puede encontrar en la dirección http://www.musa.it/gorgo/txt/NCSATelnetHack.txt

frecuentemente interrumpidas. Existen cuatro tipos principales de dispositivos destructores:

- **Bombas de correo electrónico.** Una bomba es un conjunto de mensajes (por lo general miles de ellos) que se envían a una o más cuentas de correo electrónico. El objetivo del ataque es llenar las cuentas con basura. El tamaño promedio de una bomba es de 2 MB y el ataque proviene en muchas ocasiones de foros de discusión en la red Usenet. Los mecanismos de defensa para estos ataques son las herramientas que permiten el filtrado y selección de mensajes como por ejemplo Stalker y Eudora Mail Server para Macintosh y Advanced E-mail Protector y SpamKiller para Windows. A este tipo de mensajes se le conoce también con el nombre de "Correo Negro" o "Blackmail".
- **Enlace a listas de correos[31].** Este tipo de ataque se basa en el mecanismo de envío de las bombas de correo. El propósito del enlace a listas de correo es suscribir a los usuarios en docenas de estas listas de correo, nuevamente con el objetivo de llenar las cuentas de aquellos con basura. La única cura efectiva para este tipo de ataques es desinscribirse de las listas.
- **Herramientas de rechazo de servicios**. El rechazo de servicios puede incapacitar temporalmente a una red completa y especialmente a los servidores que utilizan el TCP/IP. El primer ataque de esta categoría fue reportado en Noviembre de 1988 y se le conoció con el nombre del "gusano Morris" ("Morris Worm"). Afectó a más de 5000 computadoras por espacio de varias horas. Algunos de los programas que provocan el rechazo de servicios no tienen aún cura. Sin embargo para la gran mayoría de ellos existen otros programas que resuelven el problema.
- **Virus**. Este tema será tratado más adelante.

### 6.3.4 Quebrantadores de palabras claves ("Password Crackers")

Un quebrantador de palabras claves es un programa que engaña al sistema de seguridad revelando las palabras secretas ("passwords") que han sido previamente encriptadas. Esto no significa necesariamente que el quebrantador logra desencriptar las claves. En la mayoría de los casos no lo hace.

Muchos quebrantadores utilizan un enfoque de ataque con métodos de fuerza bruta, es decir, prueban palabra tras palabra a grandes velocidades. Este esquema casi siempre da resultado debido a que las personas no están acostumbradas a crear palabras claves fuertes[32]. Otros quebrantadores están basados en herramientas que emplean el mismo

[31] Una lista de correo distribuye mensajes de correo electrónico recolectados de varias fuentes. Estos mensajes, por lo general, se concentran en temas específicos de interés para los usuarios y son recopilados por servidores de correo, en este caso llamados servidores de lista, sobre una base diaria, semanal o mensual. Luego los servidores envían esta información a los usuarios suscritos a las listas.
[32] El término "fuerte" es sinónimo de difícil de averiguar.

algoritmo de encripción de claves. Estas herramientas hacen análisis comparativos entre los resultados de las pruebas y las palabras secretas que necesitan averiguar.

El único método efectivo para enfrentar este tipo de ataque es utilizar software que genere claves utilizando algoritmos fuertes conocidos.

### 6.3.5 Virus[33]

Los virus son los dispositivos destructores más peligrosos que existen, especialmente por su poder para destruir información, reproducirse y transformarse ("mutar") para evitar las medidas de protección como los programas antivirus (también conocidos como escáneres).

Un virus es un programa que se agrega a sí mismo a otros archivos en el sistema computacional objetivo. Durante el proceso de adición, el código del virus se entremezcla con el del programa "víctima". A este procedimiento se le conoce como *infección*, y al programa infectado, el *portador*. A partir de este momento el programa original podrá infectar a (*reproducirse en*) otros programas con solo ser ejecutado una vez, causando rápidamente una epidemia.

