UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

LA INFRAESTRUCTURA DE CLAVE PÚBLICA COMO UN ENFOQUE DE SEGURIDAD PARA LAS REDES INFORMÁTICAS

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN MATEMÁTICAS APLICADAS

Y

COMPUTACIÓN

P R E S E N T A :

CÉSAR JAVIER RAMÍREZ GONZÁLEZ

ASESOR: ANDRÉS HERNÁNDEZ BALDERAS

MARZO 2006

AGRADECIMIENTOS

Primeramente a **Dios**, por la salud, por cuidar siempre de mi seres queridos, por las oportunidades que se presentan, por iluminarme el camino, y por permitirme disfrutar lo maravilloso de la vida y de las personas que amo.

A MI MADRE, ARACELI GONZÁLEZ SANTIAGO
Gracias Mamá, primeramente por haberme dado la vida, pues la vocación de ser madre, tan marcada como la tuya, no se iguala con nada. Quiero agradecerte por medio de éstas líneas, todos tus esfuerzos, tus desvelos, tus sacrificios hacia mi, ya que toda mi vida has estado en mi mente y mi corazón, hemos compartido juntos tristezas y alegrías, éxitos y fracasos, y de los cuales, gracias a tu apoyo y consejos, he aprendido mucho. No sabes lo agradecido que estoy con la vida y con DIOS, y lo afortunado y orgulloso que me siento, el que me haya tocado una Mamá como tú, en ti encuentro paz, bondad, amor, valentía, responsabilidad, en fin, pienso que como mujer y como madre, eres única y excepcional. Mamá, tú que me tuviste dentro de tus entrañas y que me conoces mejor que nadie, sabrás que sin tu presencia, éste logro obtenido, jamás lo hubiera podido realizar, eres una parte fundamental de mi vida y en todo lo que hago, tú le das color y alegría a mi vida, le das forma y sentido a esas cuatro letras, Mamá. Este logro es más tuyo que mío, y quiero que siempre recuerdes que te AMO y que pase lo que pase siempre ocuparás un lugar muy especial en mi corazón.

A MI PADRE, JOSE ISABEL RAMÍREZ CRUZ
Creo sinceramente que nunca terminare de agradecerte el amor, comprensión y apoyo que me has dado a lo largo de mi vida, ya que siempre que te he necesitado, has estado en el lugar y en el momento correcto, pues tanto en mis triunfos como en mis derrotas, siempre me has alentado a seguir adelante. Me siento tan orgulloso de que me haya tocado ser tu hijo, siempre seras mi héroe, pues mejor Papá que tú, no me pudo haber tocado, porque desde pequeño, has sido para mí un hombre grande y maravilloso y que siempre te admirado. De verdad, te agradezco poder permitirme compartir contigo esta nueva etapa de mi vida, quiero que este triunfo en especial lo sientas más tuyo que mío, ya que sin tu presencia y sin tu incondicional apoyo, no hubieran sido igual las cosas. Te amo.

¡MUCHAS GRACIAS ! ¡ LOS AMO !
¡ DIOS LOS BENDIGA !

A mis Hermanitas
Alma y Ariadna, por soportar mi pésimo carácter, por que siempre están cuando las necesito, por su amistad, cariño, por sus palabras de aliento, sencillez y dulzura, le doy gracias a DIOS de tenerlas cerca de mí. **¡Si quieres triunfar, no te quedes mirando la escalera. Empieza a subir, escalón por escalón, hasta que llegues arriba!**

¡ DIOS LAS BENDIGA !

A la Universidad Nacional Autónoma de México, mi alma mater
Quiero agradecer a la Máxima casa de Estudios por haberme brindado la oportunidad de pertenecer a ella, primero como estudiante y ahora como Profesionista. Es un orgullo formar parte de tan honorable Institución, a través de la cual recibí una preparación intelectual y personal inigualable a las demás.

Por supuesto, muy especialmente, a la **FES ACATLÁN**, de la cual me siento muy orgulloso de ser egresado.

A mi asesor, el Lic. Andrés Hernández Balderas., por el tiempo y la atención ofrecida para la realización de este trabajo. Le estaré eternamente agradecido.

A mis sinodales por el voto de confianza al trabajo realizado.

A toda la **banda rockanrolera** Alejandro Montaño, Ángel, Cacho, Jimy, Lourdes, Mariano, Meliton, Miguel, Quiles, Rafael, Ricardo Huicochea, Roberto, Saúl, Wilfrido, gracias por brindarme su amistad y por recorrer junto conmigo este andar, por aquellos días que pasamos en nuestra vida universitaria, la cual permanecerá en mi mente, como el más maravilloso recuerdo, que aunque pase el tiempo jamas se borrara. Compartir los sueños con ustedes es empezar a convertirlos en realidad. **¡Nuestra gloria más grande no consiste en no haberse caido nunca, sino en haberse levantado después de cada caída!**

¡ GRACIAS !

Un especial agradecimiento a los **Ing**. CARLOS ARCE LEON y al **Ing**. OMAR ULISES MORALES DÁVILA, gracias por brindarme la oportunidad de trabajar con ustedes, por sus consejos, por motivarme a seguirme superando, pero sobre todo por su confianza.
¡ GRACIAS !

A todo el personal que labora en el **C.I.D**, pero en especial a mis amigos, Carmen Zavala (La jefa), a la Diseñadora Gráfica Jessica González Dueñas, no podría olvidarme de mi amore Nancy (la flaca), María (la maris), Yola, Carolina (carito), Jaime (fan # 1 de los pumas), Lucia, Patricia., muchas gracias por esas palabras de aliento que han tenido hacia mi, por sus consejos. Ustedes son como mis ángeles, que me ayudan a ponerme de pie otra vez cuando mis alas se rompen y se me ha olvidado de cómo volar. **¡Utiliza tu imaginación, no para asustarte, sino para inspirarte a lograr lo inimaginable!**

¡ GRACIAS ¡

ÍNDICE

Pág.

OBJETIVO..... 1
INTRODUCCIÓN..... 2
CAPITULO I. VISIÓN GENERAL DE LA SEGURIDAD EN REDES..... 4

1.1 Antecedentes de las redes..... 5
1.1.1 Definición de red..... 8
1.2 Tipos de redes..... 9
1.2.1 Redes por el área que abarcan..... 9
1.2.2 Por su topología..... 11
1.3 El Modelo de referencia OSI..... 13
1.4 Protocolos de red..... 15
1.4.1 Ethernet..... 15
1.4.2 Token Ring..... 16
1.4.3 TCP/IP..... 17
1.4.4 Protocolos de NetWare..... 20
1.4.5 Protocolo NetBEUI..... 20
1.4.6 Protocolo NetBIOS..... 21
1.5 Servicios de red..... 22
1.6 Perspectiva histórica de la seguridad en redes..... 23
1.7 ¿Por qué es necesaria la seguridad en las redes?..... 24
1.8 ¿Qué es la seguridad en redes?..... 25
1.9 Objetivo de la seguridad en redes..... 26
1.10 Principios fundamentales de la seguridad..... 26
1.11 Servicios de seguridad..... 28
1.11.1 Servicio de autentificación..... 31
1.11.2 Servicio de confidencialidad de datos..... 32
1.11.3 Servicio de integridad de datos..... 32
1.11.4 Servicio de no repudio..... 33
1.11.5 Servicio de control de acceso..... 34
1.11.6 Servicio de anonimato..... 35

CAPITULO II. RIESGOS Y DIRECTRICES DE PROTECCIÓN..... 37

2.1 Análisis de las amenazas a los sistemas de redes..... 38
2.1.1 Tipos de amenazas..... 40
2.2 Tipos de problemas a la integridad de las redes..... 45
2.2.1 Tráfico de red engañoso..... 45
2.2.2 Acceso inapropiado a recursos..... 45
2.2.3 Interrupción de la red..... 46

2.2.4 Modificaciones no autorizadas de software..... 47
2.2.5 Acceso no autorizado a la red..... 47
2.2.6 Suplantación de la identidad..... 49
2.2.7 Denegación de servicio..... 50
2.3 Seguridad en las capas TCP/IP..... 51
2.3.1 Capa de aplicación..... 51
2.3.2 Capa de transporte..... 52
2.3.3 Capa de red..... 53
2.3.4 Cómo utilizar la seguridad en las capas TCP/IP..... 55
2.4 Mecanismos de seguridad..... 56
2.4.1 Mecanismos de seguridad específicos..... 57
2.4.2 Mecanismos de seguridad generalizados..... 58
2.5 Análisis de las herramientas de seguridad..... 59
2.5.1 Seguridad en la infraestructura física..... 59
2.5.1.1 Protección de los dispositivos físicos..... 59
2.5.2 Controles de seguridad lógica..... 60
2.5.2.1 Controles de acceso..... 60
2.5.2.1.1 Control de acceso interno..... 61
2.5.2.1.2 Control de acceso externo..... 61
2.5.3 Niveles de seguridad..... 62
2.5.4 Infraestructura e integridad de los datos..... 64
2.5.4.1 Firewalls..... 64
2.5.5 Políticas de seguridad..... 66
2.6 Un modelo de seguridad en redes..... 67

CAPITULO III. INFRAESTRUCTURA DE CLAVE PÚBLICA..... 69

3.1 Desarrollo histórico de la PKI..... 70
3.2 ¿Qué es una PKI?..... 72
3.2.1 Ventajas..... 73
3.2.2 Desventajas..... 74
3.3 Cifrado básico..... 75
3.3.1 Cifrado simétrico..... 77
3.3.2 Cifrado asimétrico..... 80
3.3.2.1 Funciones hash..... 84
3.3.2.2 Firmas digitales..... 87
3.3.2.3 Certificados digitales..... 89
3.3.2.4 Administración de claves..... 89
3.3.2.4.1 Generación de claves..... 90
3.3.2.4.2 Distribución de claves..... 90
3.3.2.4.3 Certificación de la clave..... 91
3.3.2.4.4 Protección de la clave..... 91

3.3.2.4.5 Revocación de la clave..... 92
3.3.2.4.6 Transporte de la clave..... 92
3.4 Análisis de los componentes de la PKI..... 93
3.4.1 Autoridades de certificación..... 93
3.4.1.1 Tipos de autoridades de certificación..... 95
3.4.1.2 Organización jerárquica de las autoridades de certificación..... 96
3.4.1.2.1 Modelos jerárquicos subordinados..... 96
3.4.1.2.2 Modelos entre iguales..... 97
3.4.1.2.3 Modelos en malla..... 97
3.4.2 Autoridades de registro..... 98
3.4.3 Certificados digitales..... 99
3.4.3.1 Formato general de los certificados..... 101
3.4.3.1.1 Tipos de certificados..... 102
3.4.3.1.2 Gestión de los certificados..... 104
3.4.3.1.2.1 Generación y certificación..... 104
3.4.3.1.2.2 Revocación de los certificados..... 104
3.4.3.1.2.3 Renovación de certificados..... 104
3.4.3.1.2.4 Validación de certificado..... 105
3.4.4 Depósito de certificados y listas de certificación..... 106
3.5 Planificación de la PKI..... 109
3.5.1 Elección de los componentes para el modelo propuesto..... 109
3.5.2 Funciones del modelo..... 114
3.5.3 Selección de la plataforma de trabajo..... 115
CONCLUSIÓN..... 116
APÉNDICE I..... 119
APÉNDICE II..... 126
GLOSARIO..... 129
FUENTES DE INFORMACIÓN..... 135

INTRODUCCIÓN

El presente trabajo tiene como finalidad dar a conocer al lector una idea de los componentes de las infraestructura de clave pública (PKI, Public Key Infraestructure) con todos los conceptos que definen a la misma. Durante los últimos tiempos, la PKI aparece junto a los cortafuegos (Firewalls) y las redes privadas virtuales (RPV, Virtual Private Networks) como uno de los más importantes requisitos de seguridad para cada vez más redes de empresas.

Y es que hoy en día la mayoría de los cambios que se producen en los sistemas de comunicaciones se generan internamente. Las compañías dependen cada vez de sus redes informáticas para ofrecer importantes funciones de negocio, que tienen como resultado el crecimiento de los datos residentes en dichos sistemas. Conforme aumenta la cantidad de información, también se incrementa la dificultad de gestionarla, forzando a los administradores de las redes a buscar nuevas tecnologías y técnicas que suministren la protección que necesitan. En el mundo de las redes de computación, el procedimiento de requerir múltiples firmas en papel para requerir autorización y para atestiguar la identidad parecen procedimientos anticuados. Sin embargo sigue existiendo la misma necesidad de siempre: cómo determinar la identidad del solicitante, el cual puede ser una persona o un recurso. La dificultad radica en saber cómo podemos confiar que quien se comunica con el fin de realizar un requerimiento o satisfacerlo, es quien dice ser.

Aquí es donde la PKI juega un papel importante, ya que es capaz de añadir seguridad a las comunicaciones, lo que le permite a una compañía contar con sistemas de autenticación, control de accesos, confidencialidad y no repudiabilidad para sus aplicaciones en redes, usando tecnología avanzada, tal como firmas digitales, criptografía y certificados digitales, es decir, la PKI maneja, de manera transparente, las claves y los certificados permitiendo a una organización crear y usar un entorno de red confiable. Las ventajas obtenidas son las siguientes: comunicaciones confidenciales, autenticación (ofrecer la plataforma para que los servidores y usuarios puedan ser certificados y garantizar de esta forma su autenticidad), no repudio (prevenir que el emisor niegue su involucración en la creación de un fichero) e integridad (garantizar que el documento no ha sido alterado).

El primer Capítulo, “Visión General de la Seguridad en Redes” de esta investigación se dedica a explicar los conceptos básicos de los sistemas de redes, y se presenta una visión panorámica de los principales conceptos, servicios y técnicas presentes en la seguridad en redes, lo que nos permitirá responder a cuestiones tales como ¿por qué es necesaria la seguridad?, ¿qué servicios de seguridad se deben proporcionar?, ¿cómo se deben implementar?, etc.

El Capítulo 2, “Riesgos y Directrices de Protección” se centra en la determinación de las amenazas a las que se encuentran expuestos los sistemas de redes telemáticas. Conviene saber qué áreas de la red son más susceptibles a los intrusos y quiénes son los atacantes más habituales.

Una vez identificados los activos vitales y analizados los riesgos, es el momento de diseñar las normas definiendo las directrices y los procedimientos a seguir. En este capítulo se analizan las siguientes áreas:

- Definición de los controles de seguridad física.
- Definición de los controles de seguridad lógica.
- Garantía de la integridad del sistema y de los datos.
- Garantía de la confidencialidad de los datos.
- Definición de políticas.

Por último se presenta en el Capítulo 3, “Infraestructura de Claves Públicas” se determinara cuál es la metodología que se usa cuando se evalúa el rendimiento de la PKI y cómo ofrece servicios de seguridad para los sistemas de redes; también nos dedicaremos a explicar de forma resumida los conocimientos criptográficos imprescindibles para entender adecuadamente los protocolos y los servicios de seguridad. Asimismo estudiaremos todo lo relacionado con los ciclos de vida de las claves y de los certificados digitales dentro de una PKI, y entender cómo se pueden usar los modelos de confianza para establecer relaciones entre las organizaciones. Como complemento se citarán los estándares más significativos de la seguridad de la red e Internet, y se verán algunos aspectos de la teoría de números.

OBJETIVO DEL TRABAJO

Presentar un panorama general de los fundamentos de la Infraestructura de Claves Públicas que nos permita habilitar los servicios de autentificación, confidencialidad, integridad y no repudio para la protección de la información y de las transacciones realizadas en los sistemas de redes, es decir, que el estudio de dichas infraestructuras nos permita realizar funciones como acceso a las aplicaciones y sistemas informáticos e intercambio de la información entre estos de la forma más segura posible.

CAPÍTULO 1

VISIÓN GENERAL DE LA SEGURIDAD EN REDES

Las redes, debido a su dispersión geográfica y a los múltiples equipos y sistemas que de ellas forman parte, presentan un marco idóneo para posibles ataques y operaciones no autorizadas. El uso malicioso de las redes puede afectar tanto a la seguridad de los sistemas como a la validez de la información que se almacena o transfiere. Modificar y falsificar un documento representado en formato electrónico es mucho más sencillo que hacerlo sobre un documento escrito en papel. Asimismo, debido al acceso remoto, sin ninguna de las cortapisas que introduce una comunicación presencial, es también relativamente sencillo hacerse pasar en la red por quien realmente no se es, con los consiguientes riesgos de pérdida de fiabilidad de la información para quien la recibe. Esta vulnerabilidad de las redes hace que sea necesario introducir medidas que las protejan contra usos maliciosos. En este capítulo se estudian los principales conceptos de las redes y de su seguridad.

1.1 Antecedentes de las redes

Los tres últimos siglos han estado dominados, cada uno de ellos, por una tecnología. El siglo XVIII fue la época de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la era de las máquinas de vapor. En el siglo XX, el tremendo impacto que ocasionó la aparición de las computadoras y de los sistemas de redes, provocó que a este período de la historia se le denominara "la era de la información" [Tanenbaum, 1991].

Los antecedentes que se tienen de las redes se puede remontar a mediados del siglo XIX, donde los telégrafos conformaron las primeras redes de comunicaciones[1], la codificación en Morse constituía un método simple y eficaz para la transmisión de información a largas distancias (véase la Figura 1.1).

La aparición de las primeras redes en la era moderna se remontan a los inicios de los primeros sistemas de tiempo compartido[2]. En términos más generales, la cuestión era distribuir los recursos y la meta era hacer que todos los programas, el equipo y especialmente los datos estuvieran disponibles para cualquiera, sin importar la localización física de los recursos y de los usuarios. Una vez demostrado que un grupo de personas más o menos reducido podía compartir una misma máquina, era natural preguntarse si toda la organización podría utilizar los recursos disponibles (discos, terminales, impresoras, e incluso programas especializados y bases de datos) en sus respectivos equipos, por lo que se empezaron a estructurar protocolos e interfaces estandarizados, con lo que se conseguían unos soportes independientes de las máquinas, de los fabricantes y de las infraestructuras utilizadas. Esta tendencia catalizó el SNA[3] (la primera gran arquitectura de comunicaciones que, posteriormente inspiraría el no menos conocido modelo de referencia OSI). A partir de este momento hicieron su aparición varios diseños [Gallo y William, 2002], para la comunicación de las redes que vinieron a configurarse de un modo más genérico y abstracto.

Figura 1.1 El telégrafo es el medio más antiguo de enviar y recibir información por medio de la electricidad. Por vez primera, la gente podía ponerse en contacto instantáneo entre dos lugares enlazados por un cable.

Conforme pasaba el tiempo y progresaba la tecnología, los ingenieros comenzaron a conectar computadoras de modo que se pudiesen comunicar. Esto trajo consigo la aparición de las primeras redes de datos públicas como: Tymnet y Telenet; así como también de las grandes corporaciones como Xerox, General Motors, IBM, Digital Equipment Corporation, AT&T y Burroughs, y

[1] *http://www.cff.gob.mx/html/la_era/info_tel/it24.html*
[2] *El paradigma original de computación compartida consistía en una única y gran computadora conectada a una serie de terminales, cada uno de las cuales podía ser utilizado por un usuario diferente.*
[3] *Systems Network Architecture, es el protocolo de comunicación entre computadoras Mainframe y terminales que fue desarrollado por IBM en 1973, así como tambien en los servidores IBM AS/400.*

sistemas de investigación, como las inglesas SERCNET y NPL 1966-1968; HMI-NET de Berlín 1974; CYCLADES de Francia 1972; REDT de España 1971 y posteriormente las redes comerciales y comunidades virtuales, especialmente USENET[4] y FIDONET[5]. La siguiente Tabla 1.1 muestra las fechas de puesta en funcionamiento de redes de conmutación de datos en el mundo.

Al mismo tiempo, se volvieron más pequeñas y más baratas y aparecieron las mini y microcomputadoras. Las primeras redes utilizaban enlaces individuales, como las conexiones telefónicas, para unir dos sistemas. Tan pronto como la primera PC de IBM impactó en el mercado en 1980 y fue rápidamente aceptada como herramienta de la empresa, resultaron obvias las ventajas de conectar estas pequeñas computadoras. Cuando un usuario necesitaba entregar un archivo a otro, la red eliminaba la necesidad de intercambiar diskettes. Sin embargo, el problema fue que no era práctico conectar una docena de máquinas en una oficina con enlaces individuales punto a punto entre todas ellas. La solución eventual fue la red de área local (LAN, Local Area Network).

	Red de conmutación de formato	**Año de entrada en servicio**	**Red de conmutación de circuitos**
España	RETD / RSAN	1972	NO
	IBERPAC X.25	1985	NO
Alemania	DATEX – P	1981	DATEX – L
Austria	DATEX – P	1983	DATEX – L
Bélgica	DCS	1982	NO
Dinamarca	DATAPAK	1984	DATEX
Finlandia	DATAPAK	1984	DATEX
Francia	TRANSPAC	1978	CADUCCE
Holanda	DN – 1	1981	NO
Irlanda	EIRPAC	1984	NO
Italia	ITAPAC	1985	RFD
Luxemburgo	LUXPAC	1983	NO
Noruega	DATAPAK	1984	NPDN
Portugal	TELEPAC	1984	NO
Reino Unido	PSS	1981	NO
Suecia	DATAPAK	1985	NPDN
Suiza	TELEPAC	1983	NO
EEUU	TYMNET / TELENET	1975	SIN DATOS
Canadá	GLOBEDAT	1977	SIN DATOS

Tabla 1.1 Fechas de puesta en funcionamiento de redes de conmutación de datos en el mundo. Fuente: Ministerio de Transportes, Turismo y Comunicaciones: "Informe anual sobre los Transportes, El Turismo y Las Comunicaciones. 1986". Madrid.

[4] *Sistema de noticias de red que desarrollaron las Universidades Duke y North Carolina, en 1979.*
[5] *Sistema de interconexión y distribución de anuncios o de boletines electrónicos, creado en 1982.*

Una de las razones por las que las LAN han florecido es que, comparadas con los sistemas basados en una computadora central, permiten a los usuarios finales, y a los departamentos, mayor libertad para elegir su forma de trabajar, suministrando, de forma simultánea, un control de la información y de los empleados. La Tabla 1.2 muestra una comparación entre procesamiento basado en LAN y otras posibilidades [Farley, Stearns, Hsu, 1998].

	Costo de equipamiento	Operadores del sistema	Control del sistema	Productividad del personal
Sistema basado en una computadora central	$$$$$$	Pocos	Estricto	Mínima
Minicomputadoras	$$$$$$	Pocos	Bueno	Mínima
PC	$	Todos	Mínimo	Excelente
Lan	$$$	Pocos	Estricto	Excelente

Tabla 1.2 ¿Por qué se utilizan las LAN?: relativo bajo costo y mejor control del negocio mientras fomenta la productividad.

En la actualidad las nuevas redes de comunicaciones nacen inspiradas en las posibilidades abiertas por las tecnologías de transmisión y en la potencia de los dispositivos informáticos. Hoy vivimos la convergencia de los dos mundos, computación y telecomunicaciones, que hasta ahora únicamente habían estado relacionados haciéndose coparticipes en el proceso de transferencia de la información. Esta estrategia consiste, a groso modo, en delegar el control de flujo y control de errores a los dispositivos de los usuarios mientras que la red es solo responsable de la transmisión y la conmutación de los datos. El objetivo es claro, obtener un rendimiento y una calidad de servicio óptimos (Figura 1.2).

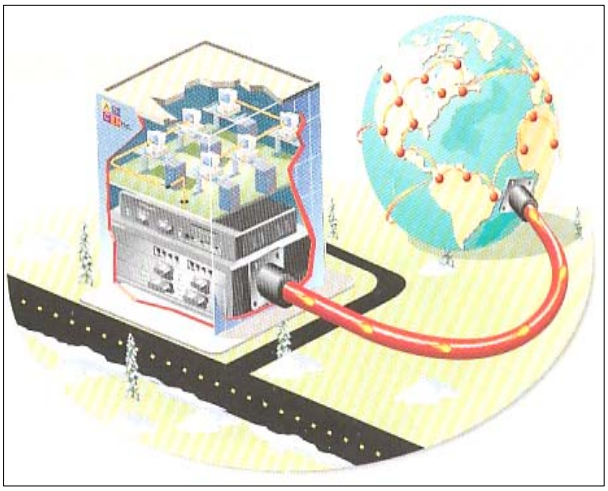


Figura 1.2 Las redes proporcionan recursos de cómputo en el punto en que se necesiten, además de la flexibilidad para soportar requisitos de información dinámica de manera continua.

1.1.1 Definición de red

Se puede definir una red informática como un sistema de comunicación que conecta computadoras y otros dispositivos (véase Figura 1.3) que son capaces de comunicarse entre sí empleando un medio de transmisión, con la finalidad de compartir información y recursos [Zacker, 2002].

A través de compartir la información y recursos en una red, los usuarios de los sistemas informáticos de una organización podrán hacer mejor uso de los mismos, mejorando de este modo el rendimiento global de las instituciones. Entre las ventajas que supone el tener instalada una red, pueden citarse las siguientes:

- Proporcionan la posibilidad de que las organizaciones puedan intercambiar datos y hacer accesibles los programas y los datos a todo el personal de la empresa.
- Pueden facilitar la función crítica de tolerancia ante fallos.
- Permiten disponer de un entorno de trabajo muy flexible.

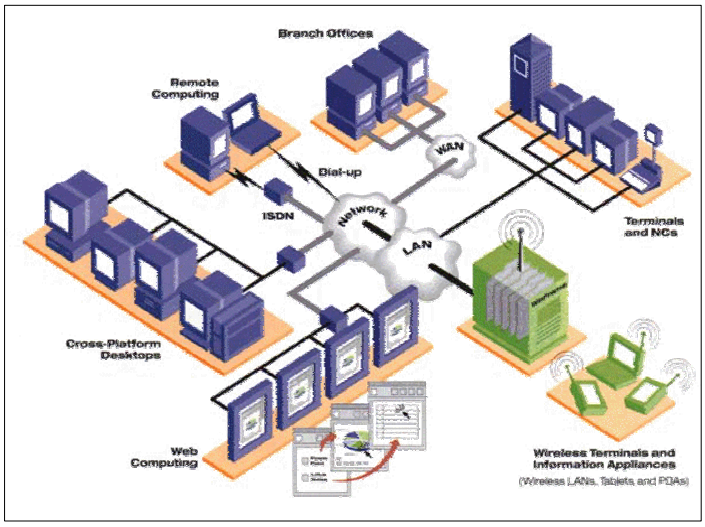


Figura 1.3 Ejemplo de una red informática.

1.2 Tipos de redes

No existe una taxonomía generalmente aceptada dentro de la cual quepan todas las redes de computadoras. Las diferencias entre ellas se fundamenta usualmente en la perspectiva o la forma que adopten. Por ejemplo, se pueden dividir por el área geográfica que abarcan (red de área local, amplia o extendida), por topologías (punto a punto o de difusión), o el tipo de rutas de comunicación que usan y la manera en que los datos son transmitidos a lo largo de esta ruta (por circuito o paquete conmutado) [Gallo y William, 2002].

1.2.1 Redes por el área que abarcan

Las LAN, representa un sistema de comunicación local que une a varios usuarios (servidores, estaciones de trabajo, etc.) que permite transferir datos a altas velocidades[6], en distancias cortas[7], y dentro de los límites de una localización privada (véase Figura 1.4).

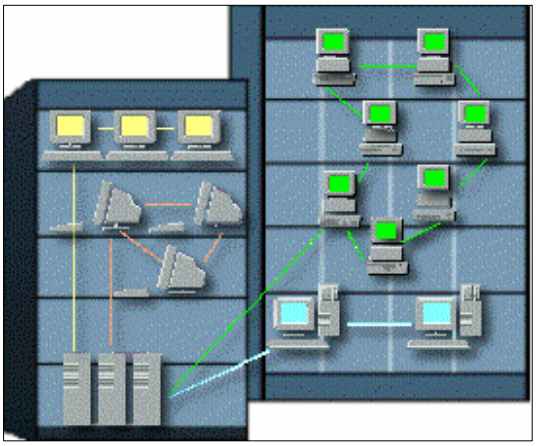
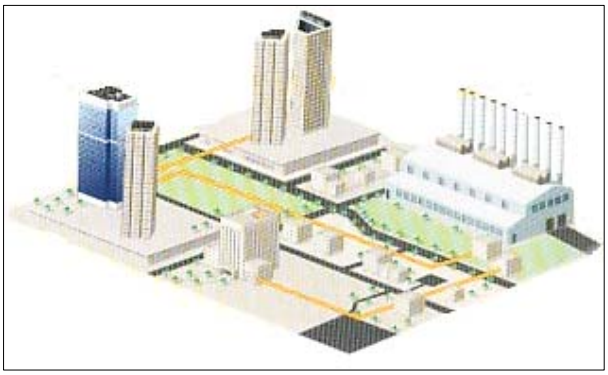


Figura 1.4 Funcionamiento de una LAN.



Una **red de área metropolitana, (**MAN , Metropolitan Area Network) es una colección de redes de área local. Estas se conectan en la misma zona geográfica, por ejemplo un pueblo o ciudad (véase Figura 1.5).

Figura. 1.5 Ejemplo de una red MAN.

[6] *Desde unos cientos de Kilobits por segundo hasta varias decenas de Megabits por segundo.*
[7] *Desde unos centenares de metros hasta unos kilómetros.*

Una **red de largo alcance** (WAN, Wide Area Network), es un sistema de interconexión de equipos informáticos geográficamente dispersos, que pueden estar incluso en continentes distintos (véase Figura 1.6).

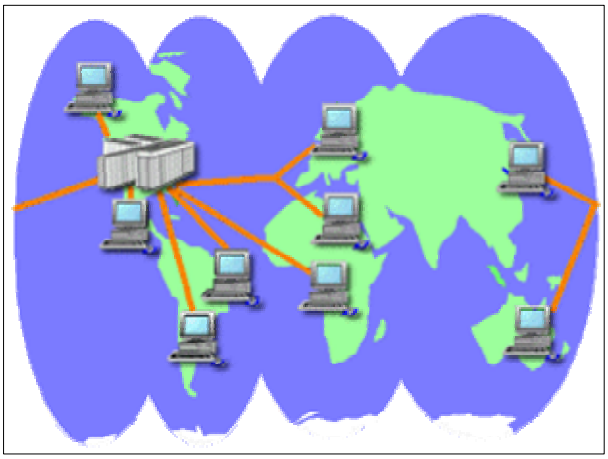
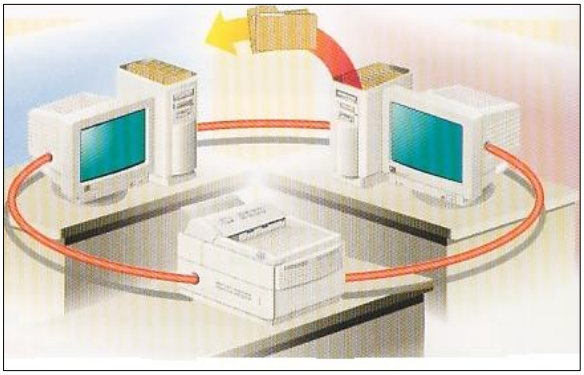


Figura 1.6 Ejemplo de una red WAN.



PAN. **Red de área personal** (PAN, Personal Area Network), se refieren a las pequeñas redes de computadoras que se encuentran en los hogares (véase Figura 1.7).

Figura 1.7 Ejemplo de una red PAN.

Las **redes de área de almacenamiento** (SAN[8], Storage Area Networks), son sistemas informáticos dedicados exclusivamente a guardar información (véase Figura 1.8).

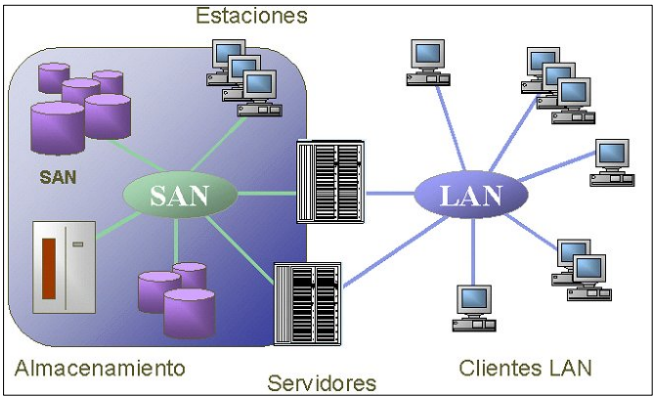


Figura 1.8 Las SANs son el resultado de la convergencia de administrar mayores cantidades de información y de la conectividad física con dispositivos de almacenamiento heterogéneo.

[8] ***NETTIMES COMMUNICATION, Año 3 No.30, México, Septiembre de 1999, Pág. 16.***

1.2.2 Por su topología

RED PUNTO A PUNTO (PEER TO PEER). Permiten que las computadoras compartan información y recursos. Cada máquina en este tipo de red almacena su propia información y no existen equipos centrales que la controlen. Varias topologías se basan en el diseño punto a punto, estas son: estrella, bucle y árbol. (véase Figuras 1.9 a, b, c).