Cientos de virus nuevos aparecen cada año. Para crearlos se utilizan lenguajes de programación como C, Basic, Pascal y Ensamblador (el más común de todos), o herramientas productoras de virus ("Virus Kits") disponibles algunos de ellos en Internet (como por ejemplo, Virus Creation Laboratories, Virus Factory, Virus Creation Set, y otros más). Estas últimas herramientas son de fácil uso, permitiendo que casi cualquier persona pueda crear un virus, en contraste con años anteriores donde se requería un conocimiento avanzado de programación, sistemas operativos y equipo computacional.

Existen tres grandes categorías de virus:

- Virus que atacan el sector de arranque maestro ("Master Boot Sector"). Los discos fijos o duros requieren de datos almacenados en el registro de arranque maestro ("Master Boot Record" – MBR) para ejecutar los procedimientos básicos de inicialización y arranque. Por lo tanto, los virus de este tipo son activados desde el comienzo de la operación de un equipo, sobrepasando cualquier medida de defensa ejecutada con posterioridad.
- Virus que atacan los archivos ("File Viruses"). Estos virus infectan solo cierto tipo de programas (los llamados ejecutables) con extensiones .COM y .EXE. Pero también son capaces de infectar archivos con otras extensiones como .OVL ("overlays"), .SYS y .DRV (archivos para el manejo de dispositivos).
- Virus que atacan los archivos de datos o Macro Virus.

[33] Aunque la literatura sobre este tema es muy amplia, se recomienda la consulta de [DENNING 1990] y [COHEN 1994] para una fácil comprensión del diseño y la arquitectura de un virus.

Los virus también se pueden dividir de acuerdo con la forma en que operan o las técnicas de programación que se emplearon en su creación, en:

- **Virus basados en el ocultamiento** ("Stealth Viruses"). Utilizan muchas técnicas para ocultar el hecho de que un archivo ha sido infectado. Cuando el virus produce una infección sobre un archivo, registra la información básica de éste para posteriormente engañar al sistema operativo.

- **Virus polimórficos** ("Polymorphic Viruses"). Este tipo de virus es bastante reciente y su diseño mucho más complejo que el de los virus de otras categorías. Un virus polimórfico puede cambiar ("*mutar*") haciendo más difícil su identificación. Algunos de estos virus usan técnicas avanzadas de encripción. En una mutación, el virus puede cambiar su tamaño y composición, volviéndose "invisible" para una buena parte de los programas antivirus que buscan patrones estáticos (fecha, tamaño, etc.) en su proceso de detección. Para enfrentar a estos virus, los escáneres son creados con la capacidad de reconocer patrones de encripción.

La gran mayoría de virus atacan la plataforma Microsoft (DOS, Windows y NT), pero también existen virus para otros sistemas operativos como UNIX y MacOS.

Algunas variantes de los virus reciben otros nombres. Las más conocidas son:

- **Gusanos** ("Worms"). Son programas autocontenidos (no se adicionan a otros programas) que pueden propagarse de una máquina a otra. A diferencia de los virus tradicionales, un gusano no requiere modificar un archivo para lograr su propagación.
- **Caballos de Troya** o Troyanos ("Trojan Horses"). Un troyano puede ser descrito como una porción de código no autorizado dentro de un programa legítimo, que realiza funciones no conocidas por el usuario (ocultas y no deseadas por éste). Algunos virus pueden caer en esta categoría. Los troyanos pueden ejecutar funciones útiles o interesantes, y siempre efectúan acciones inesperadas como robar palabras claves o copiar archivos sin el conocimiento del usuario. Al igual que que con los virus, la mayoría de los escáneres actuales están diseñados para prevenir, detectar y eliminar troyanos.
- **Bromas** ("Hoaxes"). Algunas veces se reciben mensajes por correo electrónico alertando a los usuarios sobre la aparición de un nuevo virus, los cuales no resultan ser verídicos. A este tipo de correo se le conoce como broma. El siguiente es un ejemplo de una broma reciente:

**Nombre de la broma**: Perrin.exe Virus

**Texto del mensaje**: Si reciben un mail titulado "up-grade internet2 " NO LO ABRAN, ya que contiene un ejecutable con un ícono muy gracioso ,el ejecutable se llama PERRIN.EXE. Este virus borrará toda la información del disco duro,y de alguna manera se refugia en la memoria de la computadora, por lo que cada vez que carguen información en el disco duro ,este lo borrará de nuevo, dejando prácticamente inservible la computadora. Esta información fue publicada ayer en la página Web de la CNN. Se ha dicho que este virus es muy peligroso y que aún no existe antivirus para el. Reenvíen este mensaje a toda la gente que puedan, ya que si bien es cierto no puede ser detenido, al menos que salga perjudicada la menor cantidad de gente posible.

**Recomendaciones:**

- Mantenga las computadoras protegidas con programas antivirus actualizados.
- Ningún antivirus actual es capaz de reconocer todos los virus existentes ni sus variantes, por lo que una buena práctica de seguridad es utilizar al menos dos programas de esta clase para revisar los datos y archivos de programas que se reciban en la organización por medios magnéticos o electrónicos.
- Utilice, en los servidores, programas monitores de tráfico en la red para analizar el origen y comportamiento de los paquetes de información que fluyen en ella, especialmente cuando la red está basada en el protocolo TCP/IP.
- Defina una política de seguridad concerniente al uso del correo electrónico y al manejo de los archivos que se reciben por este medio ("attachments" o agregados). Los archivos entrantes y que tengan procedencia dudosa deberán desecharse o revisarse con algún(os) programa(s) antivirus antes de proceder a usarlos.
- Verifique las características de seguridad incluidas en sus programas de navegación y correo electrónico, específicamente en lo concerniente a las funciones de confidencialidad, integridad y autenticación. Si no las poseen, cambie de producto o actualice las versiones.
- Pero, sobre todo, implante procedimientos permanentes de respaldo y recuperación de la información, evalúelos y actualícelos de manera continua. La disciplina en cuanto a este tema es de capital importancia para reducir los riegos de pérdida de información estratégica para las organizaciones. Recuerde que nadie ha sufrido serios problemas por practicar respaldos, pero sí por no haberlos hecho.

# 7. Anexo. Desarrollos previos a Internet

La primera descripción registrada de la interacción social que pudiera realizarse por medio de redes fue una serie de memorandos escritos por J.C.R. Licklider del MIT, en agosto de 1962, discutiendo su concepto de "Red Galáctica". Él previó un conjunto de computadoras globalmente interconectadas a través del cual cualquiera podría tener acceso rápidamente a datos y programas almacenados en cualquier sitio. En espíritu, el concepto fue mucho lo que es hoy en día Internet. Licklider fue el primer director del programa de investigación en computadores DARPA. Mientras estuvo en él convenció a sus sucesores en este proyecto, Ivan Sutherland, Bob Taylor, y Lawrence G. Roberts (investigador del MIT), acerca de la importancia de su concepto de redes.

Leonard Kleinrock del MIT publicó el primer escrito sobre la teoría de la conmutación de paquetes en julio de 1961 y el primer libro sobre el tema en 1964. Kleinrock convenció a Roberts de la factibilidad teórica de la comunicación utilizando paquetes en vez de circuitos, lo cual constituyó un paso importante en la ruta a las redes de computadoras. Otro paso clave fue hacer que las computadoras se hablaran entre sí. Para explorar esto, en 1965 y trabajando con Thomas Merrill, Roberts conectó la computadora TX-2 en Massachusetts con la Q-32 en California a través de una línea telefónica de baja velocidad creando la primera red WAN (aunque también fue la más pequeña).

El resultado de este experimento fue la demostración de que las computadoras de tiempo compartido podían trabajar en forma conjunta, ejecutando programas y recuperando datos conforme los requería la estación remota, aunque la conmutación de circuitos del sistema telefónico fue totalmente inadecuada para este tipo de tarea. De esta forma se confirmó la convicción de Kleinrock acerca de la necesidad de la conmutación de paquetes.