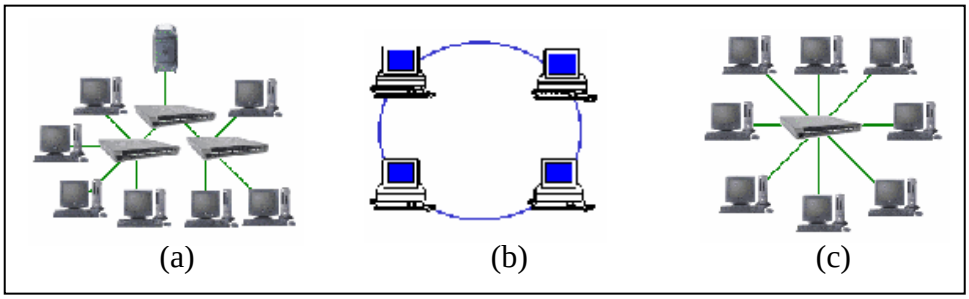


Figura. 1.9 Las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas.

RED DE DIFUSIÓN (BROADCAST). Tienen un sólo canal de comunicación compartido por todas las máquinas de la red. Los sistemas de difusión emplean varias topologías, en particular bus y anillo (véase Figura 1.10 a, b).

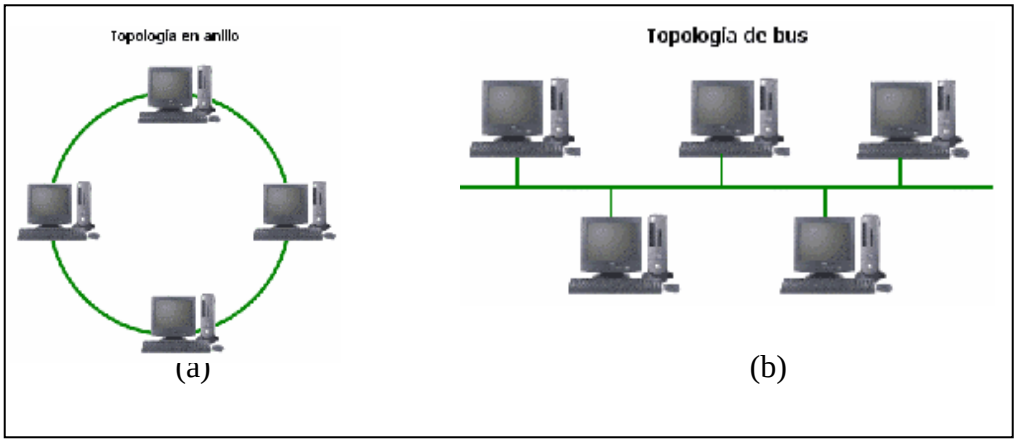


Figura. 1.10 Dos redes de difusión. (a)Anillo. (b)Bus.

REDES CONMUTADAS. Las redes también pueden clasificarse por el tipo de trayectoria de las comunicaciones que usan y la manera en que los datos son transmitidos. Dos clasificaciones particulares son circuito conmutado y paquete conmutado (véase Figura 1.11), las cuales implican una topología parcial o totalmente enmallada y usan dispositivos especiales llamados conmutadores para interconectar los enlaces entre los nodos fuente y los nodos destino.

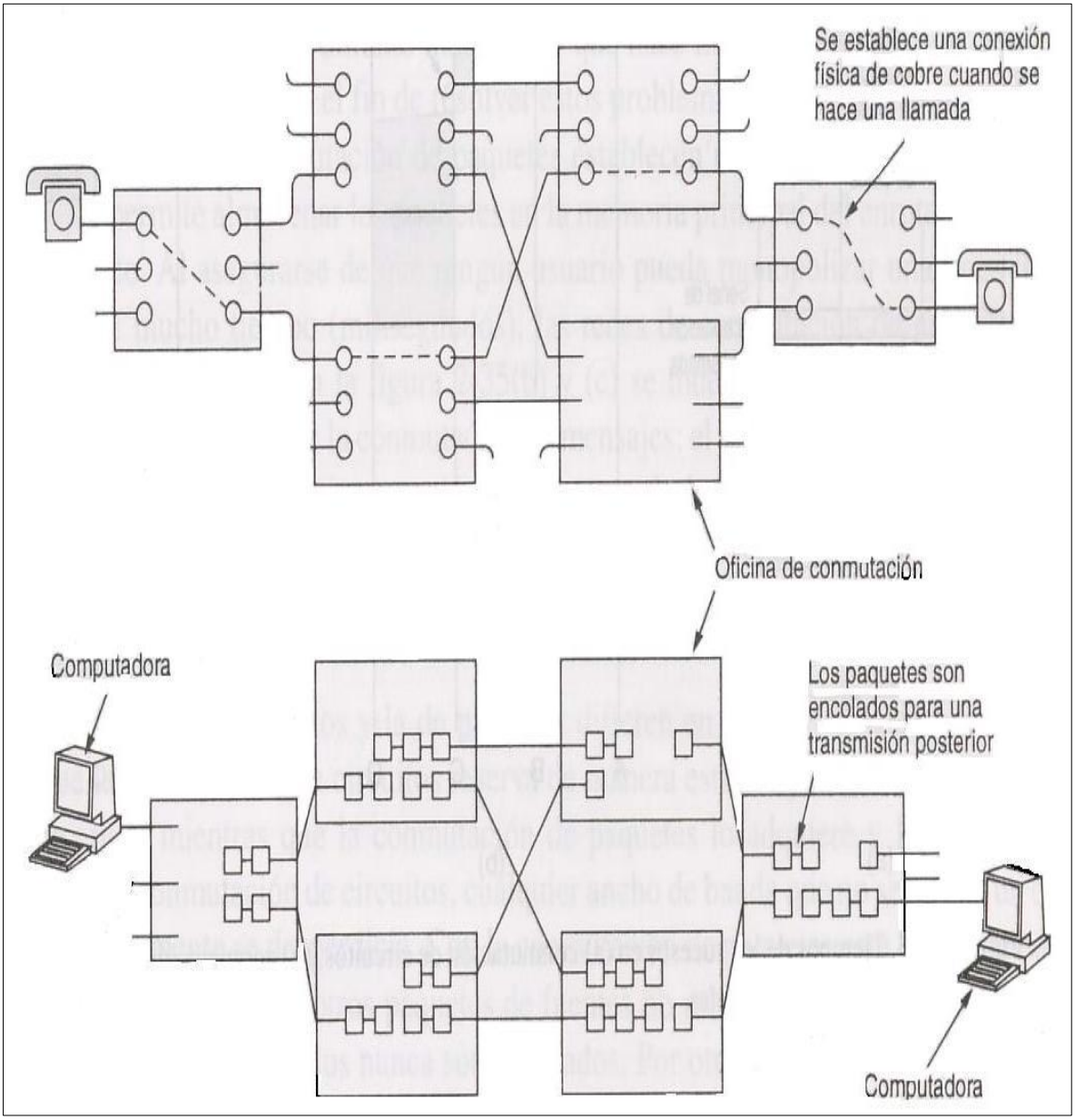


Figura 1.11 (a)Conmutación de circuitos. (b)Conmutación de paquetes.

1.3 El modelo de referencia OSI

En los primeros días de las operaciones con redes, la interoperabilidad y temas de diseño comenzaron a emerger. Para tratar esos temas, y para posibilitar la interconexión de varias redes patentadas y heterogéneas, la Federación Mundial de Organismos de Estandarización (ISO, International Organization for Standardization) desarrolló en 1974 una arquitectura y modelo de referencia para que sirviera como base de futuras actividades de estándares de redes. El Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI, Open Systems Interconnection) proporciona un conjunto detallado de estándares para la descripción de una red [Zacker, 2002] y [Heywood, 1999].

Una de las características más rescatables del OSI es que define formalmente y codifica el concepto de arquitectura de red en capas; también describe operacionalmente el procesamiento de la transmisión de los datos en cada capa (véase Figura 1.12).

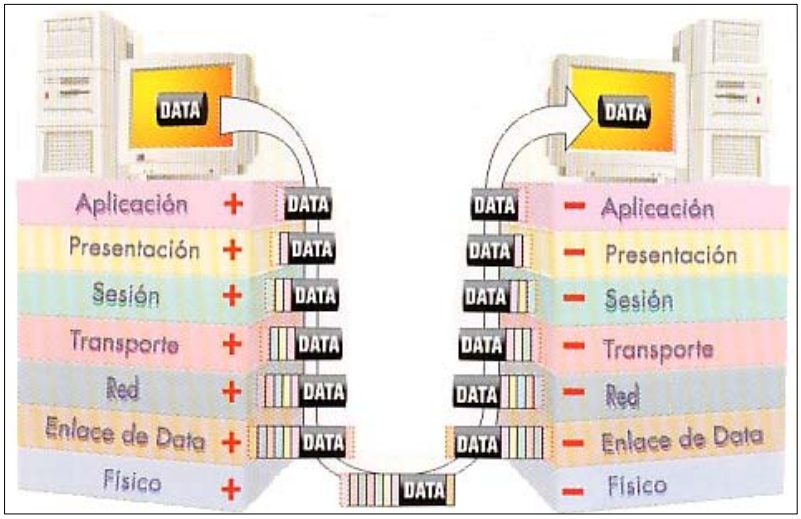


Figura 1.12 Todas las capas OSI ejecutan un protocolo para administrar las conexiones entre los dispositivos.

El modelo OSI divide las redes en siete capas funcionales y por ello se conoce a menudo con el nombre de **pila de siete capas**, las cuales definen una función o conjunto de funciones que se realizan cuando los datos se transfieren entre aplicaciones a lo largo de la red. Una definición más detallada de estos niveles se da en la Tabla 1.3. Cada capa es un protocolo para comunicaciones entre los dispositivos enlazados.

Por lo que respecta a las operaciones de red, lo principal que debe comprender es que cada capa en cada dispositivo habla a su correspondiente capa en el otro dispositivo para administrar un aspecto particular de la conexión de red. En lo concerniente a la interoperabilidad, la clave es la interfaz fija situada entre cada capa. La abstracción por capas reduce lo que de otra forma sería una desalentadora complejidad.

Número de capa	Nombre de la capa	Función
7	Aplicación	Soporta los procesos de la aplicación y del usuario final, proporciona servicios para la transferencia de archivos, correo electrónico y otros servicios del software de redes.
6	Presentación	Formatea los datos para presentarlos en la pantalla o imprimirlos. Algunos ejemplos de protocolos de la capa de presentación son el protocolo ligero de presentación (LPP, Lightweight Presentation Protocol) y el NetBios.
5	Sesión	Establece, administra y termina las conexiones entre las aplicaciones de cada uno de los extremos.
4	Transporte	Asegura que los datos alcanzan su destino intactos y en el orden correcto. El protocolo de control de transmisión (TCP, Transmisión Control Protocol) y el protocolo de datagrama de usuario (UDP, User Datagram Protocol) operan en esta capa.
3	Red	Administra el movimiento de los datos entre diferentes redes. Los protocolos de esta capa son responsables de encontrar el dispositivo al que están destinados los datos. Algunos ejemplos son IP, IPX y AppleTalk.
2	Enlace de Datos	Controla el acceso a la red y asegura la transferencia fiable de tramas sobre la red. La especificación más conocida de enlace de datos es el acceso múltiple sin portadora con detección por colisión de Ethernet. Token Ring y FDDI se adhieren a la arquitectura de enlace de datos por paso de testigo.
1	Física	Controla el medio de transporte mediante la definición de las características eléctricas y mecánicas del medio que lleva la señal. Algunos ejemplos son el cable de par trenzado, el cable de fibra óptica, el cable coaxial y las líneas serie.

Tabla 1.3 Cada una de las capas del modelo OSI dispone de una serie de funciones preestablecidas.

1.4 Protocolos de red

Los protocolos de comunicación definen las reglas para la transmisión y recepción de la información entre los nodos de la red, de modo que si se quieren comunicar entre sí es necesario que ambos empleen la misma configuración de protocolos [Zacker, 2002]., [Heywood, 1999]., [Raya y Raya 2000].

Entre los protocolos propios de una red podemos distinguir dos principales grupos. Por un lado están los protocolos de los niveles físico y de enlace, niveles 1 y 2 del modelo OSI, que definen las funciones asociadas con el uso del medio de transmisión: envió de los datos a nivel de bits y trama, y el modo de acceso de los nodos al medio. Estos protocolos vienen unívocamente determinados por el tipo de red (Ethernet, Token Ring, etc.). El segundo grupo de protocolos se refiere a aquellos que realizan las funciones de los niveles de red y transporte, niveles 3 y 4 del OSI, es decir los que se encargan básicamente del encaminamiento de la información y garantizar una comunicación extremo a extremo libre de errores. Estos protocolos transmiten la información a través de la red en pequeños segmentos llamados paquetes. Si una computadora quiere transmitir un fichero grande a otro, es dividido en paquetes en el origen y vueltos a ensamblar en la computadora destino. Cada protocolo define su propio formato de los paquetes en el que se especifica el origen, destino, longitud y tipo del paquete, así como la información redundante para el control de errores. Los protocolos de los niveles 1 y 2 dependen del tipo de red, mientras que para los niveles 3 y 4 hay diferentes alternativas, siendo TCP/IP la configuración mas extendida. Lo que la convierte en un estándar de facto. Por su parte, los protocolos OSI representan una solución técnica muy potente y flexible.

1.4.1 Ethernet

La versión I de Ethernet fue desarrollada por Xerox Corporation en 1970. Durante la siguiente década, Xerox formó un equipo con Intel y Digital Equipment Corporation (ahora H-P) para sacar la versión 2 en 1982. El protocolo Ethernet proporciona una interfaz unificada al medio de red que permite a un sistema operativo transmitir y recibir varios protocolos del nivel de red de forma simultánea. Al igual que la mayor parte de los protocolos del nivel de enlace que se utilizan en LAN, Ethernet es, en términos técnicos, no orientado a conexión y no fiable[9]. Ethernet realiza todo lo posible para transmitir datos al destino especificado, pero no existe ningún mecanismo que garantice una entrega correcta. En lugar de eso, ciertos servicios, como la entrega garantizada, son responsabilidad de los protocolos que operan en los niveles superiores del modelo OSI, en función de si los datos así lo requieren. Tal como se define en el estándar de Ethernet, el protocolo consta de tres componentes esenciales:

- Una serie de directivas del nivel físico que especifican los tipos de cable (el cable de par trenzado es el más utilizado), limitaciones de cableado y métodos de señalización para las redes Ethernet.

[9] *En este contexto, el término «no fiable» sólo significa que el protocolo carece del mecanismo para confirmar que los paquetes se reciben de forma correcta.*

- Un formato de trama que define el orden y las funciones de los bits transmitidos en un paquete Ethernet.
- Un mecanismo de control de acceso al medio (MAC, Media Access Control) denominado acceso múltiple con detección de portadora y detección de colisiones (CSMA-CD, Carrier Sense Multiple Access with Collision Detection), que permite que todas las computadoras de la LAN dispongan de un acceso similar al medio de red.

Ethernet es el protocolo del nivel de enlace de datos utilizado por la mayor parte de las redes de área local que operan en la actualidad. En el transcurso de más de 20 años se han revisado y actualizado los estándares de Ethernet para admitir muchos tipos de medios de red diferentes y para conseguir grandes mejoras de velocidad respecto al protocolo original. Puesto que todas las variantes de Ethernet trabajan utilizando los mismos principios básicos y que las tecnologías de alta velocidad se han diseñado pensando en su compatibilidad hacia atrás, el paso de una red estándar de 10 Mbps a 100 Mbps o más suele resultar relativamente sencillo.

1.4.2 Token Ring

Token Ring es la alternativa tradicional al protocolo Ethernet en el nivel de enlace de datos. IBM fue el desarrollador original de Token Ring y, posteriormente, se normalizó en el documento 802.5 del Instituto para Ingenieros Eléctricos y Electrónicos (IEEE, Institute for Electrical and Electronics Engineers), por lo que, igual que ocurre con Ethernet, existen estándares del protocolo ligeramente divergentes.

Es una arquitectura abierta basada en el protocolo de paso de estafeta sobre una topología en anillo. Utiliza el sistema de cableado, introducido por IBM[10], que contiene varios tipos de cables metálicos y la fibra óptica. Además permite emplear dos topologías: de estrella y de anillo (véase la Figura 1.13). Los datos se transmiten a una velocidad de 4 Mbps, pudiéndose conectar hasta un máximo de 8 computadores y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (MAU, Multistation Access Unit) si se utiliza con cable coaxial (si se utiliza fibra óptica puede llegar hasta una velocidad de 16 Mbps). No obstante, como se pueden conectar hasta 12 MAU, el número de computadores conectados, y la distancia máxima, pueden aumentar considerablemente.

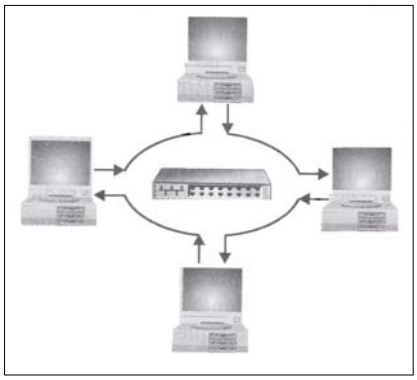


Figura 1.13 Las redes Token Ring dan la impresión de utilizar una Topología en estrella, pero los datos viajan por un anillo.

[10] *Las implementaciones de Token Ring originales utilizan un sistema de cable diseñado por IBM, al cual denominan Tipo 1 o 3, o Sistema de cable de IBM (ICS, IBM Cabling System). El tipo 1 es un cable de pares trenzados apantallados (STP,Shielded Twisted-Pair) de 150 ohmios que contiene dos pares de hilos. El otro sistema de cableado utilizado en redes Token Ring utiliza cable estándar de pares trenzados sin apantallar.*

1.4.3 TCP/IP

Cuando el Departamento de Defensa de los EE UU (DoD) desarrolló el protocolo TCP/IP[11] para la ARPANet, el modelo OSI aún no se había desarrollado, por lo que el modelo usado era ligeramente diferente, y algo más sencillo. Se le llama en ocasiones TCP/IP, pero más frecuentemente se hace referencia a él como el modelo DoD. Consiste en sólo cuatro capas, en comparación con las siete del modelo OSI. Las capas del DoD se pueden relacionar con las del modelo OSI, como se puede ver en la Figura 1.14. Desde su nacimiento, el grupo de protocolos TCP/IP se ha convertido en el estándar de la industria de los protocolos de transferencia de datos para los niveles de red y de transporte del modelo OSI. Además, el grupo incluye muchos otros protocolos que operan a un nivel tan bajo como el nivel de enlace de datos y tan alto como el nivel de aplicación. El elemento principal que diferencia a TCP/IP de los otros grupos de protocolos que proporcionan servicios de los niveles de red y de transporte es su mecanismo de direccionamiento autocontenido. A todo dispositivo de una red TCP/IP se le asigna una dirección del protocolo de Internet (IP, Internet Protocol) que lo identifica de forma única frente a otros sistemas (véase Figura 1.15). La mayor parte de los PC de las redes actuales utilizan adaptadores de interfaz de red Ethernet o Token Ring que disponen de identificadores únicos (direcciones MAC, Media Access Control Address) grabados en su interior, lo que hace que la dirección de IP sea redundante. Sin embargo, otros muchos tipos de computadoras disponen de identificadores asignados por los administradores de red, y no existen ningún mecanismo para garantizar que ningún otro sistema en una red interconectada a escala mundial como Internet utiliza el mismo identificador. Puesto que las direcciones de IP las registra un cuerpo, centralizado, se puede tener la certeza de que no existen dos máquinas en Internet, correctamente configuradas, que posean la misma dirección. Debido a este direccionamiento, los protocolos TCP/IP pueden admitir prácticamente cualquier tipo de plataforma hardware o software que se utilice en la actualidad.

[11] *TCP/IP fue desarrollado en 1972 por el Departamento de Defensa de los Estados Unidos, como parte de un proyecto dirigido por los Ingenieros Robert Kahn y Vint Cerf, para la investigación de tecnología de redes ARPA.*

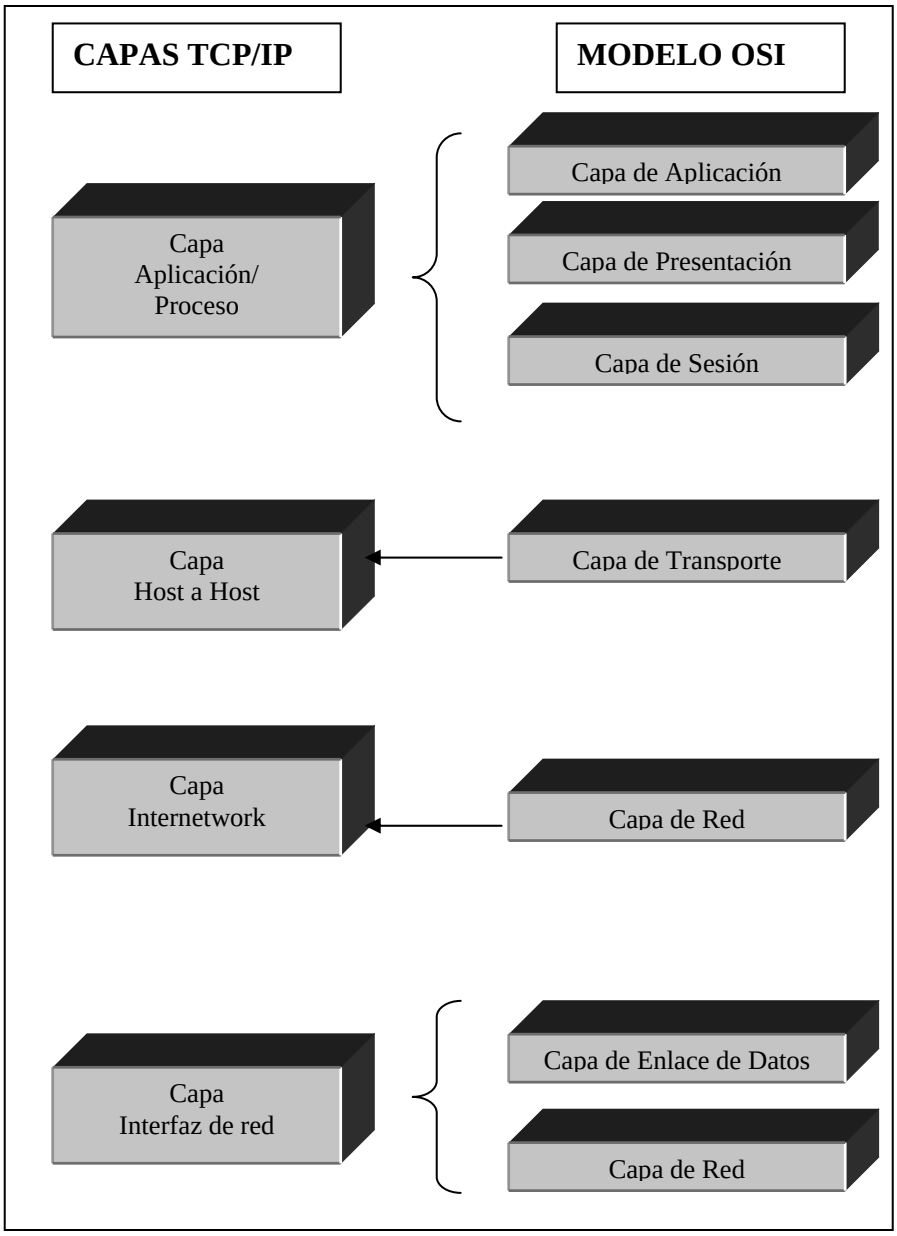
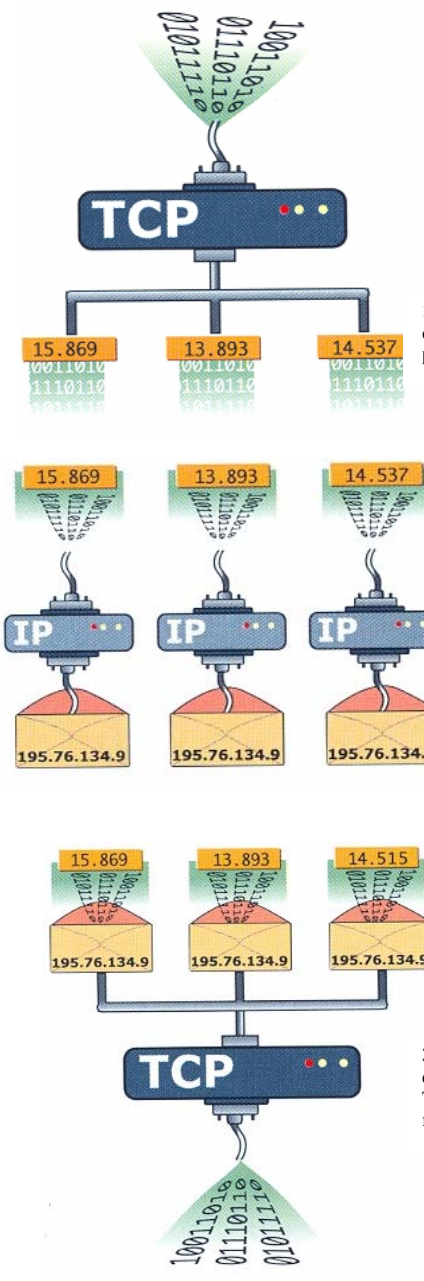


Figura 1.14 Las cuatro capas del modelo DoD se adaptan a las siete capas del modelo OSI.



1.-El protocolo TCP fragmenta el mensaje en paquetes y coloca a cada uno la "etiqueta" que lo identifica como parte de ese mensaje e indica su lugar dentro del mismo.

2.- El protocolo IP "mete en sobres" los paquetes y coloca la dirección del destinatario y el remitente.

3.- Los paquetes son enviados a los ruteadores, computadoras que los irán guiando paso a paso hasta su destino. Al llegar, el TCP reúne y ordena todos los paquetes, y comprueba que no falte ninguno.

Figura 1.15 El protocolo TCP toma los datagramas de cada mensajero y reúne una por una las piezas del mensaje original, las ordena, verifica que no falte ninguna y las entrega al usuario.

1.4.4 Protocolo de NetWare

Novell NetWare se diseñó en una época en que los productos de red propietarios eran habituales. Como resultado, para proporcionar servicios de transporte para el sistema operativo NetWare, Novell creó su propio grupo de protocolos, conocido generalmente por el nombre del protocolo del nivel de red: IPX, o intercambio de paquetes entre redes (Internetwork Packet Exchange). Por similitud con TCP/IP, el grupo se conoce a veces como IPX/SPX, que hace también referencia al protocolo de intercambio secuencial de paquetes (SPX, Sequenced Packet Exchange), que opera en el nivel de transporte. Sin embargo, al contrario de la combinación de TCP/IP, que se ocupa normalmente de gran parte del tráfico de una red, la utilización de la combinación IPX/SPX en una red NetWare es relativamente rara. A medida que se desarrolló la industria de redes, la normalización y la interoperatividad se convirtieron en los elementos más importantes del diseño de productos de red. El aumento de popularidad de los protocolos TCP/IP y del Internet hicieron que la mayoría de los desarrolladores de sistema operativos adoptaran TCP/IP como protocolo predeterminados, si aún no los utilizaban. Sin embargo, los protocolos propietarios de Novell se mantuvieron más tiempo que ningún otro, en detrimento de su cuota de mercado. Hasta la aparición de NetWare 5 en 1998 no se integró TCP/IP en NetWare de forma plena. Los protocolos IPX son similares a TCP/IP en varios aspectos. Ambos grupos de protocolos utilizan un protocolo no orientado a conexión, no fiable en el nivel de red, IPX e IP, respectivamente, para transportar datagramas que contienen la información generada por multitud de protocolos de niveles superiores que proporcionan diversos grados de servicio para diferentes aplicaciones. Al igual que IP, IPX es responsable del direccionamiento de datagramas y su enrutamiento hacia su destino en otras redes.

Sin embargo, los protocolos IPX se diseñaron para utilizarlos en LAN, y no poseen la escalabilidad casi ilimitada de los protocolos de Internet. IPX no dispone de un sistema de direccionamiento autocontenido como IP. Los sistemas de una red NetWare identifican a otros sistemas utilizando la dirección de nodo (también conocida como dirección hardware o firmware) grabada en los adaptadores de red más una dirección de red asignada por el administrador o el sistema operativo durante la instalación.

1.4.5 Protocolo NetBEUI

Aunque TCP/IP se ha convertido en el grupo de protocolos más popular de los que operan en los niveles de red y de transporte del modelo de referencia OSI, aún existen algunas alternativas. NetBEUI, la interfaz extendida de usuario de NetBIOS (NetBIOS Extended User Interface), es uno de los protocolos de red de área local más antiguos que aún se utilizan, y siguen siendo una solución excelente para redes relativamente pequeñas, debido a que necesita menos sobrecarga que otros protocolos más generales. NetBEUI se diseño a mediados de los 80 para proporcionar servicios de transporte de red a programas basados en NetBIOS (Network Basic Input/Output System, Sistema básico de entrada/salida en red).

NetBEUI es un método de transporte de datos de NetBIOS a través de una red. También es posible encapsular la información de NetBIOS utilizando los protocolos TCP/IP o IPX.

Cuando Microsoft comenzó a introducir características de red en sus sistemas operativos, NetBEUI fue su protocolo preferido. Inicialmente, tanto Windows para trabajo en grupo como Windows NT utilizaban NetBEUI como protocolos predeterminados. Sólo más tarde siguió Microsoft la estela del resto de la industria de red y comenzó a confiar en TCP/IP para transportar datos de NetBIOS.

En nuestros días NetBEUI se utiliza habitualmente en pequeñas redes de Microsoft Windows, debido a que proporciona un buen rendimiento, requiere muy poco mantenimiento, ya que el protocolo es autoconfigurable y autoajustable, y utiliza una cantidad relativamente pequeña de memoria. El principal inconveniente de NetBEUI es que no es enrutable y sólo debería utilizarse en redes que dispongan de un único dominio de colisiones. Esto se debe a que el protocolo se basa en las transmisiones de difusión para algunas de sus funciones esenciales y no tiene forma de identificarse la red en la que se encuentra un sistema.

1.4.6 Protocolo NetBIOS

NetBIOS se diseñó para proporcionar una interfaz de programación normalizada entre las aplicaciones software y el hardware de red, de forma que las aplicaciones pudieran portarse entre sistemas con mayor facilidad. La interfaz incluye un espacio de nombres, que aún utilizan todos los sistemas operativos de Microsoft, excepto Windows 2000, para identificar las computadoras de la red.

El nombre que se asigna a una computadora Windows durante la instalación del sistema operativo es, de hecho, un nombre de NetBIOS, como los nombres de dominios y grupos de trabajo. El espacio de nombres de NetBIOS realiza la misma función que las direcciones IP utilizadas por el grupo de protocolos TCP/IP y las direcciones de red y de nodo utilizadas por los protocolos IPX/SPX. Los nombres de NetBIOS proporcionan un identificador único para cada una de las computadoras de la red, de forma que los sistemas pueden enviar transmisiones de unienvío directamente a otros sistemas. Por este motivo, los nombres de los sistemas individuales se conocen como nombres únicos, mientras que los nombres de NetBIOS que representa una colección de sistemas para multidifusión, se denomina nombres de grupo.

1.5 Servicios de red

Para obtener todas las ventajas que supone el uso de una red, se deben tener instalados una serie de servicios de red, tales como, acceso, ficheros, impresión e información (véase Figura 1.16).

Los *servicios de acceso* se encargan tanto de verificar la identidad del usuario (para asegurar que sólo pueda acceder a los recursos para los que tiene permiso) como de permitir la conexión de usuarios a la red desde lugares remotos.

El *servicio de ficheros* consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

La *utilidad de impresión* permite compartir impresoras entre varias computadoras de la red, lo cual evitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costos. Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.

Los *servidores de información* pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto.

En el campo de la comunicación entre usuarios existen una serie de servicios que merece la pena comentar. El más antiguo y popular es el correo electrónico (e-mail) que permite la comunicación entre los usuarios a través de mensajes escritos.

Los mensajes se enviarán y se recuperarán usando un equipo servidor de correo. Resulta mucho más barato, económico y fiable que el correo convencional. Además, tenemos los servicios de conferencia (tanto escrita, como por voz y vídeo) que permitirán a dos o más usuarios de la red comunicarse directamente (on-line).

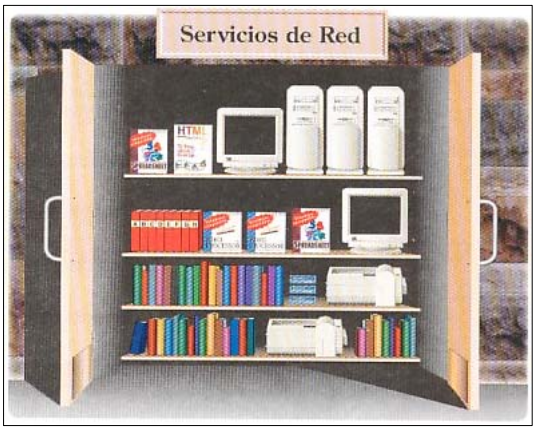


Figura. 1.16 Ejemplo de los servicios de red.