En 1966 Roberts fue a DARPA para desarrollar el concepto de redes de computadoras y rápidamente lo unió a su plan (publicado en 1967) para la creación de otra red, ARPANET. En la conferencia donde se presentó el documento también había una propuesta que versaba acerca del concepto de redes de paquetes preparado por Donald Davies y Roger Scantlebury del NPL del Reino Unido. Scantlebury le habló a Roberts acerca del trabajo del NPL, así como de Paul Baran y otros del grupo RAND.

Este grupo había escrito un documento acerca de las redes de conmutación de paquetes para la seguridad de voz, en el ámbito militar, en 1964. Sucedió entonces que los trabajos en el MIT (1961-1967), en el RAND (1962-1965), y en el NPL (1964-1967) habían procesado el tema en paralelo, sin que ninguno de los investigadores conociera acerca de los otros trabajos. La palabra “paquete” se adoptó a partir del trabajo del NPL y la propuesta de velocidad de la línea de transmisión para ser utilizada en el diseño de ARPANET fue actualizada de 2.4 kbps a 50 kbps.

En agosto de 1968, después de que Roberts y DARPA se fusionaran, la comunidad redefinió la estructura total y las especificaciones de ARPANET. Una propuesta para recibir comentarios (“Request for Comments” - RFC), fue emitida por DARPA para el desarrollo de uno de los más importantes componentes, el conmutador de paquetes llamado

"Interface Message Processors" (IMP). La propuesta en consulta fue ganada en diciembre de 1968 por un grupo encabezado por Frank Heart del Bolt, Beranek y Newman (BBN).

Conforme el equipo de BBN trabajó en lo del IMP con Bob Kahn desempeñando un papel principal en el diseño de la arquitectura de ARPANET, lo concerniente a la topología de red y aspectos económicos fueron diseñados y optimizados por Roberts, quien trabajó con Howard Frank y su equipo en la Network Analysis Corporation, mientras que el sistema de mediciones de la red fue preparado por el equipo de Kleinrock en la UCLA.

Debido al temprano desarrollo de la teoría de la conmutación de paquetes de Kleinrock y su enfoque en el análisis, diseño y medición, su centro de mediciones de red, Network Measurement Center del UCLA, fue seleccionado como el primer nodo de ARPANET. Todo esto sucedió en setiembre de 1969 cuando BBN instaló el primer IMP en UCLA y se conectó la primera computadora anfitriona ("host"). El proyecto de Doug Engelbart intitulado "Augmentation of Human Intellect", acerca del aumento del intelecto humano, que incluía NLS (un prematuro sistema de hipertexto), desarrollado en el Instituto de Investigaciones de Stanford (SRI) se constituyó en el segundo nodo.

El SRI apoyó al Centro de Información de Redes (Network Information Center), dirigido por Elizabeth (Jake) Feinler, el que incluía funciones tales como mantenimiento de tablas con los nombres de las computadoras anfitriones para traducir direcciones, así como un directorio de los RFC. Un mes después de ello, cuando SRI estuvo ya conectado a ARPANET, se envió el primer mensaje anfitrión-a-anfitrión desde el laboratorio de Kleinrock hasta el SRI. Luego se agregaron dos nodos más, en Universidad de California en Santa Bárbara (UCSB) y la Universidad de Utah. Estos dos nodos le incorporaron proyectos de visualización de aplicaciones, con Glen Culler y Burton Fried del UCSB investigando métodos para desplegar funciones matemáticas utilizando despliegues almacenados para tratar con los problemas de refrescamiento sobre la red, y Robert Taylor e Ivan Sutherland en Utah investigando métodos de representación en tercera dimensión (3-D) sobre la red.

Es así como hacia finales de 1969 habían conectados cuatro anfitriones en la red ARPANET inicial y empezaron a aparecer otros nodos. Aún en estas primeras etapas se pudo notar que la investigación en redes incorporaba dos áreas de trabajo: los fundamentos de la red y cómo utilizar ésta, lo cual continúa hoy en día.