1.6 Perspectiva histórica de la seguridad en redes

A través de toda la historia, la necesidad del hombre de asegurar y proteger su propia tierra, recursos y objetos valiosos de ladrones, intrusos y otros «indeseables» sigue siendo actual. Tanto si son muros, castillos, puertas, cercas o cajas de seguridad metálicas lo que mantiene a salvo y seguro lo que es suyo, sigue siendo un reto continuo mantener la seguridad de sus bienes. Cuando esto se asocia a los sistemas de computadoras, equipos y datos, esta necesidad de seguridad es tan grande o quizás incluso mayor. Esto se debe al hecho de que se depende fuertemente de la información, donde una pérdida de los servicios informáticos, o de los datos y registros de una empresa, podría dañar gravemente, o incluso arruinar, un negocio.

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios, y por empleados corporativos para compartir impresoras. Posteriormente la seguridad fue enfocada al control de acceso físico y administrativo, ya que para acceder a un computador se requería la presencia del usuario frente al sistema. Un ejemplo es el uso de archiveros sólidos con una cerradura de combinación para almacenar documentos delicados. Posteriormente comienzan a proliferar los sistemas multiusuario en los cuales un recurso computacional era compartido por varios individuos, surgen nuevos riesgos como la utilización del sistema por personas no autorizadas, manipulación de información o aplicaciones por suplantación de usuarios, aparece un primer esquema de protección basado en códigos de usuarios y contraseñas (password)[12] para restringir el acceso al sistema, además se establecen distintas categorías de control de acceso a los recursos.

Siguen evolucionando los sistemas y se inicia la computación en red, en la cual además de los riesgos asociados a los sistemas multiusuarios, aparece un nuevo tipo de vulnerabilidad, básicamente en el proceso de transmisión de la información; también estaban expuestas a los posibles atacantes internos. La evolución tecnológica continúa y comienza el proceso de interconexión de las distintas redes aisladas de una empresa para configurar los equipos corporativos, donde aumentan considerablemente las amenazas.

Hoy en día estamos conectando nuestras redes empresariales a Internet, en donde la protección se ha convertido en un problema realmente serio. Proveer de la suficiente garantía y confiabilidad, es la meta de la seguridad informática.

[12] *La famosa password o palabra de paso, por así decir, es la hermana menor de las medidas de seguridad que propician la identificación del usuario y la implantación de controles de acceso en los sistemas aislados.*

1.7 ¿Por qué es necesaria la seguridad en las redes?

Se ha establecido un consenso bastante generalizado acerca de la necesidad de proteger las redes contra usos indebidos (véase Figura 1.17). Desde el principio, los sistemas informáticos han presentado una vulnerabilidad muy significativa que ha hecho necesaria la adopción de medidas para evitar actuaciones incorrectas.

La más llamativa de ellas, la que primero se tuvo en consideración, fue el *control de acceso.* Obviando hacer referencia aquí a las prevenciones de seguridad física basadas en vigilantes especiales y en la limitación de acceso a determinados locales, cuando se tenían máquinas en las cuales podían trabajar simultáneamente más de una persona (los típicos centros de cálculo), lo primero que se pensó fue en crear mecanismos que sirvieran para que los usuarios tuvieran otorgados ciertos privilegios y solamente en base a esos privilegios pudieran hacer cosas en la máquina. Cuando aparecen las redes surge un fenómeno nuevo: los gestores de las máquinas empiezan a no tener un control directo sobre el sistema en su conjunto: las redes propician una suerte de *evasión* a este control. El caso más sencillo puede estar constituido por una red de área local que se extienda a lo largo de un edificio. Si existe información sensible en los servidores de esta red (por ejemplo calificaciones de alumnos en una institución universitaria) se corre el peligro de que cualquiera que tenga la habilidad suficiente puede "colgarse" en algunos de los muchos cables de interconexión y, si las medidas de protección no son las adecuadas, pueda tener acceso a su contenido o, incluso, a su modificación. Situaciones que en sistemas aislados podrían afrontarse con medidas sencillas de tipo físico (por ejemplo, vigilancia) resultan ahora mucho más difíciles de resolver.

Si, además, no se trata sólo de redes locales sino de redes públicas de área extensa, por ejemplo redes IP o X.25, donde la información sensible atraviesa una red en la que el gestor de los sistemas de una determinada organización no manda, es decir, no tiene capacidad de actuar, cuando esto ocurre, las dudas y las sospechas y los temores sobre actuaciones indebidas aumentan (no digamos ya cuando se trata de múltiples redes interconectadas, como es el caso de Internet). El riesgo de aparición de intrusos es grande y difícil de prevenir porque el usuario de estas redes desconoce casi todo respecto a su estructura, ubicación de nodos, vías de interconexión, etc.

Por todo ello, podemos aseverar que la cuestión de la seguridad es en las redes mucho más importante que en los sistemas informáticos aislados, debido a su mayor vulnerabilidad.

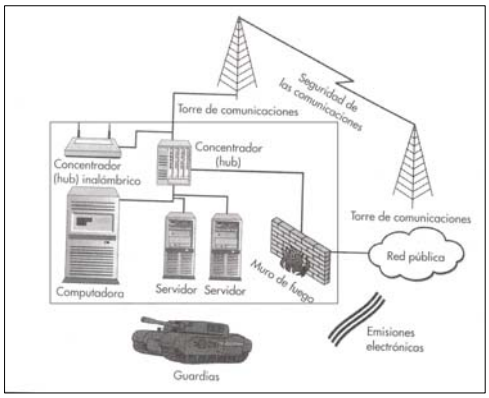


Figura 1.17 La protección de la información incluye muchos conceptos de seguridad.

1.8 ¿Qué es la seguridad en redes?

El término *seguridad de redes* abarca una increíble gama de servicios, procesos y requisitos para una organización. De manera más específica **la seguridad de una red** se define como el resguardo apropiado de todos los componentes asociados con una red, incluidos datos, medios e infraestructura [Brown, 2001]. Existen una serie de compromisos básicos sobre la seguridad en los sistemas de redes:

- *No dificultar las labores de los usuarios*. El propósito de la seguridad es la protección de recursos considerados importantes dentro de la organización donde el sistema de seguridad está activo. En ocasiones lleva consigo ciertas imposiciones a los usuarios de los recursos. Deben ser siempre aceptables y no ser una carga excesivamente grande.
- *Se deben especificar claramente las responsabilidades en seguridad*. Para asegurarse que los objetivos de la gestión se lleven a cabo, es necesario que se asignen responsabilidades de forma precisa. Los grupos a los que se le asignan estas tareas suelen ser los gestores de protección, operadores del sistema, gestores de las aplicaciones, el encargado de la seguridad física, la oficina de recuperación de desastres, los usuarios, y los responsables de los informes de supervisión.
- *La seguridad requiere una estructuración clara*. La eficacia de la protección precisa que distintos grupos y áreas dentro y fuera de la organización colaboren. La arquitectura o programa de seguridad se suele dividir en bloques que se denominan controles (técnicos y de operación). Para que la gestión de seguridad sea la óptima hay que conocer esta estructuración y la interacción entre cada uno de ellos.
- *La protección del sistema debe tener un costo soportable*. Los gastos y los beneficios de la seguridad del sistema deben ser examinados cuidadosamente, para que el primero no sobrepase al segundo. Hay que tener en cuenta que una inversión en seguridad puede suponer disminuir el número de pérdidas debido a fallos del sistema o por manipulación fraudulenta de los recursos. Los beneficios de la seguridad no son sólo monetarios.

1.9 Objetivo de la seguridad

La labor principal de la seguridad es el aislamiento de los actos no deseables, y la prevención de aquellos que no se hayan considerado, de forma que si se producen hagan el menor daño posible [Milenkovic, 1988]. Entre los principales objetivos de la seguridad están:

- Identificación de los usuarios.
- Detección de intrusos en la red.
- Análisis de riesgos.
- Clasificación apropiada de los datos.
- Control de las nuevas aplicaciones.
- Análisis de los accesos de los usuarios.

1.10 Principios fundamentales de la seguridad

En el ámbito de la seguridad informática existen una serie de principios básicos que se deben tener en cuenta al diseñar cualquier política de seguridad. A continuación se exponen los siguientes principios:

- **Principio de menor privilegio.** Este es quizás el principio más fundamental de la seguridad. Cada sujeto (usuario, administrador, programa, sistema, etc.) debería tener permitido el acceso únicamente a la información esencial necesaria para completar las tareas que el sujeto está autorizado a realizar y ninguno más. Hay que tener cuidado con este principio, ya que es necesario hacer un buen análisis para determinar efectivamente cuales son los privilegios que se necesitan para llevar a cabo una tarea. Se puede correr el riesgo de dar menos del privilegio mínimo que se necesita. Intentar cumplir con el menor privilegio con las personas, en lugar de programas, puede ser bastante peligroso, los seres humanos son menos predecibles y es más fácil que se molesten y sean una amenaza si no pueden hacer lo que quieren.
- **Principio del eslabón más débil.** Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil. El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque, aprovechando los puntos débiles o vulnerabilidades. Por ejemplo, supóngase que se establece una política de asignación de passwords muy segura, en la que éstos se asignan automáticamente, son aleatorios y se cambian cada semana. Si el sistema utiliza la red y no se protege la conexión, no servirá de nada la política de passwords establecidas (por defecto los passwords circulan descifrados). Si cualquiera puede acceder a la red y revisar todos los paquetes que circulan por la misma, es trivial que pueda conocer los passwords. En este punto débil sería la red, por mucho que se haya reforzado la seguridad en otros puntos, altamente vulnerable.

- **La Seguridad no se obtiene a través de la oscuridad**. El hecho de mantener posibles errores o debilidades en secreto, no evita que existan. Tampoco no se trata de hacer público un nuevo fallo del sistema o un método para romperlo. En primer lugar hay que intentar resolverlo, eliminar la vulnerabilidad y luego publicar el método de protección.
- **Defensa en profundidad.** La seguridad del sistema no debe depender de un solo mecanismo por muy fuerte que este sea, sino que es necesario establecer varios mecanismos sucesivos. De este modo cualquier atacante tendrá que superar varias barreras para acceder al sistema. Por ejemplo, se puede establecer un mecanismo de passwords altamente seguro como primera barrera de seguridad. Adicionalmente es posible utilizar algún método criptográfico fuerte para cifrar la información almacenada. De este modo cualquier atacante que consiga averiguar el password y atravesar la primera barrera, se encontrará con la información cifrada y se podrá seguir manteniendo la confidencialidad de la misma.
- **Punto de control centralizado**. Se trata de establecer un único punto de acceso al sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un solo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema. Este único canal de entrada simplifica el sistema de defensa, puesto que permite concentrarse en un único punto. Además permite monitorear todos los accesos o acciones sospechosas.
- **Seguridad en caso de fallo.** Este principio afirma que en caso de que cualquier mecanismo de seguridad falle, el sistema debe quedar en un estado seguro. Por ejemplo, si los mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario a que dejen pasar a cualquier aunque no esté autorizado. Algunos ejemplos de la vida cotidiana respecto a este concepto serían: cuando hay un corte de energía eléctrica, los ascensores están preparados para bloquearse mediante algún sistema de agarre, mientras que las puertas automáticas están diseñadas para poder abrirse y no quedar bloqueadas.
- **Participación universal.** Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que se establezca puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo. La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.
- **Simplicidad**. La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite

esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

1.11 Servicios de seguridad

La necesidad de normalizar el diseño de sistemas en las redes de comunicación, llevó a la ISO a definir un conjunto de **servicios o funciones básicas** que mejoran la seguridad, y los métodos o mecanismos que permiten realizar dichas funciones.

La recomendación X.800 define un servicio de seguridad como un servicio proporcionado por una capa de protocolo de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas o de las transferencias de datos. Quizás es más clara la definición recogida en RFC 2828: un servicio de procesamiento o de comunicación proporcionado por un sistema para dar un tipo especial de protección a los recursos del sistema; los servicios de seguridad implementan políticas de seguridad y son implementados, a su vez, por mecanismos de seguridad.

Se definen cinco servicios básicos de seguridad: Autenticación, Confidencialidad, Integridad, Control de Acceso y No repudio [Carracedo, 2004] y [Maiwald, 2004]., y quedan divididos en cinco categorías[13] y 14 servicios específicos (véase Tabla 1.4). Asimismo, se ha establecido la asignación de los servicios de seguridad en cada nivel del modelo OSI (véase Figura 1.18).

[13] No existe un acuerdo universal sobre la gran cantidad de términos que se emplean en la literatura sobre seguridad. Por ejemplo, el término integridad se usa a veces para referirse a todos los aspectos de la seguridad de la información. El término autentificación se usa con frecuencia para hacer alusión tanto a la verificación de la identidad como a las diferentes funciones que aparecen referidas a integridad en este capítulo.

SERVICIOS DE SEGURIDAD

AUTENTIFICACIÓN

Autentificación de las entidades origen / destino
Empleada conjuntamente con una conexión lógica para aportar confianza sobre la identidad de las entidades conectadas.

Autentificación del origen de los datos
En transferencias no orientadas a la conexión, garantiza que la fuente de los datos recibidos es la que dice ser.

INTEGRIDAD DE LOS DATOS

Integridad de la conexión con recuperación
Proporciona la integridad de los datos de todos los usuarios en una conexión y detecta cualquier modificación, inserción, omisión o repetición de cualquier dato de una secuencia completa de datos, con intento de recuperación.

Integridad de la conexión sin recuperación
Igual que el anterior, pero proporciona sólo detección sin recuperación.

Integridad de la conexión de campos seleccionados
Proporciona la integridad de los campos seleccionados en los datos del usuario del bloque de datos transferido por una conexión y determina si los campos seleccionados han sido modificados, insertados, suprimidos o repetidos.

Integridad no orientada a la conexión
Proporciona integridad de un bloque de datos sin conexión y puede detectar la alteración de datos. Además, puede proporcionar una forma limitada de detección de repetición.

Integridad no orientada a la conexión de campos seleccionados
Proporciona la integridad de los campos seleccionados en un bloque de datos sin conexión; determina si los campos seleccionados han sido modificados.

CONFIDENCIALIDAD DE LOS DATOS

Confidencialidad de la conexión
La protección de los datos de todos los usuarios en una conexión.

Confidencialidad no orientada a la conexión
La protección de los datos de todos los usuarios en un único bloque de datos.

Confidencialidad de campos seleccionados
La confidencialidad de campos seleccionados en los datos del usuario en una conexión o en único bloque de datos.

Confidencialidad del flujo de tráfico
La protección de la información que podría extraerse a partir de la observación del flujo del tráfico.

NO REPUDIO

No repudio, origen
Prueba que el mensaje fue enviado por la parte especificada.

No repudio, destino
Prueba que el mensaje fue recibido por la parte especificada.

CONTROL DE ACCESO

La prevención del uso no autorizado de una fuente (este servicio controla quién puede tener acceso a una fuente, en qué condiciones se puede producir el acceso y qué tienen permitido los que acceden a la fuente).

Tabla 1.4 Clases de servicios de seguridad (X.800).

Hay quienes consideran un sexto servicio básico: Disponibilidad (Availability). Hace referencia a la protección que es necesario introducir para que las distintas partes del sistema que componen la red estén disponibles para ser utilizadas por quienes dispongan de autorización para ello. Podríamos considerar que esto no constituye realmente un servicio telemático (provisto por un protocolo), sino más bien es un conjunto de facilidades y medidas de seguridad que sirven para contrarrestar, en parte, los ataques de denegación de servicio.

Además de estos servicios clásicos que se definieron a finales de la década de los ochenta, y debido a los requisitos que exigen algunos de los nuevos servicios telemáticos que están actualmente siendo vislumbrados (aunque aún escasamente implantados) cabe hablar de un nuevo servicio de seguridad en las redes informáticas: Anonimato.

A continuación se comentan particularizadamente cada uno de estos servicios de seguridad.

	Niveles						
Tipo de servicio	**1**	**2**	**3**	**4**	**5**	**6**	**7***
Autenticación de entidad par.	-	-	S	S	-	-	S
Autenticación del origen de los datos.	-	-	S	S	-	-	S
Control de acceso.	-	-	S	S	-	-	S
Confidencialidad (en servicio orientado a la conexión).	S	S	S	S	-	S	S
Confidencialidad (en servicio no orientado a la conexión).	-	S	S	S	-	S	S
Confidencialidad en campos seleccionados.	-	-	-	-	-	S	S
Confidencialidad en flujo de tráfico.	S	-	S	-	-	-	S
Integridad (en servicio orientado a la conexión con recuperación de errores).	-	-	-	S	-	-	S
Integridad (en servicio orientado a la conexión sin recuperación de errores).	-	-	S	S	-	-	S
Integridad en campos seleccionados (en servicio orientado a la conexión).	-	-	-	-	-	-	S
Integridad (servicio no orientado a la conexión).	-	-	S	S	-	-	S
Integridad en campos seleccionados (servicio no orientado a la conexión).	-	-	-	-	-	-	S
No - Repudio de origen.	-	-	-	-	-	-	S
No - Repudio de entrega.	-	-	-	-	-	-	S

S Significa que sí debe ser incorporado este servicio como una opción en los estándares del nivel.

- Significa que no debe proveerse el servicio.

* Cabe señalar que (respecto al nivel 7) los procesos de aplicación pueden, por sí mismos, proporcionar servicios de seguridad.

Figura 1.18 Relación entre niveles y servicios de seguridad en la arquitectura OSI.

1.11.1 Servicio de autenticación

El Servicio de Autenticación (Authentication) sirve para garantizar que una entidad comunicante (una persona o una máquina) es quien dice ser (véase Figura 1.19). Este servicio protege contra un ataque muy fácilmente perpetrable en las redes: *la suplantación de personalidad* (masquerade) mediante el cual una entidad remota se hace pasar por quien no es. Puede tratarse de autenticación de entidad simple, en cuyo caso sólo uno de los participantes en la comunicación (puede ser tanto la entidad origen de los datos como la entidad destino) está obligado a demostrar su identidad.

Un ejemplo de ello puede ser el acceso a un servidor remoto que contenga una base de datos que almacene información por cuyo consumo el cliente debe pagar. Previo a autorizarle el acceso y anotarle el correspondiente cargo, si el protocolo de acceso tiene implementado el servicio de autentificación, se garantiza a los gestores del servidor que el usuario que está tratando de acceder a la base de datos es la persona o entidad que proclama ser. En este mismo ejemplo puede darse el caso de que también el cliente quiera estar seguro de que el servidor al que se ha conectado es el auténtico y no una suplantación maliciosa. En este caso se requeriría un servicio de autenticación mutua mediante el cual la operación de aseguramiento de la identidad de las entidades se realiza en ambos sentidos de la comunicación.

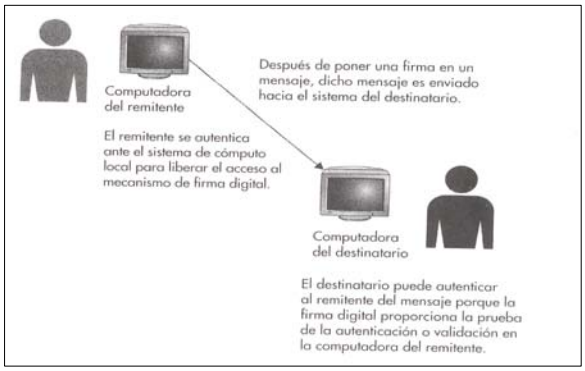


Figura 1.19 Mecanismo de autenticación.

Podrían distinguirse en este servicio dos clases, una de las cuales es la autentificación débil y está apoyada en el uso más o menos sofisticado de palabras de paso (passwords) o de identificadores, mientras que cuando el resultado es más eficaz la denominamos autentificación fuerte (Strong Authentication), que requiere del intercambio de mensajes cifrados y, posiblemente, del concurso de una tercera parte de confianza (TTP, Trusted Tirad Party). **Las tarjetas inteligentes** (véase Figura 1.20) representan un componente de seguridad importantísimo de cara a la implantación tanto del servicio de autenticación como de otros servicios de seguridad.

Figura 1.20 Ejemplo de una tarjeta inteligente.

1.11.2 Servicio de confidencialidad de los datos

Este servicio (Data Confidentiality) proporciona protección para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado. Es decir, garantiza que los datos tan sólo van a ser entendibles por el destinatario o destinatarios del mensaje (véase Figura 1.21).

En función del contenido de una transmisión de datos, existen diferentes niveles de protección. El servicio más amplio protege los datos de los usuarios que se han transmitido por conexión TCP. Se pueden distinguir formas más específicas de este servicio, incluyendo la protección de un solo mensaje o incluso de determinados campos de un mensaje. Estos refinamientos son menos útiles que el enfoque amplio y su implementación puede incluso ser más compleja y costosa.

El otro aspecto de la confidencialidad es la protección del flujo del tráfico frente al análisis del tráfico. Para ello el atacante no debería poder ver la fuente, el destino, la frecuencia, la longitud ni otras características del tráfico en una comunicación.

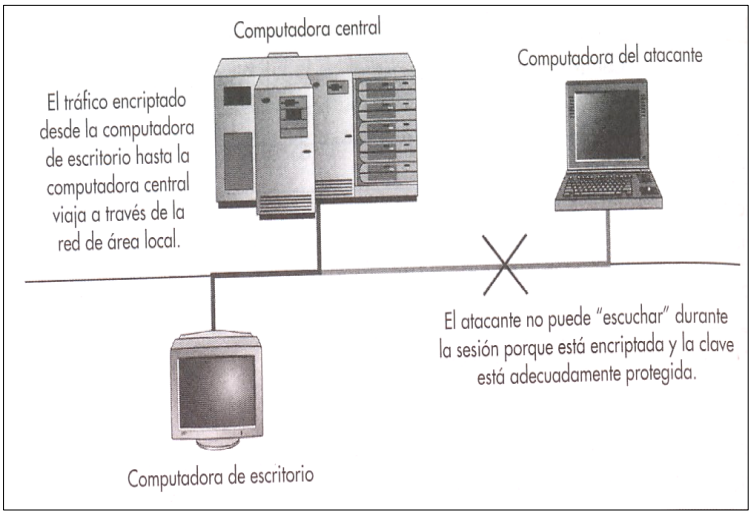


Figura 1.21 Ejemplo de la confidencialidad de datos.

1.11.3 Servicio de integridad de los datos

El Servicio de Integridad de los datos (Data Integrity) garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor de los mismos, de tal forma que puede tener garantías de que a la información original no le ha sido añadida, ni modificada, ni sustraída alguna de sus partes. Es decir, el receptor de la información (o proveedor del servicio) detectará si se ha producido o no un ataque de modificación del mensaje, lo que le permitirá rechazar o dar por buenos los datos recibidos. No es necesario remarcar la importancia que tiene este servicio para una adecuada expansión de los servicios telemáticos. En los procedimientos ordinarios de intercambio de información mediante papel u otros soportes

convencionales no ha resultado muy difícil para los falsificadores alterar mediante sustituciones el contenido de un mensaje. Pero se requiere bastante habilidad para llevarlo a cabo sin que se note el fraude. Además, las posibilidades de sustitución que tiene el falsificador están muy limitadas por el formato del documento: puede sustituir una palabra o una frase por otra de similar tamaño, pero no puede insertar párrafos demasiados grandes sin alterar sustancialmente la estructura del documento. Estas dificultades hacen que los usuarios ante, por ejemplo, un papel firmado no teman en exceso este tipo de ataques.

No obstante, cuando se trata de mensajes o datos en soporte electrónico, las posibilidades de hacer modificaciones sin dejar huella están al alcance de cualquiera, por ejemplo, en que alguien quiera presentar ante un organismo cualquiera, como elemento probatorio, un mensaje de correo impreso en el que se respalde cualquier circunstancia favorable a quien lo presenta. Resulta evidente que si no presenta una prueba robusta (por lo general será una prueba criptográfica) de la integridad del mensaje, nadie en su sano juicio va a aceptar ese mensaje como una prueba válida (cualquiera puede redactar e imprimir lo que le parezca oportuno y darle el formato que tendría un mensaje de correo). Por todo ello, resulta absolutamente imprescindible la provisión del servicio de integridad cuando se trata de intercambiar mensajes, con cierta garantía, a través de redes informáticas.

1.11.4 Servicio de no repudio

Son las funciones que impiden a una entidad emisora negarse a reconocer un envío validamente efectuado, y a una entidad receptora negar la aceptación de una entrega realizada correctamente. Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió. Podríamos distinguir tres situaciones (véase Figura 1.22):

- **No repudio con prueba de origen.** En este caso, el receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos. En muchos casos pueden bastar las garantías que el emisor introduce en el mensaje cuando aplica los mecanismos que aseguran la autenticación del origen de los datos. En otros casos pueden requerirse evidencias acerca de la relación existente entre el autor de un determinado mensaje y la entidad que procede a enviarlo a través de la red. Por ejemplo, en que alguien escriba y firme una carta vejatoria hacia otra persona pero que no se atreve a enviársela por correo postal. Si un tercero localiza ese escrito y lo pone en el correo, el receptor tendrá pruebas demostrables de quién es el autor de la carta, pero no de que además de escribirla ha sido él quien ha tomado la decisión ofensiva de enviársela.
- **No repudio con prueba de envío.** El receptor o el emisor del mensaje adquieren una prueba, demostrable ante terceros, de la fecha y hora en que el mensaje fue enviado. Este servicio trata de emular al que frecuentemente presta el servicio postal cuando al entregar una carta certificada en la estafeta se solicita que una copia del documento que se quiere enviar sea sellada con una

marca de tiempo precisa, de tal manera que pueda servir posteriormente como prueba ante determinados actos administrativos que requieren que, por ejemplo, una solicitud sea entregada antes de una fecha concreta bien en el registro de entrada de la oficina de destino o bien en una dependencia de correos.

- **No repudio con prueba de entrega**. El emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado. Como ejemplo, este servicio equivaldría al envío de cartas con acuse de recibo. En estos dos últimos ejemplos, correos se comporta como una entidad intermediaria entre el emisor y el receptor, lo que traducido al mundo de las redes significa que para implantar ese servicio es necesaria alguna entidad que actúe como una TTP. Esto equivale a decir que para este servicio pueda ser provisto es necesario que exista, en alguna medida, una *infraestructura de seguridad* que haga de garante y proporcione las evidencias exigidas.

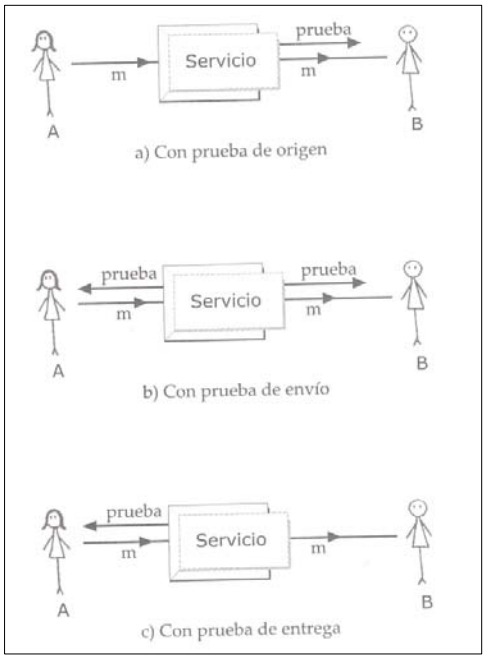


Figura 1.22 Tres casos de no repudio.

1.11.5 Servicio de control de acceso

Este servicio (Access Control) sirve para evitar el uso no autorizado de los recursos de la red. Puede servir para permitir que sólo quien esté autorizado para ello pueda conectarse a una determinada máquina, y para que, una vez conectado, cada usuario sólo pueda tener acceso a aquellas facilidades para las que ha adquirido permisos. De forma resumida, podríamos decir que este servicio permite especificar quién puede hacer qué, es decir, qué usuarios pueden hacer determinadas operaciones[14]. En las redes telemáticas se puede presentar la necesidad de disponer de un servicio de control de acceso en dos situaciones distintas. Éstas son:

- El acceso remoto a servidores de todo tipo como bases de datos, impresoras, servidores de correo, etc. El usuario accede regularmente bajo una arquitectura cliente-servidor y, tras identificarse, los mecanismos en que se apoya el servicio determinan a qué partes del servicio se les concede acceso.

[14] En realidad, este servicio no es privativo de las redes, sino que ya estaba implantado en los accesos a ordenadores aislados instalados en los centros de cálculo, en los que en función del login se permitía a acceder a determinados procesadores o programas.

- El acceso a los terminales desde los que el usuario se conecta a la red. Ellos pueden incluir desde ordenadores protegidos a tarjetas inteligentes. Con frecuencia son estos puntos externos de las redes los que necesitan ser protegidos de forma más estricta, mientras que en otros casos se permite el acceso desde cualquier terminal y los controles se centran solamente en el servidor accedido.

En la mayoría de los casos este servicio se implementa íntimamente ligado a la provisión previa de un servicio de autentificación. Una vez que el usuario ha demostrado que es quien dice ser se le aplican las restricciones o permisos correspondientes. No obstante, se dan otras circunstancias en las que el control de acceso se lleva a cabo mediante *credenciales*, esto es, piezas de información que representan una serie de privilegios a quien las porte, independientemente de su identidad. Un ejemplo en el mundo real (esto no quiere decir que el mundo de las Comunicaciones mediante ordenador no lo sea) puede ser un boleto de entrada para acceder a una butaca concreta de una sala de cine: el privilegio se adquiere al comprarla y su aplicación efectiva no depende de la identidad del portador. En cuanto al grado de implantación de este servicio, cabe decir que, desafortunadamente, con demasiada frecuencia el control se limita a decir sí o no al intento de acceso al recurso, sin mayores detalles posteriores. Cuando se trata, por ejemplo, del acceso a una base de datos plural y compleja, una adecuada implementación debería ofrecer un acceso muy pormenorizado, regulando categorías de usuarios y de actuaciones (no puede ser lo mismo tener derecho a leer información que tener derecho a insertar o modificar datos).

También con demasiada frecuencia el control de acceso se aplica a través de mecanismos de autentificación muy débiles, como puede ser una palabra de paso (password) o un PIN (número de identificación personal). En otros casos se emplean mecanismos criptográficos robustos que aportan la necesaria seguridad en la protección del acceso.

1.11.6 Servicio de anonimato

Se trata de conseguir que la identidad de la persona que realiza una determinada operación informática permanezca oculta ante algunos de los actores presentes en esa operación. Se trata de emular en la red situaciones de la vida real (si se puede seguir haciendo esta distinción por mucho tiempo) en las cuales es conveniente mantener cierto anonimato. Si dentro del correo postal es posible enviar cartas de forma anónima, también el correo electrónico debe permitir esa posibilidad [Carracedo, 2004].

Veamos también otros casos en los que este tipo de requisitos se presentan. En primer lugar, supongamos, un buzón de sugerencias o de quejas dispuesto para que estas sean depositadas en él de forma anónima. Otro caso parecido sería la realización de encuestas anónimas a un grupo de alumnos. Si estas tareas queremos llevarlas a cabo por vía telemática (ello sería cómodo, ágil y eficaz) sería necesario que el agente telemático que recibiese los mensajes no fuese capaz de relacionar las opiniones vertidas con los autores de las mismas. En el primero de los dos ejemplos podría permitirse que fuese cualquier persona quien depositase sus quejas en el buzón, y que formulase más de una. Pero en el segundo de ellos sería necesario autentificar

primero al alumno (sólo un grupo de ellos puede opinar) y garantizar después que no se conocerá cuál ha sido su opinión. Esta misma complejidad (tener que combinar la autentificación de los actores y el mantenimiento del anonimato en relación con los datos que han sido depositados) se produce también en el voto telemático en su acepción de esquema evolucionado del voto electrónico. En la proyección telemática del escenario de votación convencional habrá que garantizar que solamente depositan su voto en la urna las personas autorizadas para ello y que sólo votan una vez y por una sola opción. Por supuesto, debe permanecer oculto quiénes fueron los que votaron cada una de las opciones. Además, el votante debe disponer de mecanismos que le permitan comprobar que su voto ha sido contabilizado adecuadamente en la opción que eligió.

Otro caso interesante es el del dinero digital. Es latoso tener que llevar dinero en los bolsillos, pero tiene una enorme ventaja: podemos comprar de forma anónima. Por ello, el dinero digital mediante el que se compre a través de la red deberá ser también anónimo, cosa que no ocurre en la actualidad en las operaciones de *Comercio Electrónico*. En las tarjetas de crédito convencionales es cómodo y eficaz, pero permite que se creen registros en los que se relacione qué compramos, cuándo y dónde. Sería necesario que el uso de tarjetas de crédito estuviera dotado no sólo de confidencialidad, sino además protegido con servicios de anonimato, de forma que el banco sepa cuánto dinero se ha gastado, pero no dónde ni en qué, y el vendedor tenga certeza de que cobra el importe, pero no tenga capacidad para saber de quién.

CAPÍTULO II

RIESGOS Y DIRECTRICES DE PROTECCIÓN

El objetivo global que se pretende cubrir con este capítulo es completar la panorámica de seguridad en redes informáticas iniciada en el Capítulo I. Si bien esa visión panorámica ha estado centrada en la descripción resumida de los principales conceptos de las redes y su protección, en el presente capítulo detendremos nuestra atención en alguno de los componentes o conceptos a los que ya se había hecho referencia allí: el estudio de los mecanismos y de los servicios de seguridad. Así, trataremos de aclarar en qué consiste un dominio de seguridad y un escenario de comunicación seguro, así como los pasos que es necesario dar para averiguar cuáles son los riesgos y las amenazas contra los que es necesario prevenirse, para poder determinar posteriormente cuáles son las salvaguardas y protecciones que es necesario introducir en ese entorno de comunicación.

2.1 Análisis de amenazas a los sistemas de redes

Desde los comienzos de la computación, los sistemas informáticos (comunicación de datos, redes, la proliferación de las computadoras personales, el software de telecomunicaciones, los sitios Web y el correo electrónico) han estado expuestos a una serie de peligros o riesgos que han aumentado conforme se globalizan más las comunicaciones entre ellos. Aquí mencionamos algunas de las motivaciones más habituales de los ataques [Merike, 1995]:

- **Envidia.** El intruso es contratado por alguien para que acceda fraudulentamente a una red corporativa para apropiarse o alterar información muy valiosa.
- **Jactancia.** El intruso está aburrido, es un experto en computación y trata de obtener acceso a los sitios interesantes.
- **Notoriedad.** El intruso es muy experto y trata de acceder a áreas de probada dificultad de acceso para demostrar su habilidad. El éxito de un ataque puede proporcionar al intruso el respeto y la aceptación de sus iguales.
- **Venganza.** El intruso ha sido cesado, degradado o tratado de forma injusta. El ataque más habitual de este tipo suele suponer la destrucción de información valiosa o la interrupción de los servicios.
- **Ignorancia.** El intruso está aprendiendo acerca de la computación y las redes y tropieza con un punto débil, causando daños al destruir datos o realizar un acto ilegal.

Y es que actualmente, existe una dependencia cada vez mayor de las redes de computación para las transacciones comerciales. Con el libre flujo de información y la gran disponibilidad de recursos, las empresas tienen que conocer los potenciales riesgos que se ciernen sobre sus redes. Estas amenazas revisten de muchas formas (véase Figura 2.1), pero todas ellas suponen una pérdida de la privacidad y la posible destrucción malintencionada de la información o de los recursos, que puede llevar a grandes pérdidas económicas[15] (véase Figura 2.2).

[15] *La siguiente estadística fue tomada del Instituto de Seguridad Informatica, en cooperación con el FBI (CSI/FBI), ®http://www.gocsi.com*

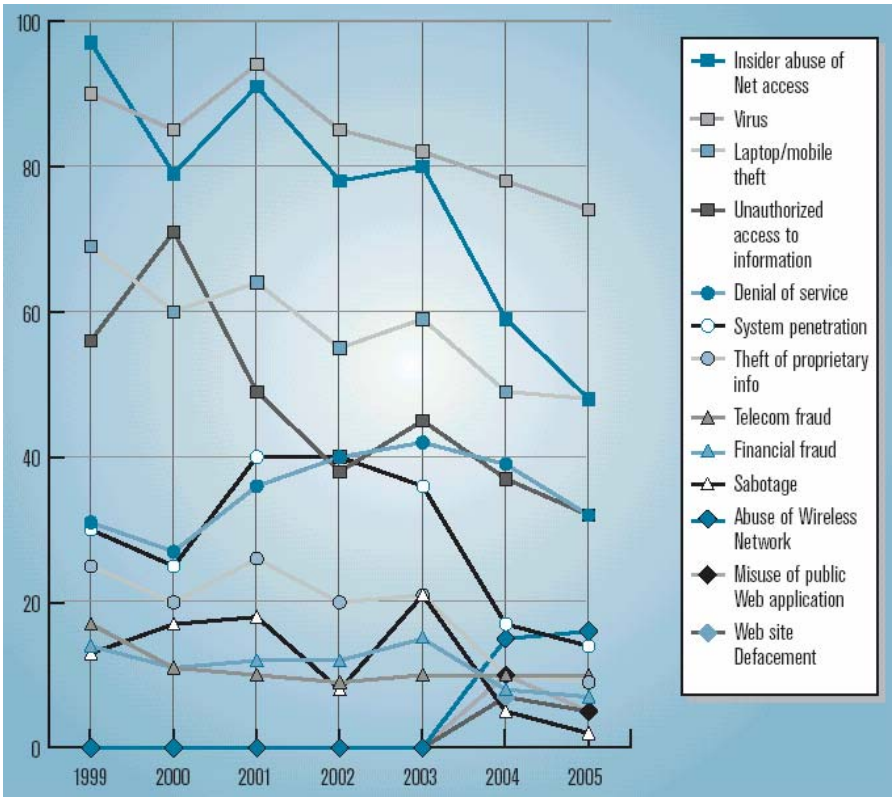


Figura 2.1 Tipos de ataques detectados en el 2005. Estos datos fueron obtenidos del reporte anual que proporciona la CSI, en colaboración con el FBI (CSI/FBI).

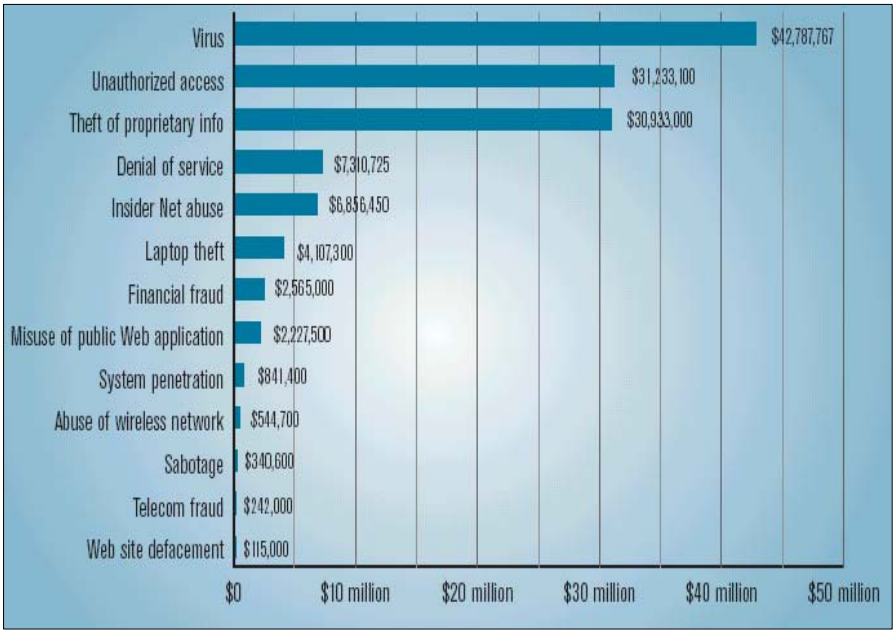


Figura 2.2 Esta figura muestra el costo agregado por brechas de seguridad durante el año de 2005.

2.1.1 Tipos de amenazas

Una amenaza (threat) es cualquier violación potencial de la seguridad [Carracedo, 2004]. La información que circula, se procesa y se almacena en una red está sometida a varios tipos de amenazas que pueden ser clasificadas, principalmente, en cuatro grupos:

- **Intercepción.** Es cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Son las más difíciles de detectar, pues en la mayoría de los casos no alteran la información o el sistema en si. Los ejemplos incluyen la intervención de las conexiones para capturar datos en una red y la copia ilícita de archivos o programas (véase la Figura 2.3).

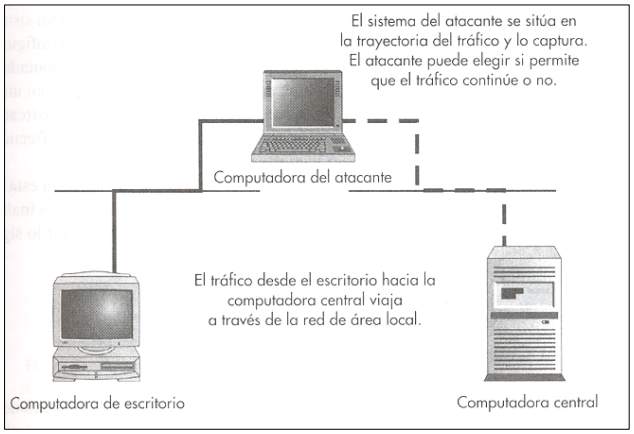


Figura 2.3 Ejemplo de la intersección de la información.

- **Interrupción**. Es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible o inutilizable. Algunos ejemplos incluyen la destrucción de una pieza de hardware, tal como un disco duro, el rompimiento de una línea de comunicación o la deshabilitación del sistema de administración de archivos (véase la Figura 2.4).

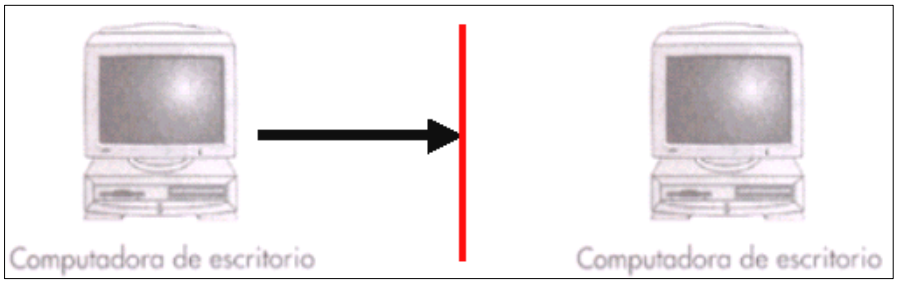


Figura 2.4 Ejemplo de la interrupción de la información.

- **Modificación.** Es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo. Los ejemplos incluyen cambiar los valores en un archivo de datos, alterar un programa de manera que se ejecute diferente y modificar el contenido de mensajes que se trasmiten en una red (véase la Figura 2.5).

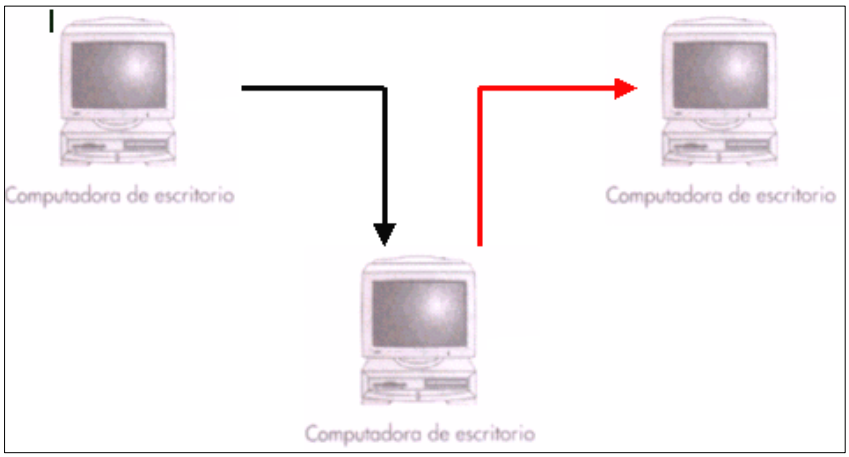


Figura 2.5 Ejemplo de la modificación de la información.

- **Falsificación**. Es cuando una entidad no autorizada tiene la posibilidad de añadir información o programas no autorizados en el sistema. Los ejemplos incluyen la inserción de mensajes impuros en una red, la adición de registros a un archivo y la sustitución de usuarios (Figura 2.6).

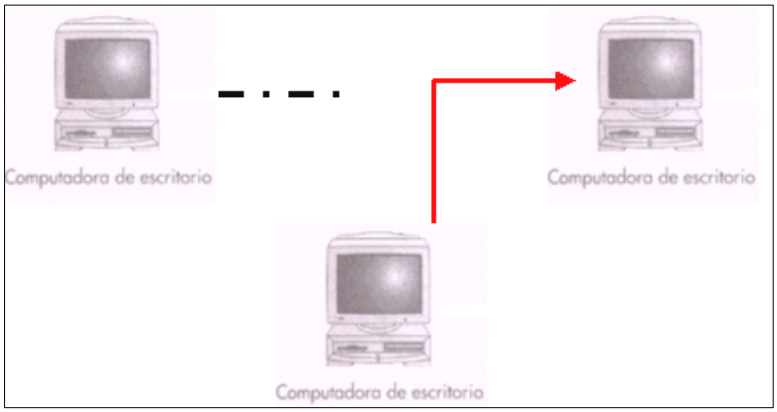


Figura 2.6 Ejemplo de la falsificación de la información.

Por otra parte, las amenazas pueden ser accidentales o intencionales. Amenazas accidentales son aquellas que aparecen de forma no premeditada: disfunciones en los sistemas, fallos de software, operaciones indebidas por parte de algún usuario inexperto, etc. El método para su tratamiento y prevención en el ámbito de las redes debe ser similar a los procedimientos que se siguen en el caso de sistemas informáticos aislados u otros sistemas: revisión periódica de equipos, prueba del correcto funcionamiento de los programas informáticos, mantenimiento de las instalaciones, formación adecuada del personal para evitar errores humanos, etc. Deberán ser tenidas en cuenta en un Análisis de Riesgos[16] global, pero su incidencia en los protocolos específicos de seguridad es secundaria. Otra cosa son las amenazas intencionales que presuponen la participación maliciosa de un sujeto o entidad que pretende hacer uso indebido de la red. Una amenaza intencional se denomina un ataque (attack). Los ataques pueden ser clasificados en ataques activos y ataques pasivos. Los primeros son aquellos que alteran el comportamiento normal del recurso o servicio telemático que está siendo atacado: una información desaparece, o es cambiada, o un sistema envía los datos hacia direcciones no previstas, etc. Los ataques pasivos, en cambio, no provocan ninguna modificación en el funcionamiento del sistema salvo el uso indebido de sus prestaciones. Es decir, si se produce, por ejemplo, un robo de información a causa de un pinchazo en la red, está seguirá fluyendo normal sin variaciones en su contenido y seguirá siendo consumida por los usuarios legitimados (además del ladrón, claro está).

Los cuatro tipos de ataques descritos en los párrafos anteriores resumen las actuaciones malintencionadas más significativas que pueden presentarse en las redes (véase Tabla 2.1), frente a las que deberán establecerse, por tanto, las medidas de protección. En todas las organizaciones resulta necesario confiar a determinadas personas la custodia de los recursos. Si los propios gestores de la seguridad se corrompen, la cosa se pone difícil. Cuando se organicen entornos de seguridad habrá que procurar que una misma persona no ostente demasiadas responsabilidades, y las que son críticas sean compartidas por más de una persona.

[16] El análisis de riesgos se encarga de detectar las debilidades y de buscar remedio para ellas, cubriendo un doble objetivo: estudiar los riesgos a los que está sometido un sistema de información y el entorno en que se encuentra inmerso; y dictaminar el establecimiento de las medidas (contramedidas) de seguridad apropiadas para prevenir y reducir esos riesgos.

Categoría de programa no deseado	Descripción	Riesgo de violaciones
Adware	Programa que muestra publicidad al usuario y que a veces realizan seguimiento de los hábitos de navegación por la Web. A menudo, el adware disminuye el rendimiento del navegador de Internet.	Riesgo medio
Backdoors	Programas diseñados para permitir el acceso a las computadoras de los usuarios sin su conocimiento o permiso.	Alto riesgo
Objetos de ayuda del navegador (BHO, por sus siglas en inglés)	A pesar de que no pertenecen específicamente a la categoría de programas no deseados, los BHOs son una forma en la que éstos pueden instalarse u obtener acceso al sistema de cómputo.	Riesgo medio
Hijackers de la página de inicio del navegador	Estos programas realizan cambios en las configuraciones de la página de inicio del navegador, para redirigirla a otro sitio (por lo general, a un sitio de pornografía). Se vuelven a instalar luego de haber sido "eliminados".	Bajo riesgo
Cookies	Archivos de texto usados para hacer seguimiento de sitios Web visitados, preferencias de los usuarios o para ayudar a aplicaciones basadas en la Web (comerciales de "desarrollo doméstico" o de marketing).	Bajo riesgo
Dialers	Los "dialers" desconectan las computadoras del ISP y vuelven a conectarla a Internet mediante costosas llamadas telefónicas. También pueden cambiar el ISP incluso si usted usa una conexión de alta velocidad. Su presencia no es fácil de reconocer.	Riesgo medio
Programas de broma	Pertenecen a la categoría de "travesuras", pues intentan hacer que el usuario haga o diga algo estúpido. Un ejemplo de esto es un programa que arroja una ventana emergente indicando al usuario que un archivo de la PC está infectado y necesita ser eliminado, el usuario lo borra y sin querer inutiliza un programa de aplicación, un servicio del sistema operativo o el equipo completo.	Riesgo medio
Usuarios de "Keystroke" o Keyloggers	Es un tipo de troyano que monitorea su sistema de cómputo para registrar todas las pulsaciones de teclas ("keystrokes") que se realizan. El registro puede monitorear correo electrónico, conversaciones de chat o mensajería instantánea y cualquier tipo de material escrito.	Alto riesgo
Crackers o Ladrones de contraseñas	Su objetivo es conocer las contraseñas de un sistema computacional o de alguna aplicación de la máquina.	Alto riesgo
Ventanas emergentes y Ventanas de segundo plano	"Ventanas" muy molestas que muestran información (generalmente relacionada con publicidad) sin permiso del usuario. Éstas pueden ser muy lentas de eliminar y aparecen en la pantalla continuamente, afectando la productividad de la persona.	Bajo riesgo

Tabla 2.1 Desde el punto de vista de la seguridad, los programas no deseados afectan a las computadoras, sistemas y redes, lo que produce una disminución en el rendimiento y pérdida de productividad.

Categoría de programa no deseado	Descripción	Riesgo de violaciones
Programas potencialmente no deseados/PUPS	Una categoría paraguas de programas de software que los propietarios o administradores de los sistemas pueden considerar indeseables de instalar, sin importar la legitimidad del mismo. Algunas de las subcategorías de los programas o deseados (PUPS) incluyen: Adware, Spyware, herramientas de administración remota, etc.	Alto riesgo
Herramientas de administración remota/RATs	Se clasifican en dos áreas. La primera, es un programa legítimo utilizado para razones legítimas (soporte de mesón de ayuda de TI). La segunda, es un programa legítimo o ilegítimo que se usa para usurpar el control de un sistema sin el permiso del usuario o de la empresa.	Alto riesgo
Scumware	No tiene una función de "desinstalación" y también trata de impedir todos los intentos de eliminación. Es uno de los tipos de PUPs más difíciles de eliminar y debido a sus agresivos esquemas de protección, ha sido apodado en la industria como "scumware" (escoriaware).	Alto riesgo
Spyware	Por lo general, el spyware se instala como un programa "incorporado" o "adicional" cuando alguien instala una aplicación gratuita o de shareware en el sistema de computo y no tan sólo con hacer clic en un sitio Web. Recopila y transmite datos desde los archivos y/o usuario de la máquina a un tercero sin notificar al usuario.	Alto riesgo
Monitor de sistemas	Consulte usuarios de "Keystroke" 7 keyloggers	Alto riesgo
Troyanos	Un troyano permite que los hackers accedan al sistema de cómputo y que puedan realizar cambios en la computadora. Puede tener la capacidad de controlar completamente una PC, como por ejemplo, tener el control del cursor, teclado e incluso enviar spam a través de correos electrónicos masivos desde su equipo infectado.	Alto riesgo

Tabla 2.1 Continuación

2.2 Tipos de problemas a la integridad de las redes

Los ataques explotan los puntos débiles de los sistemas. Estos pueden ser causados por redes mal diseñadas o por una planificación deficiente. En este apartado se mencionan las posibles amenazas y puntos vulnerables, clasificándolos en función del impacto que pueden tener en la redes [Merike, 2002] y [Parnell, 1997].

2.2.1 Tráfico de red engañoso

El tráfico tiene lugar cuando un mensaje parece haber sido enviado desde un lugar legítimo, cuando en realidad no ha sido así. Los datos que se transmiten sobre una red no deberán ser alterados de forma no autorizada como resultado de su transmisión, ni por la red ni por un intruso. Los usuarios deberían poder tener una expectativa razonable sobre si el mensaje que se envía es recibido sin alteración. Una modificación tiene lugar cuando se hace una alteración intencionada de la información. El engaño o la modificación del tráfico de una red puede ocurrir explotando los siguientes tipos de verificación:

- Transmisión del tráfico de una red en texto plano.
- Ausencia de indicación de fecha/hora.
- Ausencia de un mecanismo de verificación del mensaje o firma digital.
- Ausencia de mecanismo de verificación en tiempo real.

2.2.2 Acceso inapropiado a recursos

El acceso inapropiado a los recursos tiene lugar cuando un usuario, autorizado o no, se apropia de un recurso que no le está permitido utilizar. El acceso no autorizado podría ocurrir simplemente porque los derechos al recurso no están asignados adecuadamente, también porque el mecanismo de control de acceso del sistema de privilegios no posee la granularidad[17] suficiente. El acceso no autorizado a los recursos de una red puede darse explotando los siguientes tipos de vulnerabilidad:

- Utilizar permisos por defecto en el sistema que son excesivamente permisivos con los usuarios.
- Uso inadecuado de los privilegios del administrador o del gestor de la LAN.
- Datos que se almacenan con un nivel inadecuado o nulo de protección.
- Ausencia de, o utilización inapropiada, del mecanismo de privilegios por los usuarios.
- PC que no utilizan un control de accesos a nivel de archivos.

A medida que las redes van siendo utilizadas por una organización, determinados datos almacenados o procesados pueden requerir cierto nivel de confidencialidad. La revelación de datos o software de una red tiene lugar cuando un individuo no autorizado accede, lee e incluso hace públicos datos o software. Esto

[17] Es una de las técnicas con mayor potencial en paralelización ya que, además de poder incrementar la velocidad de ejecución de programas en arquitecturas paralelas clásicas, permite explotar el paralelismo usando máquinas con interconexiones poco eficientes (como por ejemplo entre estaciones de trabajo en una red local). Su objetivo es determinar (a ser posible en tiempo de compilación) cuál es el tamaño óptimo de las tareas paralelas para que no se desperdicie tiempo preparando y arrancando tareas demasiado pequeñas.

ocurre cuando alguien consigue acceso a información no encriptada u observa pantallas o listados de información. Los datos de la LAN pueden verse en peligro si se saca partido a los siguientes tipos de vulnerabilidad:

- Establecimiento de un control de acceso no adecuado.
- Datos, que han sido juzgados como lo suficientemente importantes como para justificar la encriptación, almacenados de manera no encriptada.
- Código fuente de aplicación almacenada de forma no encriptada.
- Pantallas visibles en áreas de mucho tráfico.
- Impresoras colocadas en áreas de mucho tráfico.
- Datos y copias de seguridad almacenados en zonas abiertas.

2.2.3 Interrupción de la red

Incluye aquellas amenazas que bloquean los recursos de la red dejándolos no disponibles repentinamente. Una interrupción de la funcionalidad de la red tiene lugar cuando la red no puede desempeñar el trabajo para el que está diseñada de una manera aceptable (véase Figura 2.7). Una interrupción de las funciones de la LAN puede deberse a los siguientes tipos de vulnerabilidades:

- Configuración de la LAN que permite un único punto de fallo.
- Falta de capacidad para detectar patrones de tráfico inusuales.
- Mantenimiento inadecuado del hardware de la red.
- Falta de capacidad para reencaminar tráfico o manejar fallos de hardware.

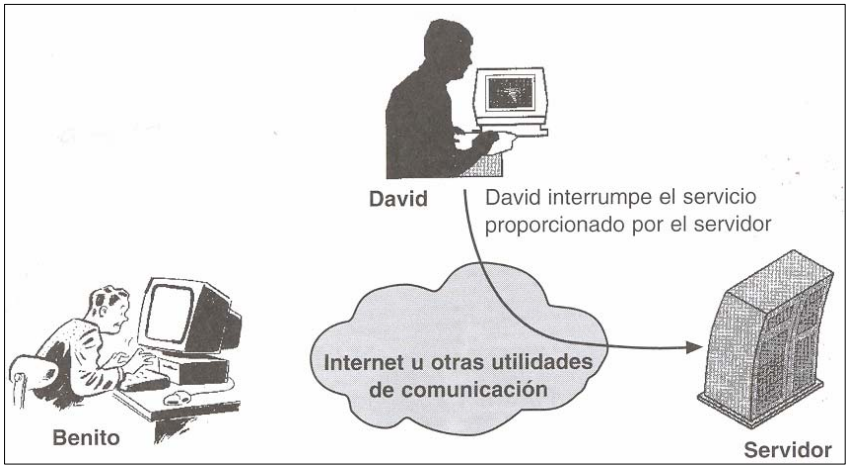


Figura 2.7 Interrupción del servicio.

2.2.4 Modificaciones no autorizadas de software

Consisten en modificar, borrar o destruir datos y software de la red de manera accidental o no autorizada. Debido a que los usuarios de una red comparten datos y aplicaciones, se deben controlar los cambios a esos recursos. Las modificaciones de datos o software ocurren cuando se hacen cambios sin previo aviso (ampliaciones, borrados o modificaciones) a un archivo o un programa. Cuando las modificaciones de datos no detectadas están presentes durante largos períodos de tiempo, la información modificada puede extenderse por el sistema, corrompiendo bases de datos, operaciones en hojas de cálculo y otros tipos de aplicaciones. Esto puede dañar la integridad de la mayoría de la información de aplicación. Cuando se realizan cambios de software no detectados, todo el sistema puede convertirse en sospechoso, obligando a una revisión minuciosa de la red y las aplicaciones relacionadas. Estos cambios se pueden realizar mediante sencillos programas de comandos, como archivos por lotes o programas de utilidades en sistemas multiusuario.

Estas modificaciones pueden desviar información a otros destinos, corromper los datos conforme se procesan o perjudicar la disponibilidad de los servicios del sistema. La modificación no autorizada de datos y software incluye claramente a los virus[18]. Actualmente los virus se limitan a corromper computadoras personales y utilizan las redes para infectar muchas estaciones de trabajo. La modificación no autorizada de datos y software puede darse aprovechando las siguientes debilidades:

- Ausencia de herramientas para detección de virus.
- Permiso de escritura otorgado a usuarios que sólo requieren permiso de lectura.
- Ausencia de una suma de comprobación cifrada en datos importantes.
- Cambios realizados al software no detectados.

2.2.5 Acceso no autorizado a la red

Las redes permiten compartir archivos, impresoras, etc. Debido a que los recursos están compartidos y no son utilizados por un único individuo, existe la necesidad de controlarlos (véase Figura 2.8). El acceso no autorizado a la red sucede cuando alguien que no tiene permitido utilizar la LAN consigue acceso a la misma (actuando normalmente como un usuario legítimo de la LAN). Existen tres métodos comunes para conseguir el acceso y son la **compartición, adivinación y captura de contraseña.**

La compartición de contraseña permite que un usuario no autorizado tenga acceso y privilegios de un usuario legítimo, y con el conocimiento y aceptación del mismo. ***La adivinación de contraseña*** es un

[18] Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos y se replica a sí mismo para continuar su esparcimiento, es decir, es un archivo ejecutable y que entra en acción toda vez que se cumplen ciertos requerimientos, desde ejecutarlo intencionalmente.

medio común de acceso no autorizado cuando no se tienen políticas de contraseña adecuadas. ***La captura de contraseña*** es un proceso en el que el usuario legítimo revela, de manera totalmente desconocida para él, el identificador de usuario y la contraseña. Esto se podría conseguir mediante la utilización de un programa llamado Caballo de Troya[19] que en apariencia es como el programa de inicio de sesión legítimo. Sin embargo, el programa está diseñado para capturar contraseñas y almacenarlas en un archivo. Otro método utilizado para conseguir acceso es capturar el identificador de usuario y la contraseña cuando éstas están siendo transmitidas a través de la red sin encriptar. El hardware y/o software que captura tráfico de LAN, incluyendo las contraseñas, está totalmente disponible. El acceso no autorizado a las redes puede ocurrir aprovechando los siguientes tipos de vulnerabilidad:

- PC no protegidos por contraseña.
- Ausencia de desconexión después de múltiples fallos en el login.
- Compartir la contraseña.
- Ausencia de un esquema de identificación y autentificación.
- Contraseñas de acceso a la LAN que se almacenan en PC.
- Escaso control físico de los dispositivos de red.
- Ausencia de período de expiración durante la fase de conexión.
- Módem desprotegidos.
- Escaso control de contraseñas.
- Ausencia de registro del «último inicio de sesión con éxito fecha/hora» e «intento fallido de inicio de sesión».

Figura 2.8 Lugares donde pueden ocurrir ataques de acceso.

[19] ***Son programas que permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar datos generalmente password enviándolos a otro sitio, o dejar indefenso el ordenador donde se ejecuta, abriendo agujeros en la seguridad del sistema, con la siguiente profanación de nuestros datos.***

2.2.6 Suplantación de la identidad

Es la capacidad de presentar credenciales de alguien o algo que no se es. Estos ataques pueden adoptar varias formas: la apropiación de una clave privada, la obtención de acceso a un par nombre de usuario/contraseña, o la reproducción de un registro de secuencia de autorización (véase Figura 2.9).

La suplantación de la identidad puede proceder del espionaje de paquetes y los ataques de reproducción. Los **ataques de espionaje** conllevan el suministro de información falsa acerca de la identidad principal con el fin de obtener acceso no autorizado a sistemas y servicios. Un **ataque de reproducción** puede ser una especie de acometida de espionaje, ya que los mensajes son registrados y enviados, generalmente para explotar los fallos en los esquemas de autenticación. Ambos tipos de ataques suelen ser el resultado de la información que se obtiene de la escucha ilegal. Muchos programas de espionaje de paquetes también incorporan prestaciones de generación de paquetes que pueden capturar lotes de datos y reproducirlos posteriormente.

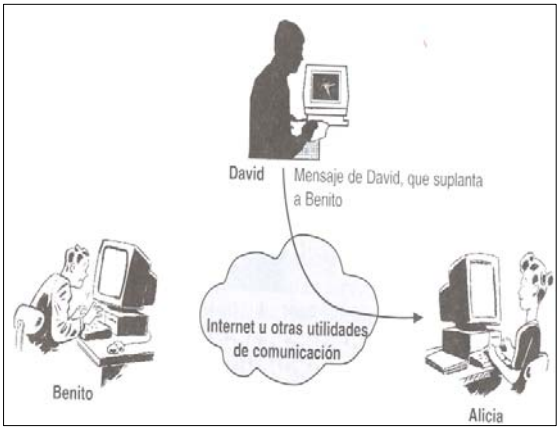


Figura 2.9 Suplantación de identidad.

La suplantación de la identidad de los dispositivos es en gran medida una cuestión de enviar paquetes de datos que se cree que son válidos, pero que pueden ser fruto del espionaje. Normalmente, este ataque genera un comportamiento no deseado en la red. El ejemplo de la Figura 2.10 muestra cómo el comportamiento inesperado cambia la información de enrutamiento. Suplantando la identidad de un router y enviando información de enrutamiento modificada. La suplantación de la identidad de los programas de una infraestructura de red pueden suponer que las imágenes o las configuraciones equivocadas sean descargadas en un dispositivo de la infraestructura de red (como un switch, un router o un firewall) y, por tanto, la ejecución de opciones y configuraciones no autorizadas.

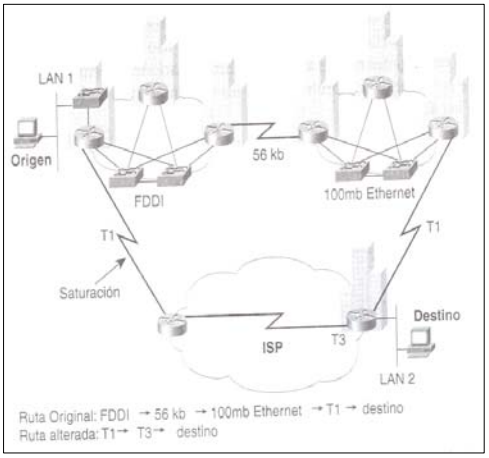


Figura 2.10 Suplantación de la identidad de las actualizaciones de enrutamiento.

2.2.7 Denegación de servicio

Es una interrupción debido a la destrucción del sistema, ya que temporalmente no está disponible. Entre los ejemplos más claros se incluye la destrucción del disco duro de una computadora, los daños en la infraestructura física y el uso de toda la memoria disponible en un recurso.

Muchos de los ataques DoS[20] más comunes son instigados desde protocolos de red, como IP (véase Figura 2.11). La Tabla 2.2 enumera los ataques DoS más comunes.