Durante los siguientes años se siguieron agregando rápidamente más y más computadoras, y el trabajo consistió en disponer de un protocolo anfitrión-a-anfitrión funcionalmente completo y algún otro software de red. En diciembre de 1970 el Grupo de Trabajo de Redes (NWG, Network Working Group), dirigido por S. Crocker finalizó el protocolo anfitrión-a-anfitrión inicial de ARPANET, denominado protocolo para el control de redes ("Network Control Protocol" - NCP). Conforme los sitios de ARPANET fueron completando la implantación de NCP, durante los años 1971-1972, los usuarios de la red finalmente pudieron empezar a desarrollar aplicaciones.

En octubre de 1972, Kahn organizó una grande y exitosa demostración de ARPANET en la Conferencia Internacional de Comunicación de Computadoras ("International Computer Communication Conference" - ICCC). Esta fue la primera demostración pública de la nueva tecnología de redes. Fue también en 1972 que se introdujo una aplicación innovadora, el correo electrónico.

En marzo, Ray Tomlinson del BBN escribió el software básico para enviar y leer correos electrónicos, motivado por la necesidad de los desarrolladores de ARPANET de disponer de un mecanismo fácil de coordinación. En julio de ese año Roberts extendió las utilidades al escribir el primer programa utilitario de correo para listar, leer selectivamente, archivar, reenviar y responder mensajes. A partir de aquí el correo electrónico se convirtió en la principal aplicación de red. Este fue un presagio de la clase de actividad que se apreciaría posteriormente sobre la red WWW y del enorme crecimiento que esta tendría en todas las clases de intercomunicación persona-a-persona.

# 8. Bibliografía


[AMOR 2000] Amor, Daniel, *"La (R)evolución E-Business*", Pearson Education S. A., Buenos Aires, Argentina, 2000.

[ANONYMOUS 1998] Anonymous, *"Maximum Security"*, Segunda Edición, Editorial SAMS Publishing, Indianápolis, Indiana, U.S.A., 1998.

[ATKINS 1997] Atkins, Derek y otros, "*Internet Security Professional Reference"*, Segunda Edición, Editorial New Riders Publishing, Indianápolis, Indiana, U.S.A., 1997.

[CHAPMAN 1997] Chapman, Brent y otros, "*Construya Firewalls para Internet"*, Editorial McGraw-Hill, Inc., México, 1997.

[COHEN 1995] Cohen, Frederick, *"Protection and Security on the Information Superhighway"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1995.

[COHEN 1994] Cohen, Frederick, *"A Short Course on Computer Viruses"*, Segunda Edición, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1994.

[COMER 1996] Comer, Douglas, *"Redes Globales de Información con Internet y TCP/IP: Principios básicos, protocolos y arquitectura"*, Editorial Prentice-Hall Hispanoamericana, S.A., México, 1996.

[DAVID 1993] David, Jon, *"Establishing a LAN Security Policy"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1993.

[DENNING 1983] Denning, Dorothy, *"Cryptography and Data Security"*, Editorial Addison-Wesley Publishing Company, Reading, Massachusetts, U.S.A., 1983.

[DENNING 1990] Denning, Peter, *"Computers Under Attack: Intruders, Worms and Viruses"*, Editorial, Addison-Wesley Publishing Company, Reading, Massachusetts, U.S.A., 1990.

[DESMOND 2000] Desmond, Paul, "A guide to e-commerce security", Artículo, www.techrepublic.com, Febrero 2000.

[EVERETT 1994] Everett, David, *"The Security Implications of EDI"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1994.

[FERREIRA 1991] Ferreyra, Gonzalo, *"Virus en las Computadoras"*, Segunda Edición, Editorial Macrobit, Miami, Florida, U.S.A., 1991.

[FORD 1994] Warwick Ford, "*Computer Communications Security. Principles, Standard Protocols and Techniques"*, Editorial PTR Prentice Hall, U.S.A., 1994.

[GAMEZ 1995] Gámez, Marco, *"Implementación de mecanismos criptográficos para la seguridad de la información utilizando firmas digitales"*, Tesis de Grado para optar por el título de Licenciado en Ingeniería de Sistemas, Universidad Internacional de las Américas, San José, Costa Rica, 1995.