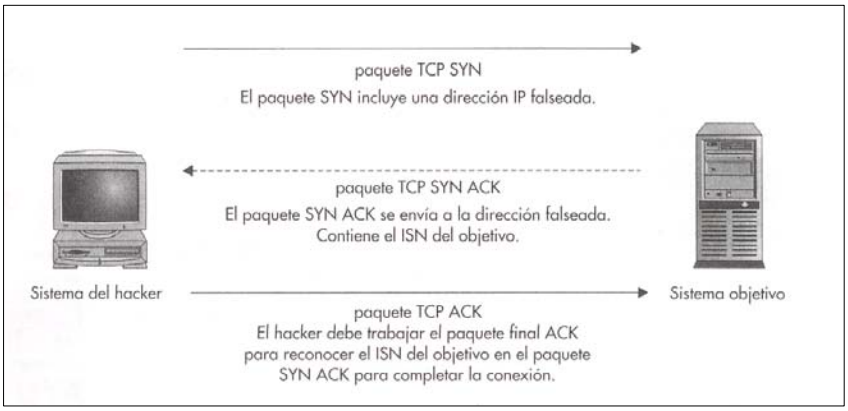


Figura 2.11 Detalles del falseamiento de IP.

Nombre del ataque DoS	Punto débil explotado
Ataque SYN de TCP	La memoria es asignada a las conexiones TCP de tal manera que no queda suficiente memoria para otras funciones.
Ping de la muerte	Implementación de la fragmentación de paquetes IP, donde los paquetes grandes son reensamblados y pueden hacer que los equipos colapsen.
Ataque Land.c	Establecimiento de la conexión TCP.
Ataque Teardrop.c	Implementación de la fragmentación de paquetes IP, donde los problemas de reensamblado pueden hacer que los equipos colapsen.
Ataque SMURF	Inundación de las redes con tráfico de difusión que congestiona la red.

Tabla 2.2 Ataques comunes de negación de servicio.

[20] Son diversas herramientas que se han utilizado para ocasionar daños y caos a través de Internet en años anteriores. Estos ataques de negación de servicio (DoS) cuestan a las empresas millones de dólares cada año y son una amenaza seria para cualquier sistema o red. Estos costos corresponden al período de indisponibilidad del sistema, pérdida de ingresos y al trabajo necesario para identificar y reaccionar a tales ataques. Esencialmente, un ataque DoS desorganiza o niega completamente el servicio a usuarios, redes, sistemas u otros recursos legítimos. La intención de cualquier ataque es, normalmente, dañina por naturaleza y frecuentemente requiere poca habilidad porque las herramientas necesarias están al alcance de cualquiera.

2.3 Seguridad en las capas TCP/IP

Esta parte del capítulo describe las principales tecnologías que se usan para garantizar la integridad y la confidencialidad de los datos en las distintas capas de TCP/IP [Merike, 2003] y [Raya y Raya, 2000]. A menudo, la colección de protocolos de comunicación está organizada en siete capas distintas, tal y como se especifica en el modelo OSI. Cómo se relacionan las capas TCP/IP con el modelo OSI se muestra en la Figura 2.12.

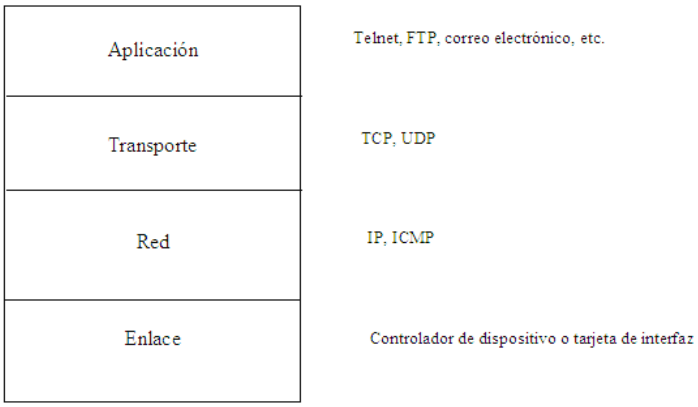


Figura 2.12 El modelo en capas TCP / IP.

La capa de aplicación alude a los detalles de una aplicación concreta, como Telnet, FTP (File Transfer Protocol, protocolo de transferencia de archivos) o HTTP (Hyper Text Transfer Protocol, protocolo de transferencia de hipertexto), y no hace referencia a los detalles del movimiento de los datos por una red. La capa de transporte proporciona los detalles del traslado del flujo de datos entre dos hosts. Tanto la capa de aplicación como la capa de transporte utilizan protocolos de extremo a extremo, donde los sistemas finales son los encargados de proporcionar seguridad al protocolo de aplicación o de transporte. La capa de red proporciona el manejo salto a salto de los paquetes de datos, donde están implicados los sistemas intermedios de una red, como los routers.

2.3.1 Capa de aplicación

El nivel de aplicación es el más difícil de definir, ya que los protocolos que operan en dicho nivel pueden ser aplicaciones totalmente completas, autocontenidas en sí mismas, como el FTP, o mecanismos utilizados por otras aplicaciones para proporcionar un servicio, como el DNS (Domain Name System, es un conjunto de protocolos y servicios) y SMTP (Simple Mail Transfer Protocol, protocolo simple de transferencia de correo electrónico), es decir, utiliza los protocolos de extremo a extremo, donde los sistemas finales son los encargados de proporcionar la seguridad. Sin embargo dado que la World Wide Web se ha convertido en una de las aplicaciones de más rápido crecimiento en Internet, se diseño un protocolo específico

de seguridad llamado protocolo seguro de transporte de hipertexto (S-HTTP).

- S-HTTP es un sistema para firmar y encriptar información enviada mediante el protocolo HTTP. Se diseño antes de la liberación pública de SSL. Incluye algunas características interesantes, como la capacidad de guardar documentos prefirmados en un servidor Web. Sin embargo, S-HTTP es un protocolo prácticamente muerto, y que Netscape y Microsoft no lo han incluido en sus navegadores.

2.3.2 Capa de transporte

En el nivel de transporte operan dos protocolos: el TCP y UDP (User Datagram Protocol, protocolo de datagrama a nivel de usuario). El primero es orientado a conexión y fiable, mientras que UDP es no orientado a conexión y no fiable. Una aplicación utilizará uno u otro en función de sus requisitos y de los servicios proporcionados por los demás niveles.

Se puede decir que, en cierto modo, el nivel de transporte engloba los niveles de sesión y de transporte del modelo OSI, pero no en todos los casos. Los sistemas Windows, por ejemplo, pueden utilizar TCP/IP para transportar los mensajes NetBIOS que utilizan para compartir archivos e impresoras, y pueden continuar proporcionando la misma funcionalidad de nivel de sesión que cuando un sistema utiliza NetBEUI o IPX en lugar de TCP/IP. Se trata sólo de un ejemplo de cómo los niveles de la pila de protocolos TCP/IP son equivalentes, en líneas generales, a las del modelo OSI, pero no totalmente.

A continuación se describen los protocolos de seguridad que funcionan sobre TCP/IP u otro transporte fiable, pero no seguro. Se clasifican como protocolos de seguridad de la capa de transporte, ya que tratan de protegerla y de proporcionar métodos para implementar la privacidad, la autenticación y la integridad por encima de la capa de transporte:

- **Protocolo de conexiones seguras (SSL, Secure Sockets Layer)** es un protocolo abierto diseñado por Netscape; especifica un mecanismo que sirve para proporcionar la seguridad de los datos clasificados entre los protocolos de aplicación (como HTTP, Telnet, NNTP o FTP) y TCP/IP (véase Figura 2.13). Incorpora el cifrado de datos, la autentificación del servidor, la integridad de los mensajes y la autentificación opcional del cliente para una conexión TCP/IP. El objetivo principal de SSL consiste en proporcionar privacidad y fiabilidad a dos aplicaciones que se comunican.

Figura 2.13 El proceso de intercambio de señales SSL.

- **El protocolo de Shell seguro (SSH, Secure Shell Protocol)** es un intérprete de comandos seguros. Proporciona operaciones protegidas para Telnet y FTP (como soporte para el inicio de sesión remota segura, la transferencia de archivos y el reenvío seguro del tráfico de sistemas TCP/IP y X Windows). Puede cifrar, autentificar y comprimir de forma automática los datos transmitidos.
- **La seguridad de Sockets (SOCKS)**[21] es un protocolo de proxy de networking basado en la capa de transporte. Está diseñado para proporcionar un marco para las aplicaciones cliente/servidor en los dominios TCP (entre las cuales se incluye Telnet, FTP y los protocolos de descubrimiento de información, como HTTP, Wais y Gopher) para usar cómodamente y de forma segura los servicios de un firewall de red (véase Figura 2.14).

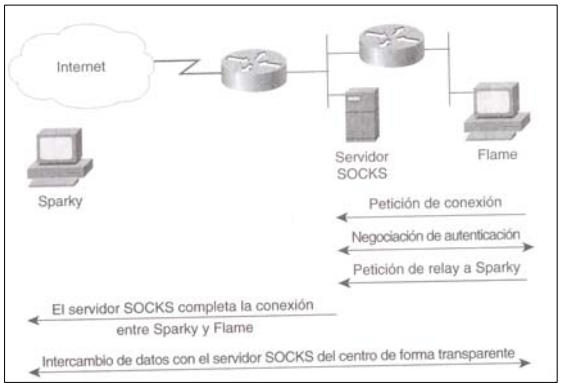


Figura 2.14 El modelo de seguridad SOCKS.

2.3.3 Capa de red

La protección de la capa de red atañe a los servicios de seguridad IP de la pila de protocolos TCP/IP. Implementando la seguridad en el nivel de red, una organización puede conseguir una red segura no sólo para las aplicaciones que poseen mecanismos de seguridad, sino también para las aplicaciones que no los tiene.

El paquete de protocolos de seguridad IP (IPsec) se basan en una serie de estándares, los más importantes de ellos, publicados en noviembre de 1998, y son los RFC 2401, 2402, 2406 y 2408:

- RFC 2401: descripción general de una arquitectura de seguridad.
- RFC 2402: descripción de la extensión de autentificación de un paquete a Ipv4 e Ipv6.
- RFC 2406: descripción de la extensión de cifrado de un paquete Ipv4 e Ipv6.
- RFC 2408: especificación de las capacidades de gestión de claves.

[21] ***Fue originalmente desarrollado por David y Michelle Koblas; el código fue puesto a disposición en Internet de forma gratuita. Desde entonces, ha habido varias revisiones importantes, pero el software sigue siendo gratuito.***

IPsec define un marco de referencia seguro y un conjunto de servicios de seguridad para las comunicaciones a nivel de red : se puede usar con ambientes IPv4 e IPv6. Permitir estas características es obligatorio para dichos ambientes. En ambos casos se implementan como cabeceras de extensión que siguen a la cabecera IP principal. La cabecera de extensión para la autentificación se conoce como cabecera de autentificación (AH, Authentication Header); y para el cifrado se conoce como cabecera de encapsulado de carga útil de seguridad (ESP, Encapsulating Security Payload Header).

Opera en uno de dos modos: de túnel o de transporte. En el modo de túnel, todo el paquete de IP está cifrado y se convierte en la parte de los datos de un nuevo paquete IP más grande, al que se agregan un nuevo encabezado IP y un encabezado Ipsec (véase Figura 2.15). En el modo de transporte, el encabezado Ipsec se inserta directamente en el paquete IP (véase Figura 2.16). El modo de túnel se usa, básicamente, con puertas o nodos de enlace, y proxys (véase Figura 2.17). Los sistemas intermedios implantan los servicios Ipsec; los extremos no saben acerca de Ipsec. En el modo de transporte, ambos extremos deben implantar Ipsec; los sistemas intermedios no realizan ningún procesamiento de Ipsec en el paquete (véase Figura 2.18).

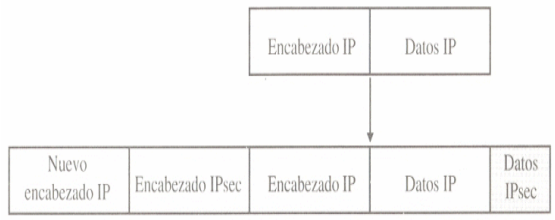


Figura 2.15 Paquete Ipsec en modo de túnel.

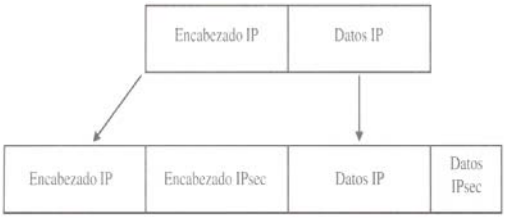


Figura 2.16 Paquete Ipsec en modo de transporte.

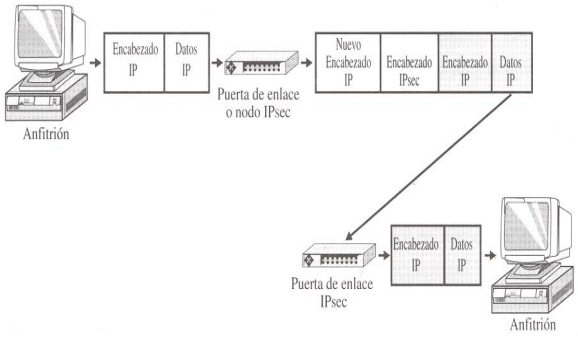


Figura 2.17 IPsec en modo de túnel.

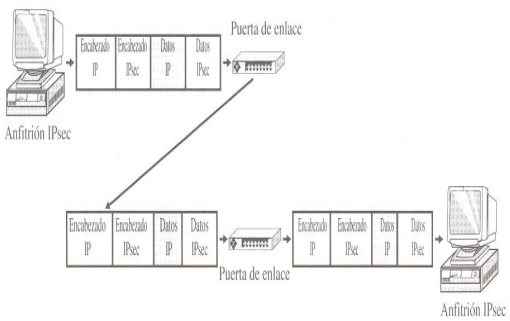


Figura 2.18 IPsec en modo de transporte.

2.3.4 Cómo utilizar la seguridad en las capas TCP/IP

El protocolo de seguridad a usar en un entorno determinado depende de los servicios de seguridad que se requieren en aplicaciones que necesitan protección. Todos los protocolos de la capa de aplicación tienen la ventaja de que el servicio de seguridad puede ser definido específicamente en términos de las actividades de la aplicación. Por ejemplo, en lo que respecta a los servidores Web, sería posible aplicar medidas de seguridad variables a las páginas Web individuales. Sin embargo, la mayoría de los protocolos de seguridad de la capa de aplicación, como HTTP, se están convirtiendo en obsoletos por el uso de los protocolos de la capa de transporte o de la capa de red.

En lo relativo a la seguridad de la capa de transporte, todos los mensajes de aplicación deberán ser tratados por igual. Sin embargo, es posible especificar distintos servicios de seguridad para aplicaciones diferentes, siempre y cuando las implementaciones de los fabricantes lo permitan. SSL se ha generalizado y está muy implementado en entornos World Wide Web, ya que suele ir empaquetado con las aplicaciones. SSH es un protocolo válido para la protección de los protocolos de capa de transporte, y se usa mucho para Telnet y FTP.

La seguridad de la capa de red, a través del uso de IPsec, puede definir los servicios de seguridad de la capa IP. Dependiendo de la implementación de cada fabricante, es posible definir los servicios de seguridad en base a las direcciones IP, o es posible proporcionar distintos servicios de seguridad en base a una combinación de dirección IP, protocolo de transporte y aplicación. Ipsec tiene la ventaja de ocultar la información de la capa de transporte, y puede soportar protocolos que no sean TCP (como UDP). Sin embargo, dado que oculta la información de la capa de transporte, si se requiere información de la cabecera de esta capa para soportar otros requisitos de red (como la calidad del servicio que podría tener que buscar números de puerto TCP/UDP), podría tener problemas. Generalmente, es necesario combinar los protocolos de seguridad; la mayoría de los entornos utilizan una combinación de los protocolos de la capa de transporte e Ipsec.

2.4 Mecanismos de seguridad

Se han desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos (véase Figura 2.19). Los Mecanismos de Seguridad son utilizados para implementar un determinado servicio de seguridad o una combinación de ellos. La Tabla 2.3, basada en X.800, indica la relación que se da entre los servicios y mecanismos de seguridad.

Podríamos decir que los mecanismos de seguridad son las piezas lógicas, los ladrillos, con los que se construyen los protocolos de seguridad, los cuales son los encargados de proporcionar los servicios de seguridad. Por lo general, estos mecanismos se apoyan en técnicas criptográficas, es decir, en la actualidad la mayoría de los mecanismos de seguridad que han sido desarrollados son mecanismos criptográficos.

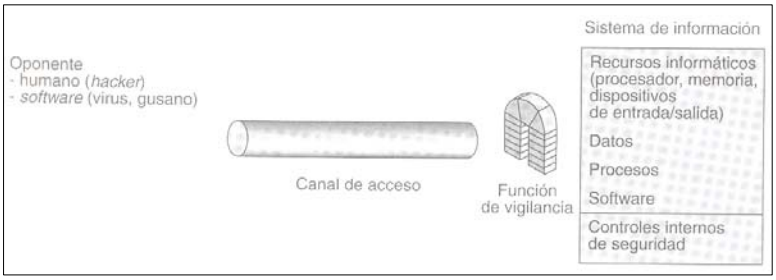


Figura 2.19 Modelo para la seguridad en el acceso a redes.

La arquitectura OSI de seguridad diferencia entre mecanismos de seguridad específicos y mecanismos de seguridad generalizados [Oppliger, 1998].

	Mecanismos							
Servicio	**Cifrado**	**Firma digital**	**Control de acceso**	**Integridad de los datos**	**Intercambio de autentificación**	**Relleno del tráfico**	**Control del enrutamiento**	**Notarización**
Autentificación de entidades origen/destino	Y	Y			Y			
Autentificación del origen de los datos	Y	Y						
Control de acceso			Y					
Confidencialidad	Y						Y	
Confidencialidad del flujo del tráfico	Y					Y	Y	
Integridad de los datos	Y	Y		Y				
No repudio		Y		Y				Y

Tabla 2.3 Relación entre servicios y mecanismos de seguridad.

2.4.1 Mecanismos de seguridad específicos

- El **cifrado** se utiliza para proteger la confidencialidad de las unidades de datos y la información de flujo de tráfico, o para dar soporte o complementar otros mecanismos de seguridad.
- Los **mecanismos de firma digital** se utilizan para proporcionar una analogía electrónica a la firma manuscrita en los documentos electrónicos. De forma similar a las manuscritas, las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas, y el firmante no debe poder rechazarlas posteriormente.
- Los **mecanismos de control de acceso** son las identidades autentificadas de los principales, información sobre dichos principales o capacidades de determinar y reforzar los derechos de acceso. Si un usuario intenta utilizar un recurso autorizado o no autorizado con un mecanismo impropio de acceso, la función de control de acceso rechazará el intento y podrá, además, informar del incidente con el propósito de generar una alarma y guardarla como parte de los informes de auditoria sobre seguridad.
- Los **mecanismos de integridad de datos** protegen la integridad bien de unidades de datos y de campos dentro de las mismas, bien de secuencias de unidades de datos y campos dentro de dichas secuencias. Nótese que, en general, los mecanismos de integridad de datos no protegen contra ataques tipo réplica. La protección de la integridad de una secuencia de unidades de datos y de campos dentro de la misma requiere habitualmente algún tipo de ordenación explícita, como numeración en secuencia, marcado temporal o encadenamiento criptográfico.
- Los **mecanismos de intercambio de autentificación** se utilizan para verificar la supuesta identidad de los principales. Se dice que un mecanismo de intercambio de autentificación es fuerte si se basa en el uso de técnicas criptográficas para proteger los mensajes que se van a intercambiar.
- Los **mecanismos de relleno del tráfico**[22] se utilizan para la protección contra ataques de análisis de tráfico. El objetivo es no revelar si los datos que se están transmitiendo representan y codifican realmente información. En consecuencia, los mecanismos de relleno de tráfico sólo serán efectivos si son protegidos por un servicio de confidencialidad de datos.
- Los **mecanismos de control de encaminamiento** se pueden utilizar para la selección dinámica o preestablecida de rutas específicas para la transmisión de los datos. Los sistemas de comunicaciones que detectan de forma persistente ataques activos o pasivos pueden indicar al proveedor de servicio de red que desea establecer una conexión por una ruta diferente. Similarmente, el transporte de datos de cierto nivel de seguridad puede estar prohibido por la política de seguridad para ciertas redes, servidores de reenvío o enlaces.

[22] *El término relleno de tráfico se refiere a la generación de ejercicios de comunicación espurios, unidades de datos espurias, y de datos espurios dentro de dichas unidades.*

- Los **mecanismos de certificación** se pueden emplear para asegurarse de ciertas propiedades de los datos que se comunican entre dos o más unidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

2.4.2 Mecanismos de seguridad generalizados

Los mecanismos de seguridad generalizados no son específicos de un servicio en particular, y en algunos casos pueden ser contemplados también como aspectos de la gestión de la seguridad. La importancia de estos mecanismos está relacionada directamente con el nivel de seguridad requerido. La arquitectura de seguridad OSI enumera cinco mecanismos de seguridad generalizados:

- **El concepto general de funcionalidad de confianza** se puede utilizar bien para extender de otros mecanismos de seguridad o para establecer su efectividad. Cualquier tipo de funcionalidad que proporcione directamente mecanismos de seguridad o el acceso a los mismos debe ser de confianza.
- **Los recursos del sistema** pueden tener asociadas etiquetas de seguridad (por ejemplo, para indicar niveles de sensibilidad). A menudo es necesario que los datos en tránsito lleven la etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito (por ejemplo, por el uso de una clave específica para cifrar los datos o por el contexto de los datos, como su fuente o ruta).
- **La detección de eventos** relevantes para la seguridad se utiliza para detectar violaciones aparentes de la seguridad.
- **La auditoria de seguridad** es la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en el control, política y procedimientos. En consecuencia, el rastreo de auditoria de seguridad se refiere a los datos que se adquieren y que potencialmente facilitan las auditorias sobre seguridad.
- **Las recuperaciones de seguridad** tratan con solicitudes de mecanismos como gestores de eventos y funciones de gestión, y realizan acciones de recuperación resultado de la aplicación de una serie de reglas.

2.5 Análisis de las herramientas de seguridad

Una vez identificados los activos vitales y analizados los riesgos, es el momento de diseñar las herramientas o normas para brindar la mayor protección a todas las áreas de la red. A continuación se explicaran dichas herramientas [Merike, 2003].

2.5.1 Seguridad en la infraestructura física

Los controles de seguridad física garantizan que no haya una manipulación maliciosa en torno de la infraestructura, la protección de los dispositivos y el acceso físico.

La infraestructura de la red física abarca la selección del tipo de medio adecuado y la ruta al cableado físico (la topografía de la red). Lo deseable es que ningún intruso sea capaz de escuchar ilegalmente los datos que recorren la red y que todos los sistemas importantes posean un alto grado de disponibilidad. Entre los medios que utiliza la infraestructura de red física, se encuentran:

- Selección de los medios físicos.
- Topografía de red.

2.5.1.1 Protección de los dispositivos físicos

La seguridad de los dispositivos físicos se suele subestimar. Los intrusos con suficiente motivación pensarán que pueden obtener lo que desean. La seguridad de los dispositivos físicos incluye la identificación de la ubicación de los dispositivos, la limitación del acceso físico y la instauración de las protecciones del entorno adecuadas.

Ubicación física.- La ubicación de los recursos vitales de la red es de suma importancia. El equipo de la infraestructura de red deberá estar físicamente ubicado en áreas de acceso restringido, a fin de eliminar la posibilidad de que haya un acceso no autorizado imputable a la proximidad física El equipo de infraestructura incluye algo más que las redes y los routers, firewalls, switches y servidores de acceso a la red que interconectan las redes. El equipo de la infraestructura también incluye los servidores que proporcionan los distintos servicios de red: administración de red (SNMP), DNS, hora de red (NTP), sistema de archivos de red (NFS), HTTP, autenticación y autorización de usuario (TACACS+, RADIUS, Kerberos), auditoria de red y detección de intrusos.

Acceso físico.- Los requisitos de acceso físico a las áreas controladas son determinados en gran medida por los resultados del análisis de riesgos o una encuesta de seguridad. Conviene restringir el acceso físico a los armarios de conexión y a las ubicaciones más importantes del equipo de la infraestructura de red. El acceso a estas áreas no deberá estar permitido a menos que la persona esté específicamente autorizada o requiera acceso para llevar a cabo sus tareas.

Protecciones del entorno.- Es preciso instalar e implementar protecciones del entorno apropiadas con el fin de proteger los recursos de red vitales. La importancia del sistema determina si la seguridad es o no "adecuada". Cuanto más importante sea un sistema, más protecciones deberán implantarse para asegurar que el recurso está disponible a cualquier costo. Como mínimo, deberá considerar las siguientes protecciones del entorno: prevención, detección, supresión y protección contra incendios; prevención, detección y control de inundaciones; protección del suministro eléctrico; control de la temperatura; control de la humedad; protección frente a desastres naturales provocados por terremotos, rayos, tormentas, etc; protección frente a campos magnéticos excesivos; buenos procedimientos de limpieza para la protección contra la suciedad y el polvo.

2.5.2 Controles de seguridad lógica

Se refiere a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. Los objetivos que se plantean son:

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

2.5.2.1 Controles de acceso

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad, etc. Constituyen una importante ayuda para proteger al sistema operativo de la red, al de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

2.5.2.1.1 Control de acceso interno

- **Palabras claves (PASSWORDS).-** Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras claves resultan de muy bajo costo.
- **Listas de control de acceso.-** Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.
- **Límites sobre la interfase de usuario.-** Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre las bases de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

2.5.2.1.2 Control de acceso externo

- **Dispositivos de control de puertos.-** Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.
- **Acceso de personal contratado o consultores.-** Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.
- **Accesos públicos.-** Para los sistemas consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

2.5.3 Niveles de seguridad

La clasificación de los sistemas de computación según sus requisitos de seguridad ha sido un tema ampliamente discutido desde los años setenta. La disparidad de criterios existentes se ha ampliado más con la conexión de las computadoras para formar redes de computación. Algunas de las clasificaciones existentes[23] en la actualidad son la del Departamento de Defensa de los Estados Unidos de América, el criterio alemán, el criterio canadiense, el ITSEC o el criterio común. Pero la más popular es la del Orange Book[24] del Departamento de Defensa (DoD) de Estados Unidos. Esta clasificación especifica cuatro niveles de seguridad: A, B, C y D [Carreto, 2001].

NIVEL D.- No pasan las pruebas de seguridad mínima exigida en el DoD. MS-DOS y Windows 3.1 son sistemas de nivel D. Puesto que están pensados para un sistema monoproceso y monousuario, no proporcionan ningún tipo de control de acceso ni de separación de recursos.

NIVEL C1 (protección discrecional).- La aplicación de los mecanismos de protección depende del usuario, o usuarios, que tienen privilegios sobre los mismos. Estos significa que un objeto puede estar disponible para lectura, escritura o cualquier operación, según el libre albedrío de su dueño. Casi todos los sistemas operativos comerciales de propósito general, como UNIX, LINUX o Windows NT, se clasifican en este nivel. A su vez se dividen en dos subniveles, dependiendo de la precisión del control de acceso:

- *Control de acceso por dominios* ***(Clase C1)***.- No hay posibilidad de establecer qué elemento de un determinado dominio ha accedido a un objeto. UNIX pertenece a esta clase. Divide a los usuarios en tres dominios: dueño, grupo y mundo. Se aplican controles de acceso según los dominios, siendo todos los elementos de un determinado dominio iguales ante el sistema de seguridad.
- *Control de acceso individualizado* ***(Clase C2)***.- Granularidad mucho más fina en el control de acceso a un objeto. El sistema de seguridad debe ser capaz de controlar y registrar los accesos a cada objeto a nivel de usuario. Windows NT pertenece a esta clase.

NIVEL B (control de acceso obligatorio).- En este nivel, los controles de acceso no son discrecionales de los usuarios o dueños de los recursos, sino que deben existir obligatoriamente. Esto significa que todo objeto controlado debe tener protección, sea del tipo que sea. En caso de que el dueño no defina cuál, el sistema de seguridad asigna una por defecto. Este nivel se divide a su vez en tres subniveles:

[23] La última clasificación ha sido definida conjuntamente en Estados Unidos y Canadá, siendo publicada su primera versión en 1994. Es un sistema complejo que todavía está en fase de elaboración y discusión, por lo que hay muy pocos sistemas comerciales que se ajusten a esta norma. Sin embargo, es importante resaltar que tiene grandes posibilidades de convertirse en un estándar.

[24] ® http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

- *Etiquetas de seguridad obligatorias (**Clase B1**).-* Cada objeto controlado debe tener su etiqueta de seguridad. Pueden existir objetos no controlados. Este modelo de seguridad se ajusta al de Bell – La Padula[25].
- *Protección estructurada **(Clase B2)**.-* Todos los objetos deben estar controlados mediante un sistema de seguridad con diseño formal y mecanismos de verificación. Estos mecanismos permiten probar que el sistema de seguridad se ajusta a los requisitos exigidos. Controles obligatorios, y asignados según el principio del menor privilegio posible, para objetos, sujetos y dispositivos.
- *Dominios de seguridad **(Clase B3)**.-* B2 ampliado con pruebas exhaustivas para evitar canales encubiertos, trampas y penetraciones. Diseño probado y verificado, que usa niveles, abstracciones de datos y ocultamiento de información. El sistema debe ser capaz de detectar intentos de violaciones de seguridad, para ello debe permitir la creación de listas de control de acceso para usuarios o grupos que no tienen acceso a un objeto.

NIVEL A (sistemas de seguridad certificados).- Para acceder a este nivel, la política de seguridad y los mecanismos de protección del sistema deben ser verificados y certificados por un organismo autorizado para ello. Organismos de verificación muy conocidos son el National Computer Security Center o el TEMPEST.

- *Diseño verificado **(Clase A1)**.-* Clase B1 más modelo formal del sistema de seguridad. La especificación formal del sistema debe ser probada y aprobada por un organismo de certificación. Para ello debe existir una demostración de que la especificación se corresponde con el modelo, una implementación consiste con el mismo y un análisis formal de distintos problemas de seguridad. El Vax Security Kernel pertenece a esta clase.
- *Desarrollo controlado **(Clase Ax)**.-* A1 más diseño con instalaciones y personal controlados. Formas de control no definidas. Se podrían incluir requisitos de integridad de programas, alta disponibilidad y comunicaciones seguras.

[25] Este modelo estaba basado en el concepto gubernamental, esto es, con varios niveles de información clasificada (desclasificada, confidencial, secreta y ultrasecreta) y con varios niveles de información de autorización. Si una persona (un sujeto) tenía un nivel de autorización que dominaba (era superior) el nivel de clasificación de un archivo (un objeto), esa persona podría tener acceso al archivo. Si el nivel de autorización de la persona era inferior que el de la clasificación del archivo, el acceso sería denegado.

2.5.4 Infraestructura e integridad de los datos

En la infraestructura de red, conviene asegurarse de que todo el tráfico de la red sea válido. El **tráfico válido** es el que puede clasificarse como tráfico de red esperado, como el siguiente:

- Servicios soportados.
- Tráfico legal.
- Datos que no han sido alterados.

Los *firewalls* controlan el flujo de tráfico entre redes y se suelen usar para controlar el flujo de los servicios de red soportados. La autenticación de los datos en la infraestructura de red proporciona una seguridad razonable frente a los paquetes alterados. La colocación de protecciones para implementar métodos cuyo fin sea el de impedir ataques puede evitar el tráfico ilegal.

2.5.4.1 Firewalls

Una forma habitual de garantizar la integridad de la infraestructura es a través de los firewalls. Su función es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos [Raya y Raya, 2000]. Un cortafuegos levanta una barrera (véase Figura 2.20) que controla el flujo de tráfico entre redes (el cortafuegos más seguro bloquearía todo el tráfico y, por tanto, no permitiría establecer conexiones, por lo que se necesita controlar estrictamente el tráfico seleccionado de un modo seguro). El firewall puede ser configurado para permitir que sólo determinadas direcciones, origen y destino, puedan acceder a una red (o desde ella). Las funciones de los firewall se pueden realizar por:

- Computadores dedicados a este fin (servidores proxy).
- Encaminadores de red (routers) configurados para esta tarea.
- Programas de software para distintos sistemas operativos.
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

Actualmente, existen tres clasificaciones de los firewalls (véase Figura 2.21) que abarcan distintas características de filtrado: Filtrado de paquetes, Filtrado de circuitos y Gateways de aplicación [Merike, 2003] y [Karanjit y Hare].

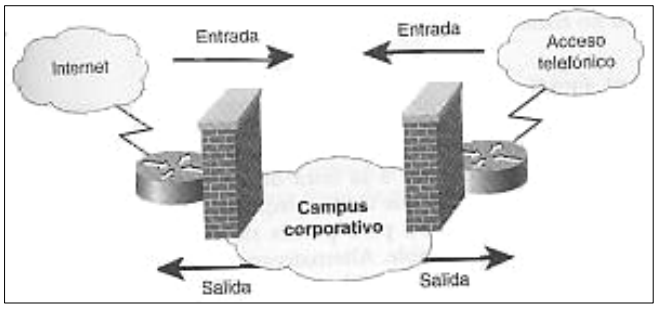


Figura 2.20 Los firewalls se asemejan a las cerraduras de las puertas en el perímetro de los edificios que permiten solamente el acceso a los usuarios autorizados (los que tengan claves o identificaciones.

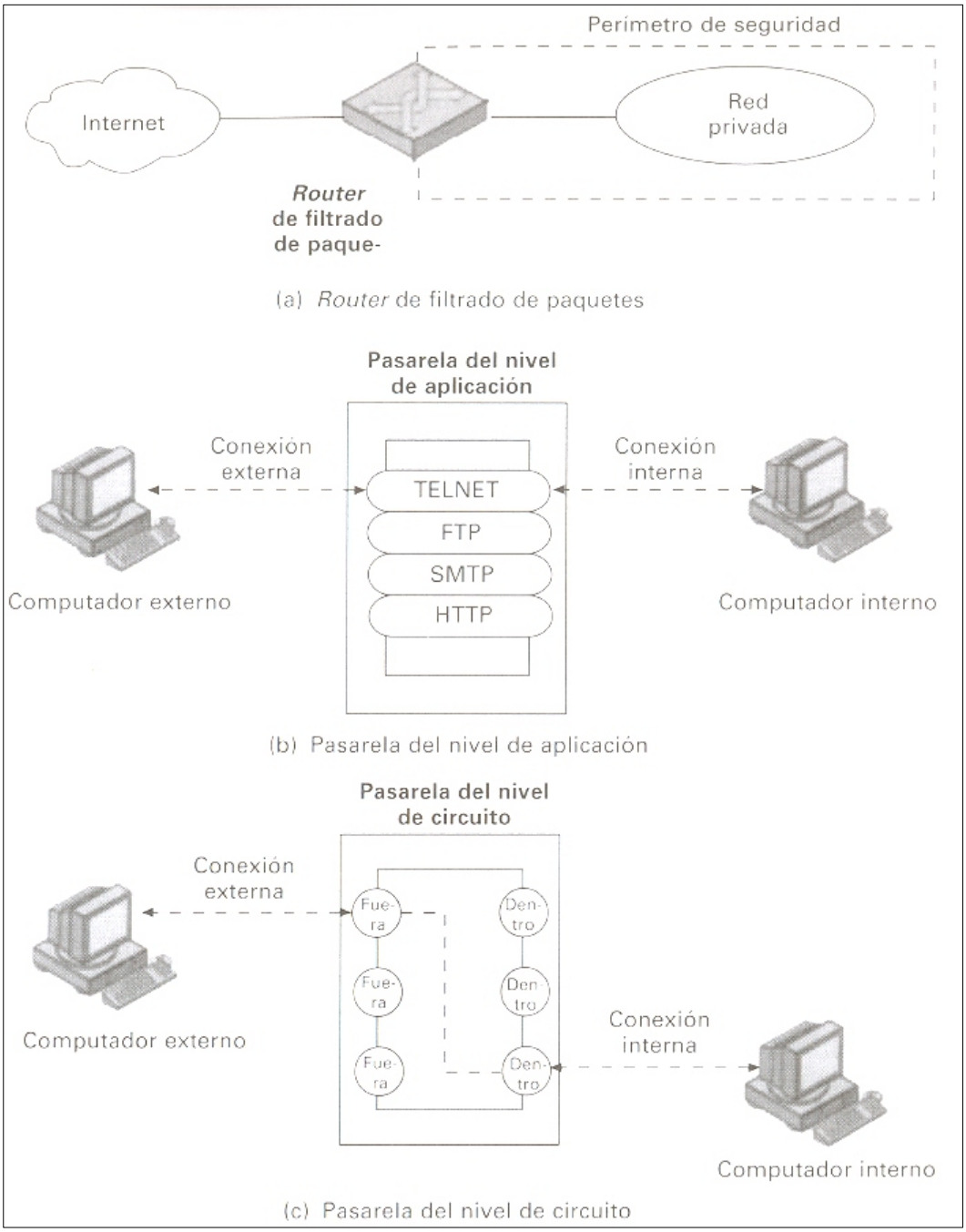


Figura 2.21 Tipos de cortafuegos.

2.5.5 Políticas de seguridad

Política de seguridad es un término, que hace referencia a un documento escrito que define el enfoque de seguridad de una organización, o de un área de específica (en este caso, de la seguridad informática y de redes) y que establece una serie de normas que deben seguirse al aplicar la filosofía de seguridad de la empresa [Littlejohn, 2003].

Las empresas pueden establecer tanto normas escritas como no escritas relacionadas con los problemas de la seguridad, además de emitir varios tipos diferentes de documentos relacionados con estos temas.

Se pueden establecer dos instancias principales en el desarrollo de políticas que reflejen la seguridad en los sistemas de comunicaciones. Estas instancias principales forman la base de todas las demás políticas de seguridad y regulan los procedimientos acomodados para implantarlas.

Aquello que no se permite en forma expresa, está prohibido, es el primer paso a la seguridad. Esto significa que la organización ofrece un grupo de servicios preciso y documentado, y que todo lo demás está prohibido. Por ejemplo, si decide permitir transferencias FTP anónimas hacia y desde una máquina particular, pero no acepta servicios Telnet, entonces el soporte documental para FTP ilustra este planteamiento, y no el de Telnet.

La alternativa del planteamiento es ***aquello que no esté prohibido de manera expresa se permite.*** Esto significa que a menos que usted indique en forma expresa que un servicio no está disponible, entonces todos los servicios estarán útiles. Por ejemplo, si no se dice con claridad que las sesiones de Telnet a un anfitrión dado están prohibidas, entonces quiere decir que están permitidas.

Sin importar qué decisión se tome, la razón para definir una política de seguridad, es determinar qué acción deberá tomarse en caso de que la seguridad de una organización se vea comprometida. La política también intenta describir qué acciones serán toleradas y cuáles no.

2.6 Un modelo de seguridad en redes

La Figura 2.22 constituye un modelo que presenta, en términos generales, parte de los aspectos que se discutieron en este capítulo. La información ha de ser transmitida de una parte a otra mediante algún tipo de Intranet. Las dos partes, que son los interlocutores en esta transacción, deben cooperar para que el intercambio tenga lugar. Se establece un canal de información definiendo una ruta a través de la Intranet que vaya de la fuente al destino y mediante el uso cooperativo de los protocolos de comunicación (TCP/IP) por parte de los dos interlocutores.

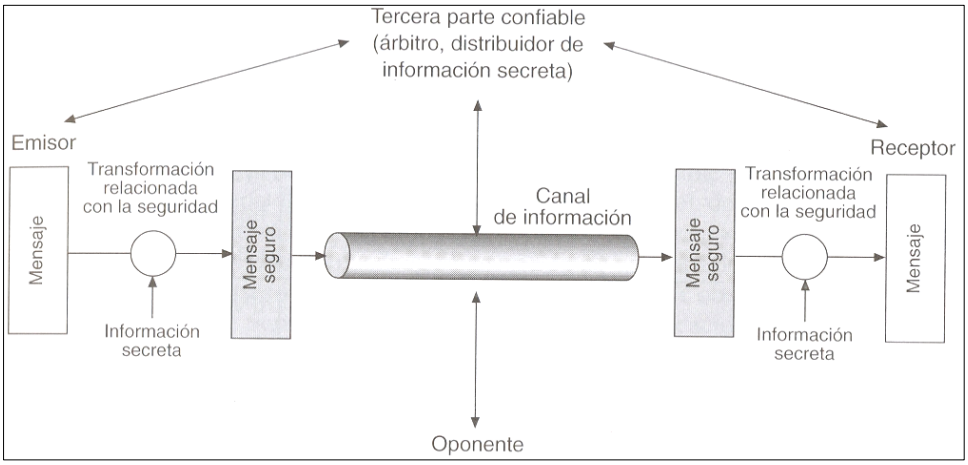


Figura 2.22 Modelo para la seguridad de redes.

Los aspectos de seguridad entran en juego cuando se necesita o requiere proteger la transmisión de información de un oponente que pudiera presentar una amenaza a la confidencialidad, a la autenticidad, etc. Todas las técnicas para proporcionar seguridad tienen dos componentes:

- Una transformación relacionada con la seguridad de la información que se va a enviar. Ejemplo de ello los tenemos en el cifrado de la información, que lo desordena para que resulte ilegible al oponente, y a la aplicación de un código basado en el contenido de los datos, que puede usarse para verificar la identidad del emisor.
- Alguna información secreta compartida por los interlocutores y desconocida por el oponente. El ejemplo lo hallamos en una clave de cifrado usada en conjunción con la transformación para desordenar el mensaje antes de la transmisión y reordenarlo en el momento de la recepción.

Para lograr una transmisión segura, puede ser necesaria una tercera parte de confianza, que , por ejemplo, sea la responsable de distribuir la información secreta a los dos interlocutores y la guarde de cualquier oponente. También puede ser necesaria para arbitrar disputas entre los interlocutores en lo relativo a la autenticidad de la transmisión de un mensaje.

Este modelo general muestra que hay cuatro tareas básicas en el diseño de un servicio de seguridad particular:

1. Diseñar un algoritmo para llevar a cabo la transformación relacionada con la seguridad. El algoritmo debe estar diseñado de forma que un oponente no pueda frustrar su finalidad.
2. Generar la información secreta que deba ser usada con el algoritmo.
3. Desarrollar métodos para distribuir y compartir la información secreta.
4. Especificar un protocolo para los dos interlocutores que hagan uso del algoritmo de seguridad y la información secreta, para obtener un servicio concreto de seguridad.

CAPÍTULO III

INFRAESTRUCTURA DE CLAVE PÚBLICA

El progresivo aumento de la digitalización está cambiando la manera en que se relacionan las personas y las organizaciones. La naturaleza inmaterial e impersonal de las comunicaciones electrónicas ha creado la necesidad de implementar mecanismos que permitan, cuando menos, comprobar la identidad de los interlocutores y la veracidad de los datos transmitidos, sobre todo en los sistemas abiertos como Internet. La Infraestructura de Clave Pública (Public Key Infraestructure), basada en la criptografía de claves asimétricas y en los conceptos de certificados digitales y autoridades de certificación, es una alternativa para que las aplicaciones provean servicios de seguridad como la autentificación, la confidencialidad, la integridad de los datos y el no rechazo de su origen.

Con anterioridad, en los Capítulos I y II, se sentaron las bases de los principales conceptos y elementos que forman parte de la Seguridad en Redes Informáticas. Es este capítulo está dedicado al estudio y análisis de las PKI.

3.1 Desarrollo histórico de la PKI

Hace 28 años los científicos hicieron el notable descubrimiento de que no se necesita compartir ningún secreto para cifrar los mensajes. En lugar del método tradicional en donde se codificaba y descifraba con la misma clave, dichos investigadores demostraron que se podía cifrar con una clave y decodificar con otra[26]. Entonces, la clave de cifrado se puede hacer pública, como un número telefónico. La clave de decodificación se mantiene en privado, como el teléfono de alguien.

Esto dio origen a la aparición de la Infraestructura de Claves Públicas, la cual permite la aplicación de muchas de las tecnologías usadas en la construcción de soluciones de protección para las redes [Nash, 2002]. Hasta hace muy poco, para la mayoría de las organizaciones la seguridad era cuestión de proteger el acceso a los datos corporativos. El tema más importante era cómo impedir que entraran a su sistema personas que lo dañaran o que vieran información exclusiva. La amplia disponibilidad de los sistemas en red dentro de las corporaciones, que comenzó a principios de la década de 1980, creó un nuevo entorno donde se podía compartir la información. Cuando los puntos de entrada con tecnología de conexiones de acceso telefónico y acopladores acústicos[27] permitieron el acceso a estas redes, se creó la oportunidad para el crecimiento de una nueva industria dedicada a proteger estos puntos de entrada.

Con la creciente disponibilidad de acceso a la red, la seguridad se convirtió en una cuestión de cómo crear la pared más sólida posible alrededor de los vulnerables y delicados sistemas internos de la empresas. Todos sabían que la seguridad de sistemas individuales era muy difícil de manejar y controlar, pero los perímetros controlados se convertían en un concepto manejable (hasta que alguien creó su propia conexión privada a Internet para su sistema interno). Básicamente, la seguridad se refería a la manera de detener a los bárbaros que arrasaban y se entrometían dentro de la red corporativa. Se debía tener mucho cuidado al enviar un mensaje a través de la red, pues era como si atravesara tierras hostiles entre ciudades amuralladas. Se creó todo un lenguaje de estrategias de defensa y se construyeron modelos basados en la mentalidad de la fortificación y las defensas del perímetro. Se crearon productos de autentificación para identificar a los residentes ante los guardias en las puertas de entrada. Se construyeron áreas donde se permitía el acceso externo a computadoras menos sensibles. Se crearon barreras de seguridad para separar las regiones dentro de la red y limitar el daño que los invasores pudieran causar cuando incursionaran en el sistema y quemaran los datos. Se construyeron sistemas para detectar intrusos y trampas.

Los retos de seguridad ahora son significativamente diferentes. El trabajo en red ha pasado de sus raíces medievales a un período renacentista. La adopción masiva de Internet como una base para el comercio electrónico ha transformado todo el modelo de seguridad. Desde luego, estamos interesados en mantener los

[26] Whitfield Diffie y Martin Hellman fueron los primeros en introducir el concepto de criptografía asimétrica a mediados de la década de 1970. El algoritmo se basa en las matemáticas de logaritmos discretos.

[27] El acoplador acústico es un módem que no necesita conectarse directamente a la línea telefónica, sino que se acopla a través del teléfono. Solo puede realizar la transmisión de datos a la velocidad máxima de 300 baudios (300 bits por segundo). Al igual que todos los módems, al realizar una comunicación entre dos puntos, un acoplador acústico hace de modulador y el otro de demodulador. Esta posibilidad normalmente se selecciona mediante un interruptor que posee el acoplador; por ello, al realizar una comunicación entre dos acopladores acústicos el interruptor del que transmite deberá estar en la posición contraria del interruptor del que recibe.

datos corporativos a salvo, pero el énfasis se ha desplazado hacia las necesidades de maximizar el libre comercio. Ayer, la seguridad se refería en primera instancia a limitar el acceso; en la actualidad se trata de maximizar el acceso a la gente correcta.

Muchos de los mecanismos de seguridad tradicionales siguen siendo esenciales (véase Figura 3.1), pero hay una diferencia significativamente: ya no existe un perímetro fuertemente custodiado. El estado actual del desarrollo de la PKI se debe considerar en perspectiva. En muchas formas, es similar al estado de la infraestructura de redes de comienzos de la década de 1980, lo cual significa que constantemente hay nuevos adelantos. Lo que hace muy agradable a la PKI como una propuesta es que hay cantidades de elementos verdaderamente novedosos con los que se puede trabajar.

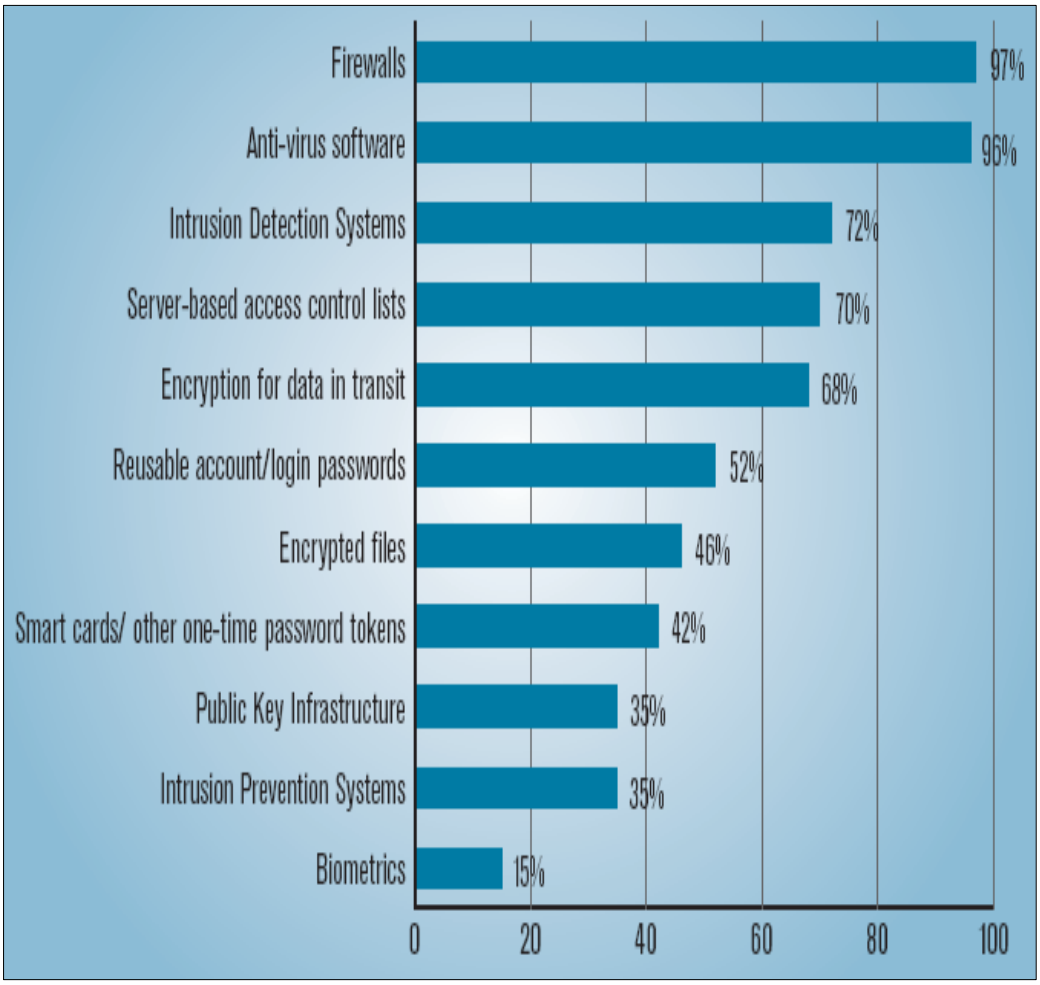


Figura 3.1 Porcentaje de las tecnologías de seguridad implementadas.

3.2 ¿Qué es una PKI?

Muchos protocolos de seguridad se apoyan en el cifrado de clave pública para proporcionar servicios como la confidencialidad, la integridad de los datos, la autenticación del origen de los datos y la irrebatibilidad. La finalidad de una PKI consiste en proporcionar una administración de claves y certificados eficiente y fiable que soporte estos protocolos. La PKI es un sistema de certificados digitales, autoridades emisoras de certificados (CA, Certificación Authority), servicios de administración de certificados y servicios de directorio (LDAP; X.500) que verifica la identidad y la autoridad de cada parte involucrada en cualquier transacción a través de Internet [Brown, 2001]. Las funciones de una PKI se pueden resumir de esta forma:

- **Registro**. El proceso en virtud del cual un sujeto se da a conocer a una CA (directamente o a través de una autoridad de registro [RA]) antes de que la CA emita un certificado o certificados para ese sujeto.
- **Inicialización**. El punto en el que el sistema de usuarios o cliente obtiene los valores necesarios para empezar a comunicarse con la PKI. Por ejemplo, la inicialización puede implicar dotar al sistema cliente con la clave pública o el certificado de una CA, o la generación de un par de claves pública/privada del propio sistema cliente.
- **Certificación**. El proceso en virtud del cual una CA emite un certificado para la clave pública de un sujeto y le devuelve ese certificado (o lo edita en un almacén).
- **Recuperación de pares de claves**. Si la CA ha generado y emitido el par de claves, la clave privada del usuario podrá o bien ser duplicada por una CA, o bien por un sistema de duplicación de claves aparte. Si un usuario o su empleador desea recuperar estos materiales de claves duplicados, la PKI deberá proporcionar un sistema que permita la recuperación sin que suponga un riesgo inaceptable para la clave privada.
- **Generación de claves**. Dependiendo de las normas de la CA, el par de claves pública/privada puede o bien ser generado por el usuario en su entorno local, o bien por la CA. En el último caso, los materiales de claves pueden ser distribuidos al usuario en un archivo cifrado o en un token físico (como una tarjeta inteligente o una tarjeta PCMCIA).
- **Actualización de las claves**. Todos los pares de claves deberán ser actualizados de forma regular (es decir, deberán ser sustituidos por un nuevo par de claves) y se deberán emitir nuevos certificados. Esto ocurre en dos casos: normalmente, cuando una clave ha pasado su tiempo de existencia máximo, y excepcionalmente, cuando se ha comprometido una clave y ésta debe ser sustituida.
- **Certificación cruzada**. Un certificado es emitido por una CA para otra CA; el certificado contiene una clave CA pública asociada a la clave de firma CA privada que se usa para emitir certificados. Normalmente, un certificado cruzado se usa para permitir a los sistemas cliente y a

las entidades finales de un dominio administrativo a fin de comunicar la seguridad con los sistemas cliente y con los usuarios finales de otro dominio administrativo.

- **Revocación**. Cuando se emite un certificado, se espera que esté en uso para el periodo de validez completo. Sin embargo, distintas circunstancias pueden hacer que un certificado se vuelva inválido antes de la expiración del periodo de validez. Tales circunstancias son, por ejemplo, el cambio de nombre, el cambio de asociación entre el sujeto y la CA (por ejemplo, un empleado que concluye su contrato de trabajo con una empresa), y el compromiso (real o presunto) de la clave privada correspondiente. En tales circunstancias, la CA deberá revocar el certificado.

3.2.1 Ventajas

La PKI resulta ideal en una Intranet, en la que se comparten documentos (trabajo en grupo), se accede a recursos de red (servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. La PKI resulta mucho más ágil que los sistemas tradicionales de control basados en nombre y contraseña y lista de control de acceso. Algunas ventajas son:

- Las claves no viajan a través de la red desde el cliente al servidor, dado que los certificados constituyen información pública.
- Ofrece mejores medios para identificar al usuario ya que los certificados contienen información verificable relacionada con la identidad del usuario, lo cual no ocurre en la autenticación basada en dirección IP del equipo del usuario, en nombre de dominio o en dirección de e-mail, dado que las direcciones IP pueden ser dinámicas, y los nombres de dominio y direcciones de e-mail pueden ser espiadas.
- Los usuarios pueden conectarse a diferentes servidores de una Intranet logueandose una sola vez.
- Los certificados basados en tecnología de clave pública proveen un mecanismo de autenticación más fuerte. Sólo el usuario conoce la forma de acceder a su clave privada.
- Simplificación en la administración y disminución de costos.

3.2.2 Desventajas

Existen algunos cuestionamientos que se realizan a esta infraestructura:

- La falta de interoperabilidad, ya que el solo hecho de ceñirse al estándar X.509 no garantiza en absoluto que dos certificados generados por dos sistemas diferentes sean mutuamente compatibles. Además, existen problemas de confianza entre CA de distintas organizaciones, que puede imposibilitar la verificación con éxito de cadenas de certificación cuya CA raíz sea desconocida o no confiable, invalidándose todo el esquema de la PKI.
- Un conflicto que permanece sin resolver es la seguridad de la clave privada con respecto al almacenamiento de la misma. Que un empleado guarde su clave privada en una PC resulta un hecho riesgoso partiendo de la base de que esa PC puede ser utilizada por varios miembros de la oficina. Como solución surge la aparición de las smart cards y entonces ahora la seguridad de la clave privada pasará a depender de la seguridad de estos dispositivos. No puede garantizarse el hecho de que una clave privada será únicamente utilizada por su dueño.
- El costo ha sido un problema desde el principio. Al no existir un mercado suficientemente maduro en la PKI, cada empresa que ofrece soluciones de clave pública factura en función de criterios diversos (por certificado, servidores instalados) y cobra honorarios también dispares, de manera que la inversión en la PKI como respuesta a las necesidades de seguridad y accesibilidad a los activos informáticos de la empresa puede resultar cuando menos inesperadamente elevada.
- La PKI termina presentando problemas de escalabilidad, cuando el número de certificados emitidos a los usuarios va creciendo, debido a que las listas de revocación deben ser consultadas en cada operación que involucre certificados y firmas digitales, si se desea una implementación seria y robusta de la PKI. Bien es cierto que el esquema de confianza vertical, promulgado por las estructuras de certificación en árbol, resulta más escalable que los modelos de confianza horizontal, como el adoptado por PGP[28], cuya problemática es tan seria que no se prevé solución satisfactoria.
- Finalmente, la tecnología de la PKI se le antoja un tanto esotérica al usuario final, que no termina de entender del todo la jerga relacionada. Acostumbrado a autenticarse sin más que introducir su nombre y contraseña, puede sentirse fácilmente rebasado por la complejidad tecnológica de las firmas digitales y demás funciones criptográficas.

[28] ***Proporciona un servicio de confidencialidad y de autentificación que se puede usar para el correo electrónico y aplicaciones de almacenamiento de ficheros. Fue diseñado por Phil Zimmerman.***

3.3 Cifrado básico

Múltiples y bien fundados estudios has puesto de manifiesto que en las distintas organizaciones sociales que han ido surgiendo a lo largo de la Historia, cuando el nivel de complejidad de las relaciones en ellas establecidas hacía necesario el intercambio de mensajes escritos, también aparecía con frecuencia la necesidad de que algunos de estos mensajes, por las razones que fuese, sólo pudieran ser entendidas por personas y en circunstancias concretas.

La Criptografía es una palabra derivada del griego *Kryptos* (oculto), y su uso antecede a la informática en cientos de años; es la pieza fundamental que está en la base de los mecanismos de autenticación, integridad y confidencialidad. Originalmente fue un arte que, a lo largo de los siglos, a ejercido una poderosa fascinación en el ser humano, agudizando su ingenio para encontrar nuevos y mejores métodos para encriptar la información que desea ocultar a terceros y que sólo puede ser leída por el destinatario, siempre y cuando cuente con la clave para descifrar el código secreto. Este arte-ciencia se remonta en sus orígenes hasta la época de los egipcios y los antiguos hebreos. Los primeros testimonios escritos deben ser de los espartanos (véase Figura 3.2) alrededor de 400 a.C.

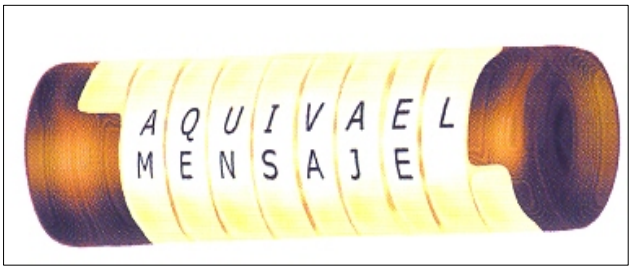


Figura 3.2 Un ejemplo de transposición histórico es el del escítalo espartano, el primer aparato criptográfico militar de la historia. El escítalo era un bastón, del que se tenían dos ejemplares idénticos. El emisor enrollaba una tira de cuero alrededor del bastón y escribía longitudinalmente sobre el mismo el mensaje que quería transmitir. Entonces se retiraba la cinta, quedando un mensaje incomprensible y se enviaba al destinatario, que disponía de una copia del escítalo. Al colocar la cinta sobre el bastón se recuperaba el mensaje, lo que era imposible si se desconocía el diámetro exacto del escítalo.

Los romanos utilizaron diversos métodos de codificación, entre ellos, la sustitución de cada letra del alfabeto por la correspondiente tres posiciones adelante (véase Figura 3.3). Éste método se conoce como el "Cifrado de César", pues fue Julio César quien lo utilizó constantemente para enviar sus mensajes secretos[29]. La criptografía moderna parte del año 1200 d.C., cuando comenzó a emplearse extensivamente entre los estados papales y las ciudades-Estado italianas.

Figura 3.3 En la criptografía de sustitución cada letra del alfabeto se sustituye por una letra del alfabeto cifrado; aquí, este último se ha movido cinco lugares con respecto al alfabeto normal.

[29] *Mensajes Ocultos, Revista de Tecnología Empresarial. Agosto 1999, pp. 39-42.*

Pero fue hasta 1470 cuando apareció la primera descripción de un aparato mecánico para el cifrado de un texto. El matemático francés Vignére, publicó, en 1856, un método de sustitución polialfabética, en el cual se sustituían las letras del alfabeto por números, A=0, B=1, C=2, etcétera. Este método fue usado ampliamente por los reyes franceses, para enviar mensajes a sus generales en el frente de batalla. Un método similar al de Vignére fue usado por el entonces gobernador del estado de Coahuila, Venustiano Carranza, cuando desconoce al gobierno de Huerta y se levanta en contra de él. Hoy en día, los algoritmos de encriptación, que se ejecutan en computadoras digitales de alta velocidad emplean sustitución y transposición combinadas, así como otras funciones matemáticas. Normalmente los mecanismos de cifrado utilizan un algoritmo (una función matemática) y un valor secreto, que se conoce como clave.

Son públicamente conocidos y están disponibles; es la clave la que se mantiene secreta y la que proporciona la seguridad requerida. La clave es similar a la combinación de un candado. Aunque el concepto de candado de apertura por combinación es bien conocido, no es posible abrirlo fácilmente si no se conoce la combinación [Maiwald, 2004].

Además, cuantos más números haya en una combinación, mayor será el trabajo a la hora de descifrar la combinación, al igual que ocurre con las claves de cifrado. Cuantos más bits haya en una clave, menos susceptible será de ser descifrada por un tercero. El número de bits necesario en una clave para garantizar el cifrado seguro en un entorno determinado puede ser controvertido. Cuanto más largo sea el espacio de claves (el intervalo de valores posibles de la clave), más difícil será descifrar la clave en un ataque de fuerza bruta (véase la Tabla 3.1).

Longitud de clave (en bits)	Número de combinaciones
40	2^{40} = 1.099.511.627.776
56	2^{56} = 7,205759403793 x 10^{16}
64	2^{64} = 1,844674407371 x 10^{19}
112	2^{112} = 5,192296585535 x 10^{33}
128	2^{128} = 3,402823669209 x 10^{38}

Tabla 3.1 Número de claves que hay que utilizar para agotar todas las posibilidades, con respecto a una longitud de clave concreta.

La tendencia natural consiste en utilizar la clave de mayor longitud disponible, lo que hace que la clave sea más difícil de descifrar. Sin embargo, cuanto más larga sea la clave, más onerosos serán los procesos de cifrado y descifrado. El objetivo es que el costo de descifrar la clave sea mayor que el valor de la información que ésta protege.

Hay dos tipos de funciones criptográficas que permiten la autenticación, la integridad y la confidencialidad: el cifrado simétrico de claves y el cifrado asimétrico de claves [Merike, 2003] y [Carracedo, 2004].

3.3.1 Cifrado simétrico

A la *encriptación simétrica* también se le llama *cifrado convencional*, de *clave secreta* o de *clave única*, ya que únicamente usa una clave, llamada *secreto compartido*, tanto para la encriptación como para la desencriptación (véase Figura 3.4).

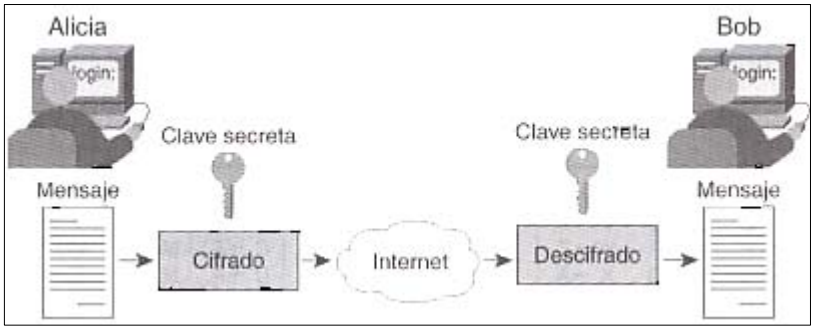


Figura 3.4 Cifrado de clave secreta.

Un esquema de cifrado simétrico tiene cinco componentes:

- **Texto claro**: es el mensaje o los datos originales que se introducen en el algoritmo como entrada.
- **Algoritmo de cifrado**: el algoritmo de cifrado realiza varias sustituciones y transformaciones en el texto claro.
- **Clave secreta**: la clave secreta es también una entrada del algoritmo. Las sustituciones y transformaciones realizadas por el algoritmo dependen de ella.
- **Texto cifrado**: el mensaje ilegible que se produce como salida. Dependen del texto claro y de la clave secreta. Para un mensaje determinado, dos claves diferentes producirían dos textos cifrados diferentes.
- **Algoritmo de descifrado**: es, básicamente, el algoritmo de cifrado ejecutado a la inversa. Toma el texto cifrado y la misma clave secreta, y genera el texto claro.

Es importante observar que la seguridad del cifrado simétrico depende de la privacidad de la clave, no de la del algoritmo. Es decir, se asume que no es práctico descifrar un mensaje teniendo el texto cifrado y conociendo el algoritmo de cifrado/descifrado. En otras palabras, no es necesario que el algoritmo sea secreto, lo único que hay que mantener en secreto es la clave. Esta característica del cifrado simétrico es la causa de su uso tan extendido, ya que es un método sencillo y fácil de usar, está diseñados para ser muy rápido y (por lo general) tiene un gran número de llaves posibles. Los mejores algoritmos de llaves simétricas ofrecen Confidencialidad casi perfecta: una vez que los datos son encriptados mediante una llave no hay forma de desencriptarlos sin poseer la misma llave.