[GARFINKEL 1997] Garfinkel, Simon, *"Web Security & Commerce"*, Editorial O'Reilly & Associates, Inc., 1997.

[GONÇALVES 1997] Marcus Gonçalves y otros, "*Internet Privacy Kit"*, Editorial Que Corporation, Indianápolis, Indiana, U.S.A., 1997.

[GONÇALVES 1998] Marcus Gonçalves, "*Firewalls Complete"*, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1998.

[GRANT 1998] Grant, Gail, "*Understanding Digital Signatures: Establishing Trust over the Internet and other networks"*, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1998.

[HADFIELD 1997] Hadfield, Lee y otros, "*Windows NT Server 4 Security Handbook"*, Editorial Que Corporation, Indianápolis, Indiana, U.S.A., 1997.

[HARE 1996] Hare, Chris y otros, "*Internet Firewalls and Network Security"*, Segunda Edición, Editorial New Riders Publishing, Indianápolis, Indiana, U.S.A., 1996.

[HERMAN 1992] Herman, Gary, *"UNIX Security: An Overview"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1992.

[HERNÁNDEZ 1998] Hernández, José, *"Seguridad en Redes"*, Trabajo de Investigación del Seminario Científico #1, Programa de Maestría en Computación, Instituto Tecnológico de Costa Rica, Cartago, 1998.

[HERNÁNDEZ 1999] Hernández, Edgar, *"Un Enfoque Gerencial sobre Seguridad en Sistemas de Información"*, Material del seminario para la II Jornada nacional de Tecnología de la Información, Centro para la Formación de Formadores – CEFOF, Alajuela, Costa Rica, 1999.

[HETHERINGTON 1992] Hetherington, Philip, *"Digital Equipment Corp. VAX Security: An Overview"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1992.

[HUBEL 1996] Hubel, Martin, *"Who Cares About Database Security?"*, Revista Database Programming & Design, Vol. 9, N° 2, Febrero 1996, págs. 43-45.

[HUBLEY 1994] Hubley, Mary, *"Securing UNIX Systems"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1994.

[HUGHES 1995] Hughes, Larry, "*Actually Useful Internet Security Techniques"*, Editorial New Riders Publishing, Indianápolis, Indiana, U.S.A., 1995.

[INMON 1997] Inmon, William, *"Security in the Data Warehouse/Internet Environment"*, IS Audit & Control Journal, Vol. IV, 1997, págs. 8-11.

[JACKSON 1991] Jackson, Carl. "The Need for Security", DataPro Reports on Information Security, Volumen 1, McGraw-Hill, 1991.

[JANAL 1998] Janal, Daniel, *"Risky Business: Protect Your Business from Being Stalked, Conned, or Blackmailed on the Web"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1998.

[KAY 1997] Kay, Emily, *"Interested In... ..DataWarehouse?: Security"*, Revista Data Warehousing Management, Julio 1997, URL: **http://www.sentrytech.com/dw07sec.htm.**

[KANE 1989] Kane, Pamela, *"V.I.R.U.S. Protection Vital Information Resources Under Siege"*, Editorial The Bantam Book, New York, U.S.A., 1989.

[KIMBALL 1997] Kimball, Ralph, *"Hackers, Crackers, and Spooks"*, DBMS online, Abril 1997, URL: **http://www.dbmsmag.com/9704d05.html.**

[LAMBERT 1997] Lambert, Nevin y otros, "*Windows NT Security. System Administrator's Guide"*, Revista PCWeek, Editorial Ziff-Davis Press, U.S.A., 1997.

[LILLY 1997] Lilly, Stephen, *"Client/Server Database Security Starts with Strong Passwords and Robust Auditing"*, IS Audit & Control Journal, Vol. VI, 1997, págs. 50-51.

[LYONS 1994] Lyons, Frank, *"An Introduction to Client/Server Security"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1994.

[MADRON 1992] Madron, Thomas, *"Network Security in the 90's: Issues and Solutions For Managers"*, Editorial John Wile & Sons, Inc., New York, U.S.A., 1992.