Los algoritmos de llaves simétricas pueden dividirse en dos categorías: de bloque y de flujo. Los primeros encriptan los datos en bloque a la vez y los algoritmos de flujo encriptan byte por byte. La mayoría de los algoritmos de cifrado simétrico de bloque, incluido DES, tienen una estructura descrita inicialmente por Horst Feistel de IBM en 1973, y que se muestra en la Figura 3.5. Las entradas al algoritmo de cifrado son un bloque de texto claro de tamaño 2w bits y una clave K. El bloque de texto claro se divide en dos mitades, L_0 y R_0.

Las dos mitades de datos pasan a través de n etapas de procesamiento y luego se combinan para producir el bloque de texto cifrado. Cada etapa i tiene como entradas L_{i-1} y R_{i-1}, que se derivan de la etapa anterior, así como una subclave K_i generada a partir de K. En general, las subclaves K_i son diferentes a K y entre ellas mismas, y se generan a partir de la clave mediante un algoritmo de generación de subclaves. Hoy en día se emplean muchos algoritmos de llaves simétricas[30]. En la Tabla 3.2 se analizan algunos de los algoritmos simétricos que se encuentran comúnmente en el campo de la seguridad.

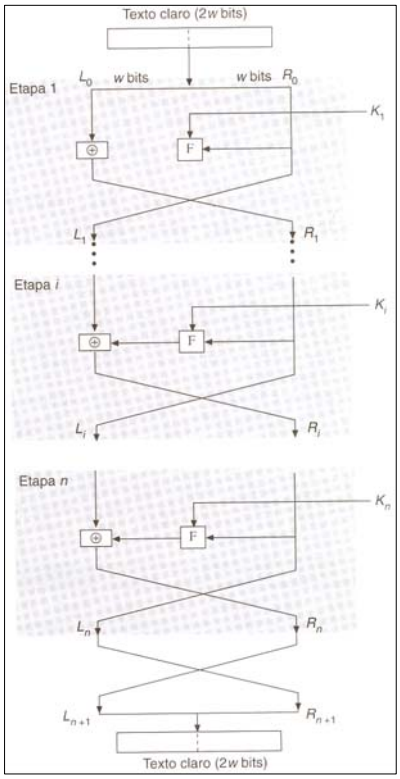


Figura 3.5 Red clásica de Feistel.

[30] *Puede ver una lista completa, incluyendo código fuente, en el libro Applied Cryptography de Bruce Schneier, editado por John Wiley & Sons, segunda edición, 1996.*

Nombre del algoritmo	Descripción
DES	El estándar de Encriptación de Datos fue adoptado como modelo del gobierno estadounidense en 1977, y como estándar ANSI en 1981. DES es un algoritmo de bloque que utiliza una llave de 56 bits y tiene varios modos de operación, de acuerdo con el propósito con el que se utilice DES es un algoritmo fuerte, pero se conjetura que es posible construir una máquina capaz de desencriptar un mensaje con DES a un costo menor de un millón de dólares.
DESX	Consiste en una sencilla modificación al algoritmo DES, construida alrededor de dos pasos de blanqueo. Estos pasos al parecer mejoran con mucho la seguridad del algoritmo, haciendo casi imposible la búsqueda de las llaves
TRIPLE–DES	Brinda una forma de, por lo menos, duplicar la seguridad de DES, mediante el uso del algoritmo tres veces con tres diferentes llaves (utilizar simplemente DES dos veces con dos diferentes llaves no mejora la seguridad al grado que se podría esperar, debido a un tipo teórico de ataque conocido como encontrarlo a la mitad, en el cual el atacante intenta, de modo simultáneo, encriptar el texto llano con una sola operación DES y desencriptar el texto cifrado con otra operación DES, hasta que se encuentra una correspondencia a la mitad). Triple-DES actualmente se utiliza en instituciones financieras y gobiernos como alternativa a DES
BLOWFISH	Blowfish (pez globo) es un algoritmo de bloque rápido, compacto y sencillo, inventado por Bruce Schneier. Permite una llave de longitud variable de hasta 48 bits, y está optimado para ejecutarse en procesadores de 32 y 64 bits.
IDEA	EL Algoritmo Internacional de Encriptación de Datos fue desarrollado en Zurich, Suiza, por James L. Massey y Xuejia Lai, y publicado en 1990. Utiliza una llave de 128 bits que se piensa es bastante segura. IDEA se utiliza dentro del popular programa PGP para encriptar archivos y correo electrónico.
RC2	Ronald Rivest desarrolló originalmente este algoritmo de bloque y RSA lo mantuvo como secreto comercial. Luego se divulgó en un mensaje anónimo en Usenet en 1996, y parece ser razonablemente seguro (aunque hay algunas llaves específicas que son débiles). RC2 se vende con una implementación que permite llaves de entre 1 y 2048 bits.
RC4	Este algoritmo de flujo fue desarrollado originalmente por Ronald Rivest y RSA Data Security lo mantuvo como secreto comercial. Fue divulgado también en un mensaje anónimo en Usenet en 1994, y parece ser razonable seguro (aunque hay algunas llaves específicas que son débiles). RC4 se vende con una implementación que permite llaves de entre 1 y 2048 bits.
RC5	Este algoritmo de bloque fue desarrollado por Ronald Rivest y publicado en 1994. RC5 permite que la longitud de la llave, el tamaño del bloque de datos, y número de pasadas de encriptación las defina el usuario.

Tabla 3.2 Algoritmos simétricos.

Existen otros algoritmos de clave privada disponibles en varios sistemas de seguridad, como son: Skipjack, Twofish, Cast-128, Gost, Rijndael , Safer, Deal, AST-256, MARS, Serpent, LOKI-97, FROG y HASTY PUDÍN. Algunos sistemas no son muy buenos para la protección de datos, pues permiten desencriptar la información sin conocer la llave correspondiente. Otros son bastantes resistentes aun a los ataques más obstinados. La capacidad de un sistema criptográfico para proteger información contra ataques se conoce como **fortaleza**, la cual depende de muchos factores, incluyendo:

- La confidencialidad de la llave.
- La dificultad de adivinar la llave o intentar todas las llaves posibles (una búsqueda de llaves). Las llaves más largas por lo general son más difíciles de adivinar o encontrar.
- La dificultad de invertir el algoritmo de encriptación sin conocer la llave (romper el algoritmo de encriptación).

- La existencia (o falta) de puertas traseras, es decir, formas adicionales de poder desencriptar un archivo encriptado más fácilmente sin conocer la llave.
- La habilidad de desencriptar un mensaje encriptado si se conoce cómo se desencripta una parte de él (conocido como ataque de texto llano conocido).
- Las propiedades del texto llano y el conocimiento de estas que tenga un atacante; por ejemplo, un sistema criptográfico puede ser vulnerable al ataque si todos los mensajes encriptados con él comienzan o terminan con un fragmento conocido de texto llano. Los aliados emplearon este tipo de propiedades para romper el código alemán Enigma durante la Segunda Guerra Mundial.

Hablando en términos generales, la encriptación de clave privada es rápida y puede ser fácil de implementar tanto en hardware como en software, pero tiene un problema: la clave debe compartirse entre el emisor y el receptor de los datos, por lo que debe disponerse de un método seguro de intercambio de claves. De otra forma, si una tercera persona intercepta la clave durante el intercambio podría desencriptar los datos con facilidad.

3.3.2 Cifrado asimétrico

Todos los sistemas criptográficos presentados anteriormente, desde los más primitivos a los más modernos, comparten una filosofía de funcionamiento común: el proceso de cifrado y el de descifrado se realizan con la misma clave. Además, básicamente, todos estos algoritmos se basan en técnicas de sustitución y de permutación de bits o caracteres para conseguir el oscurecimiento del mensaje. Con la publicación, en 1976, por W. Diffie y M. Hellman de su artículo «New Directions in Cryptograghy», donde se proponía un nuevo tipo de cifradores, se inaugura una nueva manera de concebir el cifrado de mensajes que rompe con una tradición milenaria. Surgen así los **criptosistemas asimétricos o de clave pública**, en los que la llave usada para cifrar el mensaje es distinta de la que se requiere para el descifrado. En esta nueva y revolucionaria concepción de la Criptografía, los algoritmos se basan en la transformación del mensaje mediante funciones matemáticas, en lugar de revolverlo mediante técnicas de difusión y confusión. El uso de dos claves tiene importantes consecuencias en el terreno de la Confidencialidad, la distribución de claves y la Autentificación. Un esquema de cifrado de clave pública tiene los siguientes componentes (véase Figura 3.6):

- **Texto claro:** consiste en el mensaje o los datos legibles que se introducen en el algoritmo como entrada.
- **Algoritmo de cifrado:** el algoritmo de cifrado realiza diferentes transformaciones en el texto claro.
- **Clave pública y privada:** es una pareja de claves que han sido seleccionadas, de las cuales una se usa para el cifrado y la otra para el descifrado. Las transformaciones exactas llevadas a cabo por el algoritmo de cifrado dependen de la clave pública o privada que se proporciona como entrada.

- **Texto cifrado:** es el mensaje desordenado producido como salida. Depende del texto claro y de la clave. Para un mensaje dado, dos claves diferentes producirán dos textos cifrados diferentes.
- **Algoritmo de descifrado:** este algoritmo acepta el texto cifrado y la clave correspondiente y produce el texto claro original.

Como lo mencionamos anteriormente, las claves tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves asociadas también lo son, y viceversa.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el algoritmo. Ambas claves, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

A continuación se detallan algunos de los usos más comunes de los algoritmos de clave pública:

- Integridad de los datos.
- Confidencialidad de los datos.
- Irrebatibilidad del emisor.
- Autenticación del emisor.

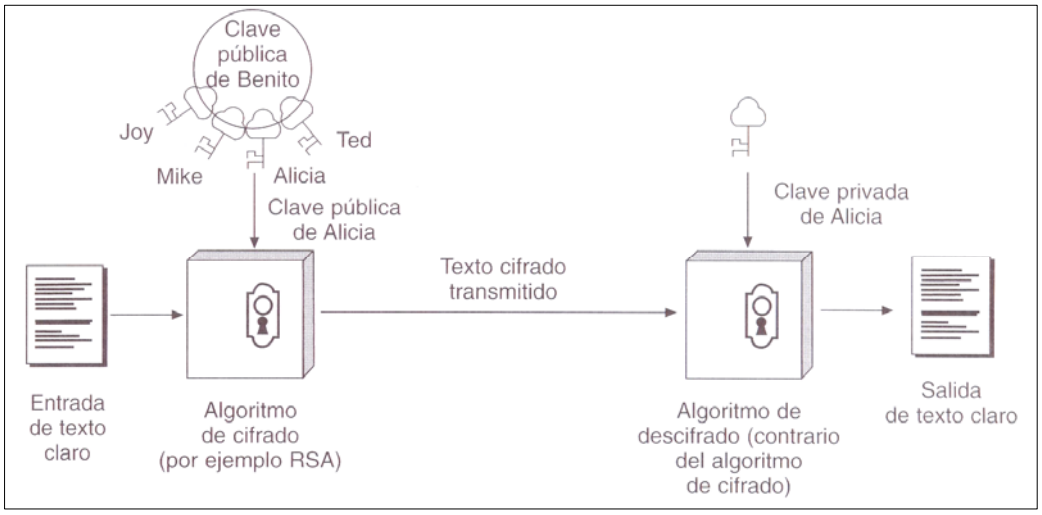


Figura 3.6 Criptografía de clave pública.

La confidencialidad de los datos y la autenticación del emisor pueden conseguirse utilizando el algoritmo de clave pública. La Figura 3.7 muestra cómo la integridad y la confidencialidad de los datos se proporciona utilizando el cifrado de clave pública.

Por ejemplo, la confidencialidad de los datos se asegura cuando Alicia (véase Figura 3.7) envía el mensaje original, porque Bob es el único que puede descifrar el mensaje con su clave privada. La integridad también se mantiene porque, para modificar el mensaje, un usuario malintencionado necesitaría la clave de Bob. La integridad y la confidencialidad de los datos también se garantiza para la respuesta, porque sólo Alicia tiene acceso a su clave privada y es la única que puede modificar o descifrar la respuesta con su clave privada.

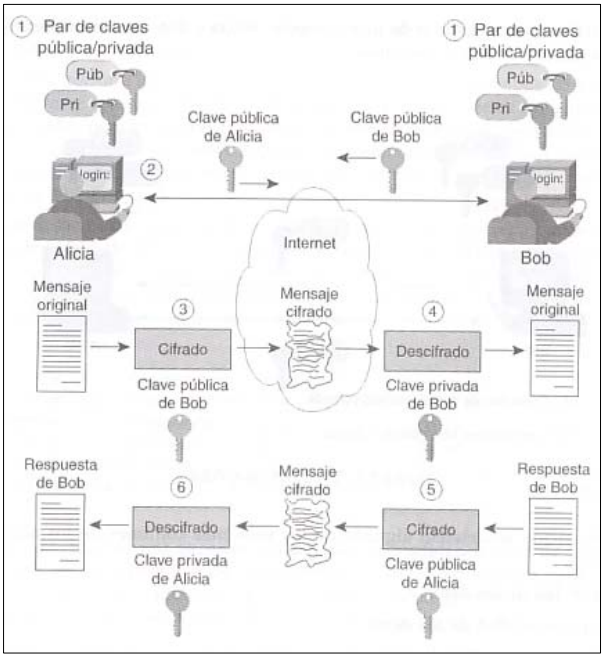


Figura 3.7 Mantenimiento de la integridad y la confidencialidad de los datos con el cifrado de clave pública.

Sin embargo, este intercambio no es muy seguro, porque es fácil que un tercero se haga pasar por Alicia y envíe un mensaje a Bob cifrado con la clave pública de él. La clave pública está a disposición de todo el mundo. La Figura 3.8 muestra cómo el cifrado de clave pública resuelve este problema y garantiza la autenticación y la irrebatibilidad del emisor. Un intercambio autenticado se garantiza porque solamente Bob y Alicia tienen acceso a sus respectivas claves privadas. Bob y Alicia cumplen los requisitos de irrebatibilidad (luego no pueden negar haber enviado el mensaje si sus claves no han sido reveladas). Esto, por supuesto, lleva a otro debate sobre la honestidad de Bob y Alicia; ellos pueden negar haber enviado mensajes indicando únicamente que sus claves privadas han sido descubiertas.

Si queremos utilizar el cifrado de clave pública para llevar a cabo intercambios autenticados y para garantizar la confidencialidad y la integridad de los datos, será necesario utilizar el doble cifrado. Alicia primero cifraría su mensaje confidencial a Bob con la clave pública de este y luego lo cifraría de nuevo con su propia clave privada. Cualquier persona sería capaz de descifrar el mensaje para llegar al mensaje cifrado intercalado, pero Bob sería el único capaz de descifrar el mensaje cifrado con su clave privada.

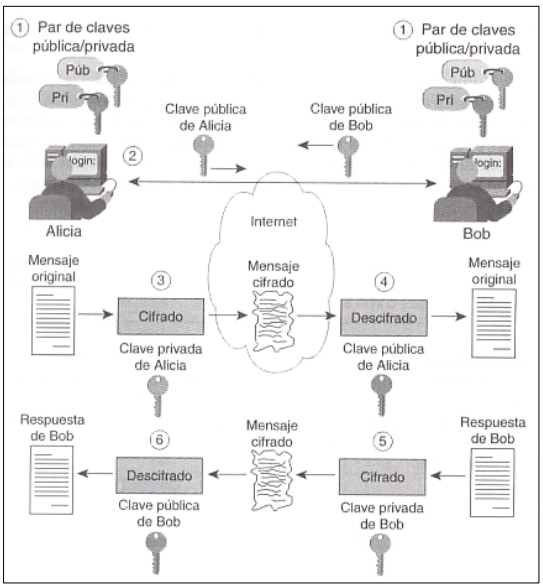


Figura 3.8 Autenticación e irrebatibilidad del emisor utilizando el cifrado de clave pública.

A continuación, en la Tabla 3.3 se resumen los sistemas de llave pública que se utilizan comúnmente en la actualidad:

Nombre del sistema	Descripción
Intercambio de llaves Diffie–Hellman	Sistema para intercambio de llaves criptográficas entre partes activas. Diffie-Hellman no es en realidad un método de encriptación y desencriptación sino un método para desarrollar e intercambiar una llave privada compartida mediante un canal de comunicación público. A fin de cuentas, ambas partes acuerdan utilizar algunos valores numéricos comunes, y luego cada una de ellas crea una llave. Se intercambian transformaciones matemáticas de las llaves. Cada parte puede calcular entonces una tercera llave de sesión, la cual no puede ser fácilmente derivada por un atacante que conozca ambos valores intercambiados.
RSA	Es un sistema criptográfico de llave pública bien conocido, desarrollado por Ronald Rivest, Adi Shamir y Leonard Adleman; RSA puede ocuparse para encriptar información y como fundamento de un sistema de firmas digitales. Las firmas digitales pueden utilizarse para probar la autoría y autenticidad de información digital. La llave puede tener cualquier longitud, dependiendo de la implementación que se utilice.
ELGAMAL	Llamado así en honor a su creador, Taher ElGamal, este es un sistema de encriptación de llave pública basado en el protocolo de intercambio de llaves Diffie-Hellman. En forma similar a RSA, ElGamal puede emplearse tanto para encriptación como para firmas digitales.
DSS	El Estándar de Firmas Digitales (DSS, Digital Signature Standard) fue desarrollado por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y adoptado como Estándar de Procesamiento de Información Federal (FIPS) por el Instituto Nacional de Estándares y Tecnología (NIST). DSS se basa en el algoritmo de firmas digitales (DSA). Aunque DSA permite utilizar llaves de cualquier longitud, bajo el DSS de FIPS solo se permiten llaves de 512 y 1024 bits. DSS especifica que solo puede ocuparse para firmas digitales, aunque es posible utilizar implementaciones de DSA también para encriptación.
Curva Elíptica	En 1985, Neil Koblitz y Victor Miller propusieron el Elliptic Curve Cryptosystem (ECC), o Criptosistema de Curva. El algoritmo cuya seguridad descansa en el mismo problema que los métodos de Diffie-Hellman y DSA, pero en vez de usar números enteros como los símbolos del alfabeto del mensaje a encriptar (o firmar), usa puntos en un objeto matemático llamado Curva Elíptica. ECC puede ser usado tanto para encriptar como para firmar digitalmente.

Tabla 3.3 Sistemas de llave públicas.

3.3.2.1 Funciones hash

El **resumen** o **valor hash** del mensaje M es un elemento de información de tamaño fijo generado mediante una función unidireccional que también puede ser utilizado como autenticador de mensajes (véase Figura 3.9). No obstante, el verdadero interés de las funciones hash radica en que son parte fundamental en la estructura de los algoritmos de firmado. Por tratarse de funciones unidireccionales (one way functions), el cálculo de la función directa es computacionalmente fácil de realizar, pero la operación inversa es computacionalmente impracticable [Carracedo, 2004].

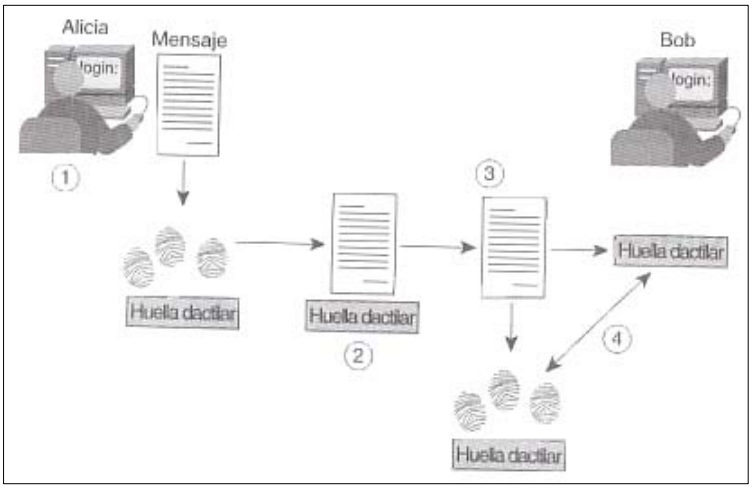


Figura 3.9 Uso de una función hash para la integridad de los datos.

Al igual que con el código de autentificación de mensajes, una función hash acepta un mensaje de tamaño variable, M, como entrada y produce un resumen del mensaje de tamaño fijo H(M) como salida. A diferencia del MAC, una función hash no acepta una clave secreta como entrada. Para autentificar un mensaje, el resumen se envía con el mensaje, con lo cual se verifica la autenticidad del resumen. La Figura 3.10 ilustra tres formas de autentificar un mensaje. El resumen del mensaje puede ser cifrado por medio de cifrado convencional (parte a); si sólo el emisor y el receptor comparten la clave de cifrado, la autentificación está organizada. El mensaje también puede ser cifrado por medio de cifrado de clave pública (parte b). El enfoque de clave pública tiene dos ventajas: proporciona una firma digital además de autentificación del mensaje y no necesita la distribución de claves a las partes que se comunican entre sí. La ventaja que tienen estos dos enfoques sobre las perspectivas que cifran el mensaje completo es que implican un costo computacional menor.

La Figura 3.10c muestra una técnica que emplea una función hash y no usa cifrado para la autentificación de un mensaje. Esta técnica implica que dos partes que se comunican, A y B, comparten un valor secreto común S_{AB}. Cuando A tiene un mensaje que enviar a B, calcula la función hash de la

concatenación del valor secreto y el mensaje $MD_M = H(S_{AB} || M)$[31]. Luego envía [M || MD_M] a B Como B posee S_{AB}, puede volver a calcular $H(S_{AB} || M)$ y verificar MD_M. Como la clave secreta no se ha enviado, no es posible que un oponente modifique un mensaje interceptado. Mientras el valor secreto permanezca como tal, tampoco es posible que un oponente genere un nuevo mensaje.

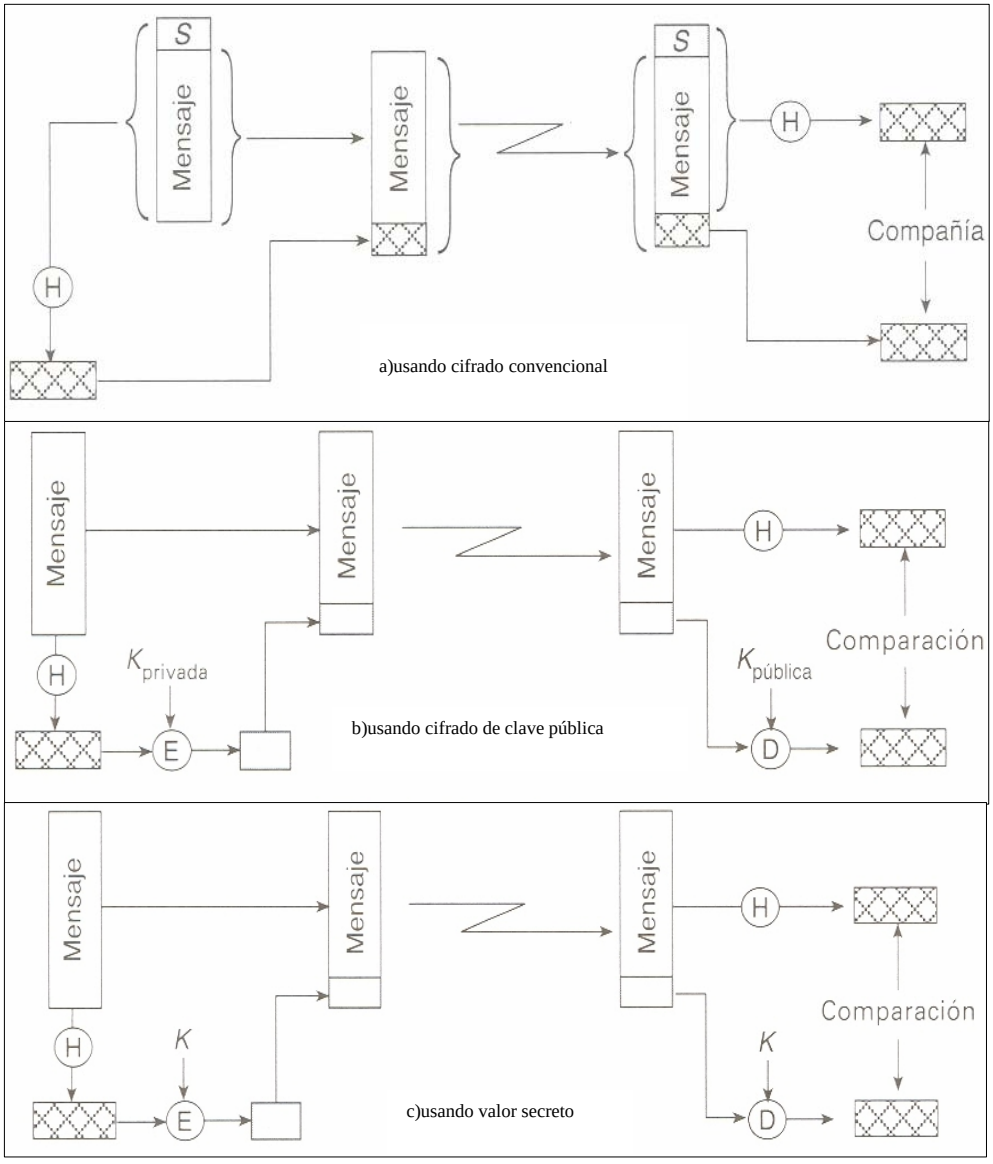


Figura 3.10 Autentificación de mensaje por medio de una función hash unidireccional.

[31] || indica concatenación.

Para que resulte útil a la autentificación de mensajes, una función hash H debe poseer las siguientes propiedades:

1.- H puede aplicarse a un bloque de datos de cualquier tamaño.

2.- H produce una salida de tamaño fijo.

3.- H(x) es relativamente fácil de computar para cualquier x dado, haciendo que tanto las implementaciones de hardware como de software sean prácticas.

4.- Para cualquier valor h dado, es imposible desde el punto de vista computacional encontrar x tal que H(x) = h, con frecuencia, se conoce en la literatura como propiedad **unidireccional**.

5.- Para cualquier bloque dado x, es imposible desde el punto de vista de computo , encontrar $y \neq x$ con H(y) = H(x), lo que a veces se conoce como **resistencia débil a la colisión**.

6.- Es imposible desde el punto de vista computacional encontrar un par (x, y) tal que H(x) = H(y), lo que normalmente se conoce como **resistencia fuerte a la colisión**.

Las tres primeras propiedades son requisitos para la aplicación práctica de una función hash a la autentificación de mensajes. La cuarta propiedad es la propiedad unidireccional: dado un mensaje, es fácil generar un código, pero dado un código, es prácticamente imposible generar un mensaje. Esta propiedad es importante si la técnica de autentificación implica el uso de un valor secreto (Figura 3.10c). El valor secreto no se envía; sin embargo, si la función hash no es unidireccional, un oponente puede descubrir fácilmente el valor secreto: si el oponente puede observar o interceptar una transmisión, obtiene el mensaje M y el código hash $MD_M = H(S_{AB} || M)$. Entonces el oponente invierte la función hash para obtener $S_{AB} || M = H^{-1}(MD_M)$. Debido a que ahora el oponente tiene M y $S_{AB} || M$, no tiene importancia recuperar S_{AB}. La quinta propiedad garantiza que es imposible encontrar un mensaje alternativo con el mismo valor hash que un mensaje dado. Esto evita la falsificación cuando se usa un código hash cifrado (Figuras 3.10a y b). Si no se diera esta propiedad, un oponente conseguiría, primero, observar o interceptar un mensaje y su código hash cifrado; segundo, generar un código hash no cifrado desde el mensaje; y tercero, generar un mensaje alternativo con el mismo código hash.

Una función hash que cumpla las cinco primeras propiedades se denomina función hash débil. Si también posee la sexta propiedad, se denomina función hash robusta. La sexta propiedad protege de un tipo sofisticado de ataque conocido como ataque basado en la paradoja del cumpleaños[32]. Además de proporcionar autentificación, un resumen de un mensaje también proporciona integridad de los datos. Realiza la misma función que una secuencia de comprobación: si cualquier bit del mensaje se altera accidentalmente durante la transmisión, el mensaje del mensaje dará error. Las funciones hash más comunes son:

[32] *Se trata de una clase de ataques por fuerza bruta. El nombre viene de la paradoja del cumpleaños: la probabilidad de que dos o más personas en un grupo de 23 personas cumplan años el mismo día es superior a 1/2. Si una función retorna uno de k valores equiprobables cuando se le proporciona una entrada aleatoria, cuando le proporcionamos repetidamente valores de entrada distintos, obtendremos dos salidas iguales después de* $1.2k^{1/2}$ *ejecuciones. Si buscamos una colisión en una función de dispersión, por la paradoja del cumpleaños sabemos que después de probar* $1.2 * 2^{pi/2}$ *entradas tendremos alguna.*

- Algoritmo Message Digest 4 (MD4).
- Algoritmo Message Digest 6 (MD5).
- Algoritmo hash seguro (SHA).

MD4 y MD5 fueron diseñados por Ron Rivest; SHA fue desarrollado por el NIST. Actualmente, MD5 y SHA son las funciones hash que más se utilizan para la implementación de la seguridad, ya que ambas están basadas en MD4. MD5 procesa las entradas de bloques de 512 bits y genera un conjunto de mensajes de 128 bits. SHA también procesa sus entradas en bloques de 512 bits, pero genera un conjunto de mensajes de 160 bits. SHA requiere más capacidad del procesador y suele ejecutarse sensiblemente más despacio que MD5.

3.3.2.2 Firmas digitales

Durante siglos y siglos, la firma caligráfica (ó signatura) ha sido un mecanismo de autenticación en el intercambio convencional de documentos escritos que ha gozado de un predicamento notable y que tiene una importancia de primer orden en todos los ámbitos sociales, tanto en las comunicaciones personales como en las relaciones económicas y jurídicas. Podemos definir la firma digital como una pieza de información añadida a una unidad de datos, que es el resultado de una transformación criptográfica de ésta en la que se ha usado una información privada del signatario, que permite a una entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos, es decir que es un conjunto de mensajes cifrado que se adjunta a un documento (véase Figura 3.11). Este mecanismo define a su vez dos procesos:

1. Firmado de una pieza digital de información por parte del **firmante** o **signatario**.
2. Verificación de una pieza de información firmada.

A partir del documento original m, mediante un proceso de firma se genera:

$$f = A_{sig}(m)$$

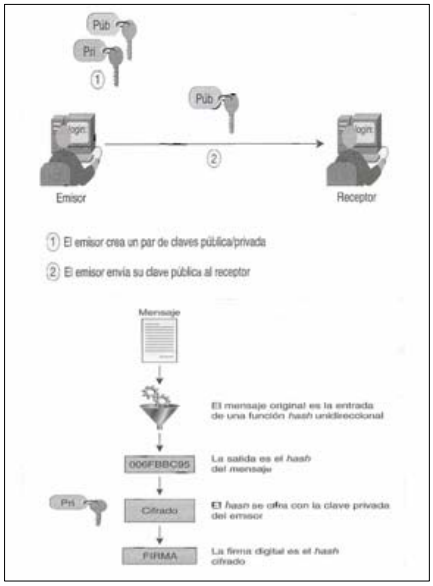


Figura 3.11 Creación de una firma digital.

El documento firmado es el conjunto formado por la concatenación de m y f. Tras la recepción del mensaje firmado por parte de la entidad verificadora, mediante un proceso de verificación se genera una información que indica la validez o falsedad de la firma. Conforme a estos planteamientos, además, para acercar más la definición a los casos que nos interesan, podemos imponer dos nuevas condiciones:

- La firma f debe ser de longitud reducida e independiente del tamaño de m.
- La generación de la firma se realiza a partir del resumen (hash) del mensaje m mediante un proceso de cifrado en el que se utiliza la clave privada del signatario que la emite.

Podemos considerar tres tipos de firma[33]:

- **Firma simple:** La firma simple de m sería el mero cifrado con la clave privada (secreta) del firmante.
- **Firma digital:** Se realiza a partir del resumen (hash) del mensaje m mediante un proceso de cifrado en el que se utiliza la clave privada del firmante.
- **Firma electrónica:** Consiste en una firma digital con informaciones añadidas para potenciar su validez.

En los tres casos el mensaje firmado es el conjunto de m y de la firma f. Para verificar la validez de una firma, además de conocer la clave pública del firmante:

- En el caso de firma digital y firma electrónica es necesario conocer m para poder obtener el resumen.
- En el caso de firma simple si m es inteligible (por ejemplo un contrato) bastaría sólo con la firma f. Si el mensaje es ininteligible (por ejemplo una clave criptográfica) para una verificación que aporte confianza al verificador es necesario (conveniente) disponer no sólo de la firma sino también de m.