[MARTIN 1994] Martin, Richard, "*The Moving Wave of Techonology"*, Revista Client/Server Strategies, 1994.

[MCGRAW 1999] McGraw, Gary y otros, "*Securing JAVA"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1999.

[MILLER 1998] Miller, Stewart, "*Windows NT Security Guide"*, Editorial Digital Press, Boston, U.S.A., 1998.

[MULLENDER 1989] Mullender, Sape, "*Distributed Systems"*, Editorial ACM Press, Estados Unidos, 1989.

[NAIK 1998] Naik, Dilip, "*Internet Standards and Protocols"*, Editorial Microsoft Press, Redmont, Washington, 1998.

[NUTT 1992] Nutt, Gary J., "*Open Systems"*, Editorial, Prentice-Hall, U.S.A., 1992.

[PARKER 1998] Parker, Donn, "*Fighting Computer Crime"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1998.

[PRICE 1995] Price Waterhouse Interamerica Consulting Group, "*Estándares de Sistemas Abiertos de Software"*, Informe No. 18 del Club de Investigación Tecnológica, Costa Rica, 1995.

[RIVERA 1993] Rivera, Angel, *"LAN Security: NOS-Versus Application-Level Implementation"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1993.

[RODRÍGUEZ 1995] Rodríguez, Luis, "*Seguridad de la información en sistemas de cómputo"*, Editorial Ventura Ediciones, México D. F., 1995.

[ROSEN 1998] Rosen, Michele, *"Internet Security Standards"*, Revista PC Magazine, Vol. 17, N° 2, Enero 20, 1998, págs. 241-242.

[ROTHBERG 1992] Rothberg, Michael, *"LAN Security"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1992.

[RUBIN 1997] Rubin, Aviel y otros, *"Web Security Sourcebook: A Complete Guide to Web Security Threats and Solutions"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1997.

[SCHNEIER 1995] Schneier, Bruce, *"E-Mail Security: How to Keep Your Electronic Messages Private"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1995.

[SHELDON 1997] Sheldon, Tom, "*Windows NT Security Handbook"*, Editorial Osborne McGraw-Hill, Delran, New Jersey, U.S.A., 1997.

[SHERMAN 1997] Sherman, Richard, "*Intranet Data Access: The Fire Inside the Firewall"*, Revista Database Programming & Design, Vol. 10, N° 4, Abril 1997, págs. 36-41.

[TIWANA 1999] Tiwana, Amrit, *"Web Security"*, Editorial Digital Press, Boston, U.S.A., 1999.

[UCI 1997] Autores Varios, *"Seguridad Informática y Control: Capacitación para Ejecutivos"*, Material elaborado por la Universidad para la Cooperación Internacional, Maestría en Administración Informática, San José, Costa Rica, 1997

[UDELL 1998] Udell, Jon, *"In Search of SSL Spidering"*, Revista Byte, Vol. 23, N° 2, Febrero 1998, págs. 97-100.

[VALLABHANENI 1989] Vallabhaneni, Rao, *"Auditing Computer Security. A Manual with Case Studies"*, Editorial John Wiley & Sons, Inc., New York, U.S.A., 1989.

[VERISIGN 2001] Verisign Company, *"Building an E-Commerce Trust Infrastructure: SLL Server Certificates and Online Payment Services"*, White Paper, 2001.

[WARIGON 1997] Warigon, Slemo, "*Data Warehouse Control and Security"*, Editorial Association of College and University Auditors Ledger, Vol. 41, N° 2, Abril 1997, págs. 3-7, URL: **http://all.net/books/audit/kits/dw.html.**

[WAYNER 1997] Wayner, Peter, *"Digital Copyright Protection"*, Editorial Academic Press, Chestnut Hill, Massachusetts, U.S.A., 1997.

[WONG 1993] Wong, Ken, *"Networking/Distributed Systems Security"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1993.

[YUSSOF 1992] Yussof, Nora, *"Apple Macintosh Security: An Overview"*, Revista DATAPRO, Editorial McGraw-Hill, Inc., Delran, New Jersey, U.S.A., 1992.