Las firmas digitales no proporcionan confidencialidad a los contenidos del mensaje. Sin embargo, a menudo es más importante saber quién es el emisor del mensaje que esconder sus contenidos. Es posible que se desee la autenticación y la integridad del mensaje sin confidencialidad, como es el caso de las actualizaciones de enrutamiento en una red. Los contenidos de enrutamiento pueden no ser confidenciales, pero es vital verificar que la actualización procede de una fuente fiable. Algunos de los algoritmos de firma digital de clave pública más comunes son el algoritmo Ron Rivest, Adi Shamir y Leonard Adleman (RSA) y el algoritmo Digital Signature Standard (DSS, estándar de firma digital)[34].

[33] A estas definiciones de firma habría que añadir la firma a ciegas o firma opaca, que esta involucrada en los servicios de anonimato. Además, en las definiciones del ETSI se distingue, a su vez, entre distintas clases de Firma Electrónica (con sus distintos nombres), en la directiva de la Unión Europea se introduce la categoría de Firma Electrónica Avanzada y en la legislación española se tipifica la Firma Electrónica Reconocida.

[34] Es el estándar propuesto para la firma digital y forma parte del proyecto gubernamental Capstone. Fue seleccionado por el NIST, en cooperación con la NSA, para ser el estándar de identificación digital del gobierno de los Estados Unidos, y se basa en el algoritmo de clave pública de ElGamal. Comparado con el RSA, el DSS genera las claves más rápidamente y tiene el mismo rendimiento para la creación de firmas, pero es mucho más lento para su verificación.

3.3.2.3 Certificados digitales

Un certificado digital[35] en un mensaje firmado digitalmente que se suele usar para atestiguar la validez de la clave pública de un empleado. Los certificados necesitan un formato común, y actualmente están basados mayoritariamente en el estándar ITU-T X.509 (véase Figura 3.12). Más adelante, se explicara con más detalle los certificados digitales.

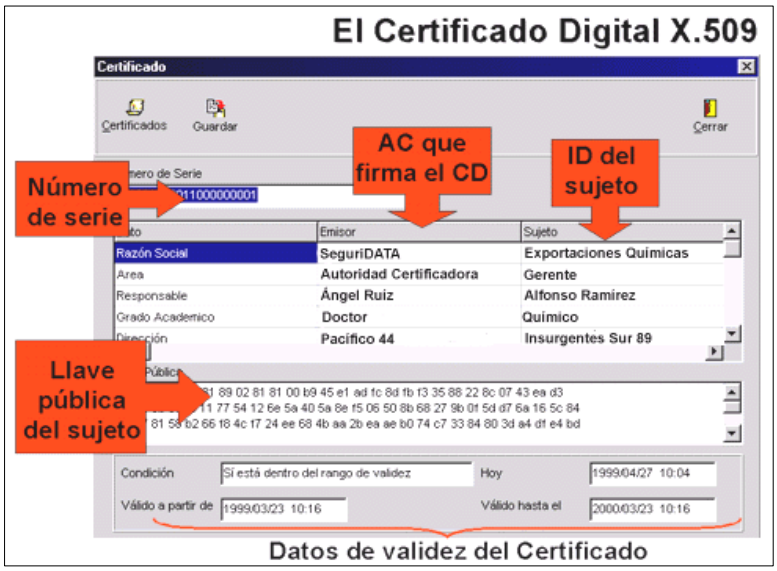


Figura 3.12 Ejemplo de un certificado digital.

3.3.2.4 Administración de claves

La gestión de claves es un problema difícil en las comunicaciones, debido más bien a factores sociales. Existen mecanismos criptográficamente seguros para la creación y distribución de claves. Sin embargo, el eslabón más débil en cualquier sistema es el que compete a las personas el mantenimiento de la confidencialidad de las claves. La administración de las claves[36] no tiene que ver sólo con la protección de las mismas mientras que están en uso. También tiene que ver la creación de claves robustas, la distribución segura de claves de usuario, la certificación de que estás sean correctas y la revocación de las mismas cuando hayan sido comprometidas o hayan caducado [Nash, 2002] y [Maiwald, 2004].

[35] *Loren Kohnfelder definió en 1978 el termino "certificado digital" como un documento firmado digitalmente, que contiene tanto un nombre como una clave pública.*

[36] *La administración de las claves que se trata aquí se concentra en las claves públicas/privadas y no en las claves simétricas. La gestión de las claves es un problema complejo, pero de ninguna manera tan difícil como la administración de un sistema puro de claves simétricas.*

3.3.2.4.1 Generación de claves

El tamaño de las claves generadas para un algoritmo cifrado en particular determina directamente la dificultad para descifrar una clave específica. En general, la cantidad de potencia de procesamiento y el tiempo necesario crecen muy rápidamente, a medida que el número de bits de la clave aumenta. La recomendación general para las longitudes de claves RSA es de 1024 bits para su uso personal y 2048 bits para claves más sensibles, como las que utilizan las CA para firmar certificados de entidades destino. Obviamente, las claves deben ser creadas con cuidado. Ciertas claves tienen un rendimiento de seguridad deficiente respecto a ciertos algoritmos, Por ejemplo, una clave compuesta únicamente de ceros cuando se utiliza con DES no proporciona una seguridad robusta. Asimismo, cuando se crean claves para su uso con RSA, debe tenerse cuidado para elegir p y q del conjunto de los números primos[37]. La mayor parte de los sistemas de encriptación tienen algún método para generar claves. En algunos casos, se permite que los usuarios elijan la clave al seleccionar una contraseña. En este caso, puede ser inteligente enseñar a los usuarios cómo elegir contraseñas robustas que incluyan números y caracteres especiales. De otro modo el espacio total de claves se reduce significativamente (esto permite búsquedas más rápidas de las claves aplicando la fuerza bruta). Algunas claves son elegidas mediante números aleatorios. Por desgracia, existen muy pocos generadores de números verdaderamente aleatorios. La mayoría son pseudo-aleatorios (lo que quiere decir existen patrones que se repetirán en algún momento). Si el generador no es verdaderamente aleatorio, puede ser posible predecir el siguiente número.

3.3.2.4.2 Distribución de claves

Las claves han sido generadas y ahora deben llegar a diversas localidades y equipos para ser usadas. Si la clave no se protege durante el tránsito, puede ser copiada o hurtada, y todo el sistema de encriptación quedará inseguro. Por tanto, el canal de distribución debe ser seguro por sí mismo. Las claves podrían ser colocadas fuera de banda. En otras palabras, las claves podrían ser transportadas personalmente por los administradores. Esto puede funcionar si los sitios remotos se encuentran apartados por distancias cortas. No obstante, existe una solución parcial a este problema. Puede ser posible utilizar el intercambio de clave Diffie-Hellman para crear y distribuir muchas claves de sesión (claves a corto plazo utilizadas para una sesión simple o una pequeña cantidad de tráfico). Esto puede reducir la necesidad de viajar a localidades remotas.

[37] Un número primo es aquel que sólo se puede dividir exactamente por sí mismo y por la unidad. Si se manejan números aleatorios muy grandes, el tiempo que se requiere para determinar si el número es primo, es tedioso y muy amplio, de manera que se utilizan métodos probabilísticos para establecer el carácter primo del número. Si estos métodos no están bien diseñados, se puede llegar a la conclusión de que los números no son realmente primos.

3.3.2.4.3 Certificación de la clave

Si las claves son transmitidas hacia un destino remoto por algún medio, deben ser verificadas una vez que lleguen, para asegurarse de que no han sido alteradas durante el tránsito. Esto puede ser un proceso manual o puede realizarse mediante algún tipo de firma digital. Las claves públicas están destinadas a ser divulgadas o proporcionarse a otros usuarios, y también deben ser certificadas como pertenecientes al propietario. Esto puede hacerse a través de una autoridad central (normalmente conocida como una autoridad de certificación, o CA. En este caso, la CA proporciona una firma digital en la clave pública y esto certifica que la CA considera que la clave pública pertenece al propietario del par de claves (véase la Figura 3.13).

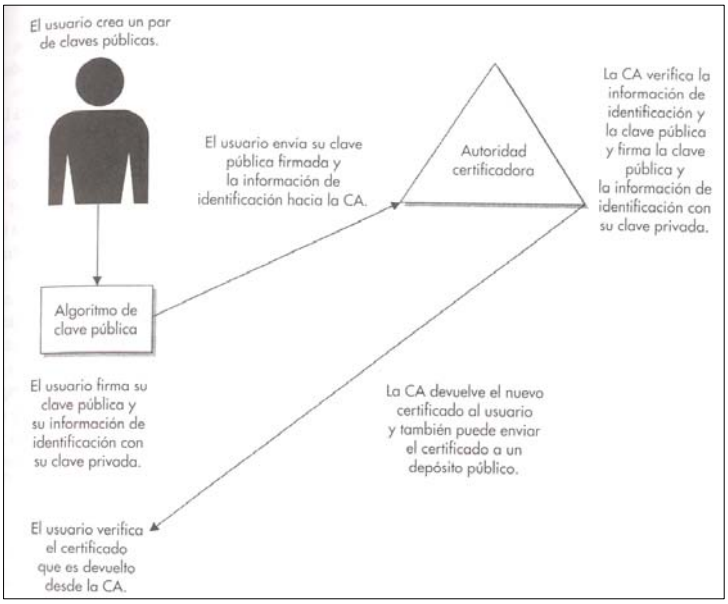


Figura 3.13 Las claves públicas son certificadas por autoridades certificadoras.

3.3.2.4.4 Protección de la clave

Las claves públicas de un par clave público no requieren de protección de la confidencialidad. Únicamente requieren la protección de la integridad proporcionada por su certificación. La clave privada de un par clave público debe ser protegida en todo momento. Si un atacante obtuviera una copia de la clave privada, podría leer todo el tráfico confidencial dirigido hacia el propietario del par clave, así como información firmada digitalmente como si él fuera el propietario del par clave. La protección de la clave privada incluye todas las copias de la misma. Por tanto, el archivo que mantiene la clave debe quedar protegido igual que cualquier cinta de respaldo que pueda incluir el archivo. La mayor parte de los sistemas protegen la clave privada con una contraseña. Esto protegerá la clave del fisgoneo casual, pero no de un ataque mediante fuerza bruta. Sin embargo, la mejor manera de proteger la clave es evitar que un atacante obtenga el acceso al archivo en primer lugar. Todas las claves para un sistema de clave privada deben ser

protegidas. Si la clave se mantiene en un archivo, éste debe ser protegido dondequiera que pueda residir (incluyendo cintas de respaldo). Si la clave residirá en la memoria, debe tenerse cuidado de proteger el espacio de memoria de algún examen que pueda ser llevado a cabo por un usuario o por un proceso. Igualmente, en el caso de un depósito central, el archivo central debe ser protegido, puesto que puede incluir la clave.

3.3.2.4.5 Revocación de la clave

Las claves no tienen vidas infinitas. Las claves de sesión solamente pueden existir para una sesión dada. Puede no haber ninguna necesidad de revocar la clave si está es eliminada al final de la sesión. Algunas claves pueden ser certificadas para un periodo dado. Hablando en términos generales, los pares públicos son certificados para uno o dos años. La clave pública certificada identificará la fecha de caducidad. Los sistemas que leen el certificado no lo considerarán válido después de esa fecha, de modo que casi no hay necesidad de revocar un certificado caducado. Sin embargo, las claves también pueden perderse o ser comprometidas. Cuando esto ocurre, el propietario de la clave debe informar a los otros usuarios que la clave ya no es válida y debería ser utilizada. En el caso de un sistema de encriptación de clave privada, si una clave es comprometida (y si los usuarios del sistema lo saben) pueden comunicarse esta información entre sí y comenzar a utilizar una nueva clave. El caso de los sistemas de encriptación de clave pública es un poco diferente. Si un par de clave está comprometido y es revocado, no hay forma obvia para informar a todos los usuarios potenciales de que la clave pública ya no es válida. En algunos casos, las claves públicas son publicadas en servidores de clave. Alguien que desee comunicarse con el propietario de la clave puede acudir al servidor una vez para recuperar la clave pública certificada.

3.3.2.4.6 Transporte de claves

Como no existe una API[38] (Application Programming Interface, Interfaz de Programación de Aplicaciones) única común para acceder a los almacenes de claves, el método alterno para compartir claves es suministrar mecanismos de importación/exportación que permitan la transferencia de las claves entre almacenes de claves. El estándar PKCS #12[39] define un contenedor de almacenamiento cifrado que se puede usar como un formato de intercambio para transferir con seguridad las claves entre almacenes de claves. Netscape , Microsoft y muchos otros desarrolladores de aplicaciones han implantado el PKCS #12 con este propósito. Se pueden compartir las claves utilizando contenedores PKCS #12 para trasladarlas de una

[38] Es un conjunto de especificaciones de comunicación entre componentes software. Representa un método para conseguir abstracción en la programación, generalmente (aunque no necesariamente) entre los niveles o capas inferiores y los superiores del software. Uno de los principales propósitos de una API consiste en proporcionar un conjunto de funciones de uso general, por ejemplo, para dibujar ventanas o iconos en la pantalla. De esta forma, los programadores se benefician de las ventajas de la API haciendo uso de su funcionalidad, evitándose el trabajo de programar todo desde el principio.

[39] Este estándar especifica un formato portable para almacenar o transportar las llaves privadas de un usuario, los certificados, los secretos misceláneos, etc. Para más información: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf.

aplicación a otra; dichos contenedores se pueden transportar en mensajes de correo, archivos o en protocolos de red generales como el HTTP.

3.4 Análisis de los componentes de la PKI

Una PKI es un marco de seguridad basado en certificados digitales. La PKI proporciona un sistema para que los usuarios soliciten certificados y para que las CA emitan, administren y revoquen, además de diseminar las listas de revocación de certificados (CRL, Certificate Revocation Lists) de manera que otras entidades sepan cuándo un certificado ya no es válido [Carracedo, 2004]. La PKI se basa en los estándares X.509 establecidos por ISO.

Un componente importante de la PKI es el grupo de políticas de seguridad que lo gobierna. Estas políticas deben definir las reglas de emisión y uso de los certificados digitales y de las claves asociadas con ellos. La expansión en el uso de la tecnología de clave pública se ha logrado por el conjunto de servicios, interfaces de programación, herramientas administrativas y aplicaciones de usuario que forman una PKI. Aunque los estándares, las tecnologías y la manera de implementar una PKI están en evolución, como es típico de cualquier infraestructura compleja, tienen una estructura bastante estándar que es fácilmente reconocible y generalmente aceptada.

3.4.1 Autoridades de certificación

Una autoridad certificadora (CA, Certification Authority) es una organización que se responsabiliza de la validez de los certificados (véase Figura. 3.14). Es función de la CA recibir, distribuir y finalmente eliminar (cancelar) los certificados cuando la información que contienen sea inválida. En la Tabla 3.4 se muestran algunas plantillas de certificados.

La CA es responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves pública/privada. A nivel mecánico, comprende el conjunto de componentes y servicios de software y hardware que se usan durante este proceso. También incluye el personal, los procedimientos de operación, el ambiente y las directivas que definen cómo se establecen las identidades y cuál es la forma de certificado digital que se expide [Nash, 2002].

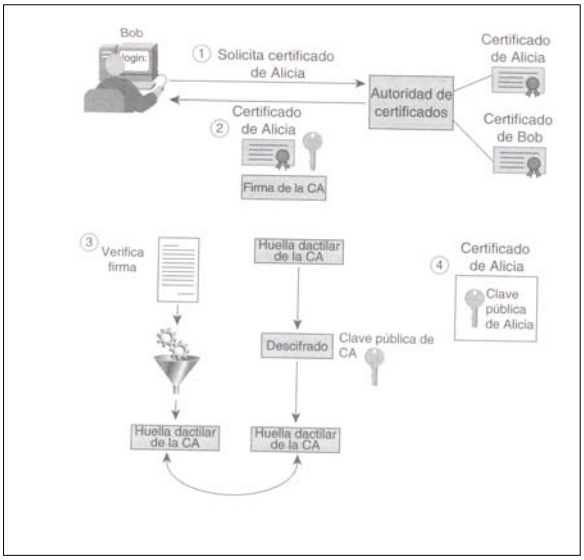


Figura 3.14 Obtención de un certificado digital a través de una autoridad de certificados.

Nombre de la plantilla	Objeto del certificado	Emitido a usuarios o equipos
Administrador (Administrator)	Firma de código, firma de CTL, EFS, correo seguro, autenticación de cliente	Usuarios
Sesión autenticada (Authenticated Session)	Autenticación de cliente	Usuarios
EFS básico (Basic EFS)	EFS	Usuarios
Equipo (Computer)	Autenticación de cliente, autenticación de servidor	Equipos
Firma de código (Code Signing)	Firma de código	Usuarios
Controlador de dominios (Domain Controller)	Autenticación de cliente, autenticación de servidor	Equipos
Agente de recuperación EFS (EFS Recovery Agent)	Recuperación de archivo	Usuarios
Agente de inscripción (Enrollment Agent)	Agente de solicitud de certificado	Usuarios
Agente de inscripción (petición sin conexión) (Enrollment Agent Offline Request)	Agente de solicitud de certificado	Usuarios
IPSec (petición sin conexión) IPSec (Offline Request)	Seguridad Internet Protocol	Equipos
IPSec	Seguridad Internet Protocol	Equipos
Enrutador (solicitud sin conexión)	Autenticación de cliente	Equipos/enrutadores
Sesión de tarjeta inteligente (Smart Card Logon)	Autenticación de cliente	Usuarios
Usuario de tarjeta inteligente (Smart Card User)	Autenticación de cliente, correo seguro	Usuarios
CA subordinada (Subordinate Certificación Authority)	Todo	Equipos
Firma de listas de confianza (Trust List Signing)	Firma de CTL	Usuarios
Usuario (User)	EFS, correo seguro, autenticación de cliente	Usuarios
Sólo firma de usuario (User Signature Only)	Correo seguro, autenticación de cliente	Usuarios
Servidor Web (Web Server)	Autenticación de servidor	Equipos

Tabla 3.4 Plantillas de certificados.

3.4.1.1 Tipos de autoridades de certificación

Existen muchas formas en que las autoridades certificadoras pueden ofrecer sus servicios.

- **Interna**.- Una organización puede operar una CA para certificar a sus propios empleados, sus puestos y sus niveles de autoridad. Tal jerarquía de certificación podría emplearse para controlar el acceso a los recursos o al flujo de información internos. Por ejemplo, cada empleado de una organización podría crear una llave y recibir un certificado para ella. Además, dicho certificado sería enviado a los sistemas a los que deba tener acceso. Las computadoras en toda la organización podrían entonces decidir si otorgan o no acceso a un empleado basados en la certificación de su llave. De esta forma, la empresa evita la necesidad de distribuir una lista de control de acceso y archivos de claves para el ingreso a todas sus computadoras.
- **Externa de empleados.-** Una empresa podría contratar a una compañía externa para que le dé servicios de certificación para sus empleados, de la misma forma en que podría contratar a un laboratorio fotográfico para crear tarjetas de identificación.
- **Externa de clientes.-** Una empresa podría contratar a una compañía externa para operar una autoridad certificadora para sus clientes actuales o potenciales. Al confiar en las prácticas de certificación de una compañía externa, la empresa se ahorraría el costo de crear sus propios procedimientos.
- **Confiable a terceros.-** Una compañía o un gobierno puede operar una CA que relacione llaves públicas con los nombres legales de individuos y empresas. Esa CA puede utilizarse para permitir a personas sin relación anterior establecer mutuamente su identidad y participar en transacciones legales.

3.4.1.2 Organización jerárquica de las autoridades de certificación

En esta sección examinaremos algunos de los modelos específicos que han sido creados para establecer relaciones de confianza. Consideraremos los tres modelos de confianza más comunes: jerarquías subordinadas, entre iguales y los modelos de malla conectados.

3.4.1.2.1 Modelos jerárquicos subordinados

El modelo jerárquico subordinado permite las relaciones de confianza bidireccionales y que los usuarios de certificados seleccionaran las anclas de confianza según se ajustaran. La jerarquía subordinada es un subconjunto de la jerarquía generalizada que aplica algunas restricciones adicionales (véase Figura 3.15).

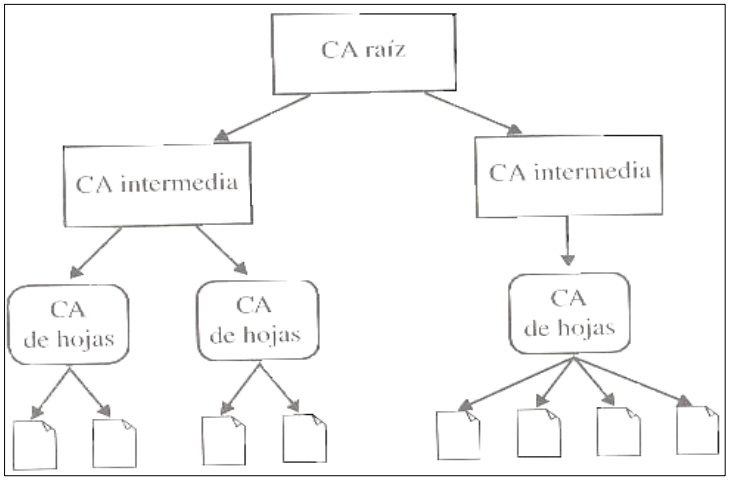


Figura 3.15 Jerarquía subordinada.

La CA raíz toma un significado en particular en el modelo de la jerarquía subordinada. Está diseñada como el ancla de confianza común para todas las entidades destino. Como tal, por definición, es la autoridad de certificación de más confianza y todas las demás relaciones de confianza salen a partir de ella. Certifica el siguiente conjunto más bajo de la CA subordinada con un conjunto de relaciones de confianza unidireccionales. En este modelo, solamente la CA superior expide certificados a sus subordinadas; las CA subordinadas no certifican a sus superiores.

3.4.1.2.2 Modelos entre iguales

Un modelo de confianza entre iguales asume el establecimiento de la confianza entre dos autoridades de certificación que no se pueden considerar subordinadas entre sí; por el contrario, se consideran iguales. Las dos CA podrían ser parte de una sola empresa o dominio de confianza, pero lo más común es que estén en diferentes empresas o dominios de confianza (véase Figura 3.16).

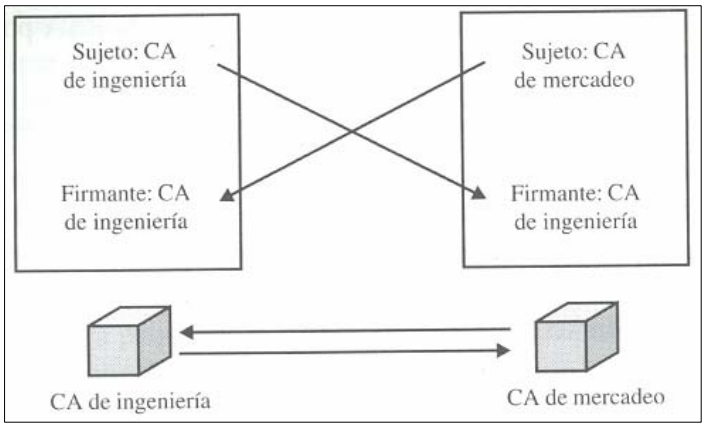


Figura 3.16 Ejemplo de modelos entre iguales.

En este modelo no hay CA raíz que actúe como un ancla de confianza. Por lo común, lo usuarios del certificado se basarán en su propia autoridad expedidora local para que actúe como el ancla de confianza. El usuario del certificado siempre validará una ruta que llega hasta la CA expedidora, la cual, a su vez, ha tenido su clave pública certificada por la propia CA del usuario del certificado. Es usual que cada CA certifique la clave pública de la otra creando una confianza bilateral. Con frecuencia, este proceso se conoce como certificación cruzada.

3.4.1.2.3 Modelos en malla

El uso de la certificación cruzada entre iguales es útil, pero, de alguna manera, está limitado mientras estemos restringidos a la certificación cruzada directa de una pareja única de autoridades de certificación. Sin embargo, la misma técnica se puede aplicar de un modo más general para construir modelos de confianza sofisticados. El modelo de confianza que veremos aquí es aquel en el cual se puede construir una malla conectada total o parcialmente, permitiendo más de dos certificados CA en una ruta de certificado. Para construir un conjunto de relaciones de confianza en este modelo, permitimos que cada participante en una relación de certificación cruzada entre iguales tenga certificaciones cruzadas con otros iguales. Al permitir que la ruta del certificado atraviese múltiples CA, creamos un mecanismo general para construir cadenas largas de certificados. Usando este mecanismo, podríamos construir una estructura jerárquica subordinada permitiendo únicamente la certificación en un solo sentido, de una CA superior hacia una CA subordinada.

Si admitimos relaciones de confianza bilaterales y cada CA en una ruta tiene certificación cruzada con las demás, podríamos construir la estructura jerárquica generalizada (véase Figura 3.17).

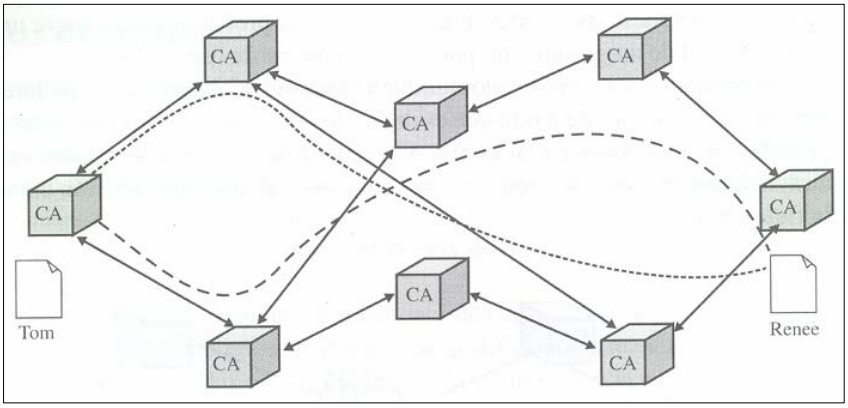


Figura 3.17 Ejemplo de un modelo de malla.

3.4.2 Autoridades de registro

Una Autoridad de registro efectúa la relación entre el usuario y una CA. La RA es responsable del registro y la autenticación inicial de suscriptores, que son los usuarios a quienes se les expide un certificado después de que les ha sido aprobada una solicitud de registro.

Las funciones de una RA variaran con base en la necesidad de la instalación de la PKI, pero deben soportar el principio de establecer o verificar la identidad del usuario. Es probable que estas funciones incluyan:

- Autenticación personal del sujeto que se registra para un certificado.
- Verificación de la validez de la información suministrada por el usuario.
- Validar el derecho del sujeto a los atributos del certificado solicitado.
- Verificar que el usuario en realidad posee la clave privada que se va a registrar; por lo general, esto se conoce como prueba de posesión (POP).
- Informar los casos de terminación o compromiso de clave donde se requiera la renovación.
- Asignación de nombres con propósitos de identificación.
- Generación de secretos compartidos para utilizarlos durante las fases de iniciación y escogencia del certificado del proceso de registro.
- Generación de la pareja de claves pública/privada.
- Iniciación del proceso de registro con la CA en nombre de la entidad destino del sujeto.
- Almacenamiento de la clave privada.
- Iniciación del proceso de recuperación de la clave.
- Distribución de señales físicas (como las tarjetas inteligentes) que contienen las claves privadas.

En general, la RA maneja los intercambios (con frecuencia involucran interacciones del usuario) entre la entidad destino del usuario y la PKI para el registro, la entrega del certificado y otros procesos de la administración del ciclo de vida del certificado y la clave.

Estas interacciones también pueden incluir la revocación del certificado y los demás servicios que los suscriptores necesitan cuando interactúan con la PKI. Una RA y sus interfaces se pueden implementar como parte de un servidor de certificados, o pueden formar un componente independiente.

Una persona puede realizar las obligaciones de una RA. Todo el proceso de validación de la identidad se puede desarrollar como un conjunto de procedimientos manuales (de hecho, puede ser necesaria la verificación humana directa para algunos entornos de alta seguridad. El envío de un certificado solicitado por parte de un individuo calificado y autenticado es una culminación válida de las responsabilidades de la RA. Las normas comerciales que controlan la generación de certificados y el registro del suscriptor del certificado varían ampliamente, pero se deben describir en la CPS (Declaración de Prácticas de Certificación, Certification Practices Statement) para la CA. Los administradores de seguridad y los asesores legales dentro de las empresas que utilizarán los certificados expedidos por la CA deberán revisar los aspectos de la CPS.

3.4.3 Certificados digitales

Los certificados digitales otorgan a las personas, organizaciones y negocios que se encuentran en Internet formas sencillas de comprobar mutuamente su identidad. Un certificado tiene un tiempo de existencia válido limitado, que viene indicado en su contenido firmado. Dado que la firma y exactitud de un certificado pueden ser comprobadas de forma independiente por un cliente que utilice un certificado, los cuales pueden ser distribuidos por medio de comunicaciones no fiables y sistemas de servidor, y pueden ser colocados en la caché de almacenamiento no seguro de los sistemas. Los certificados se emplean en el proceso de validación de los datos firmados. Las especificaciones varían en función del algoritmo que se use, pero el proceso general funciona de este modo:

1. El destinatario de los datos firmados verifica que la identidad reivindicada por el usuario coincide con la identidad contenida en el certificado.
2. El destinatario valida que no se ha revocado ningún certificado en la ruta (por ejemplo, recuperando una CRL actual o consultando un contestador on-line de estado del certificado), y que todos los certificados estaban dentro de sus periodos de validez en el momento en que se firmaron los datos.
3. El destinatario verifica que los datos no reivindican tener atributos para los cuales el certificado indique que el firmante no está autorizado.
4. El destinatario verifica que los datos no han sido alterados desde que fueron firmados utilizando la clave pública del certificado.

Para los consumidores, algunas de las ventajas de los certificados son:

- Una forma sencilla de verificar la autenticidad de una organización antes de darle información confidencial.
- El conocimiento de que, en el peor de los casos, pueden obtener la dirección física

Para los negocios, las ventajas incluyen:

- Una forma sencilla de verificar la dirección de correo electrónico de un individuo sin tener que enviarle un mensaje, lo cual disminuye el tiempo de transacción y reduce los costos. También puede evitar el abuso del correo electrónico -por ejemplo, si una organización solo permite a las personas suscribirse a una lista de correo presentado una identificación digital, no es posible que un atacante suscriba a las personas a la lista sin su permiso-.
- Una forma sencilla y muy utilizada de comprobar la identidad de un individuo sin utilizar nombres de usuario y claves de acceso, las cuales se olvidan con facilidad y los usuarios las comparten.
- En vez de intentar administrar largas listas de usuarios y claves de acceso, los negocios pueden emitir certificados a sus empleados y socios de negocios. Los programas que otorgan el acceso a los servicios solo tienen que validar la firma de un certificado.
- Hoy en día, muchos de los servicios por suscripción en Internet que cobran una cuota fija mensual autentifican a sus usuarios mediante un nombre de usuario y una clave de acceso. Por desgracia, varios usuarios coludidos pueden violar este sistema compartiendo entre ellos un solo nombre de usuario y una clave de acceso. Los servicios que utilizan la autenticación con base en certificados son menos propensos a ser víctimas de tales abusos, ya que es más difícil para los usuarios compartir llaves y certificados que nombres de usuario y claves de acceso. Además, si se utiliza una sola llave para varios propósitos (por ejemplo, si sirve tanto para desbloquear una página Web como para proporcionar acceso a la cuenta de banco del usuario), es menos probable que los usuarios se coludan. El riesgo de compartir llaves secretas puede ser mayor que los beneficios obtenidos al hacerlo.

Un certificado digital forma una asociación entre una identidad y la pareja de claves pública/privada que posee el tenedor de la identidad. Los usuarios de los sistemas basados en claves públicas deberán estar seguros de que, siempre que se apoyen en una clave pública, la clave privada asociada será propiedad del sujeto con el que se estén comunicando (esto es aplicable independientemente de si se utiliza un mecanismo de cifrado o de firma digital). Esta confianza se obtiene a través del uso de certificados de clave pública, que son estructuras de datos que enlazan valores de clave pública a sujetos. El enlace se consigue haciendo que una CA de confianza verifique la identidad del sujeto y firme digitalmente cada certificado. Por tanto, la finalidad de una CA consiste en enlazar una clave pública con el nombre común del certificado.

3.4.3.1 Formato general de los certificados

La primera versión apareció en 1988 y fue publicada como el formato X.509v1, siendo la propuesta más antigua para una PKI a nivel mundial. Esto junto con su origen ISO/ITU han hecho del X.509 el más utilizado. Más tarde fue ampliada en 1993 por la versión 2 únicamente en dos campos, identificando de forma única el emisor y usuario del certificado. La versión 3 de X.509 amplia la funcionalidad del estándar X.509 (véase Figura 3.18). El estándar X.509 constituye una base comúnmente aceptada para una PKI, y define los formatos y procedimientos de datos relacionados con la distribución de claves públicas que utilizan los certificados firmados digitalmente por las CA. La RFC 1422[40] especificó los principios básicos de una PKI basada en el estándar X.509, destinada principalmente a satisfacer las necesidades del correo por Internet con privacidad mejorada (PEM). Desde que se publicó la RFC 1422, los requisitos de aplicación de una PKI de Internet se han ampliado enormemente, y las posibilidades de X.509 han avanzado mucho.

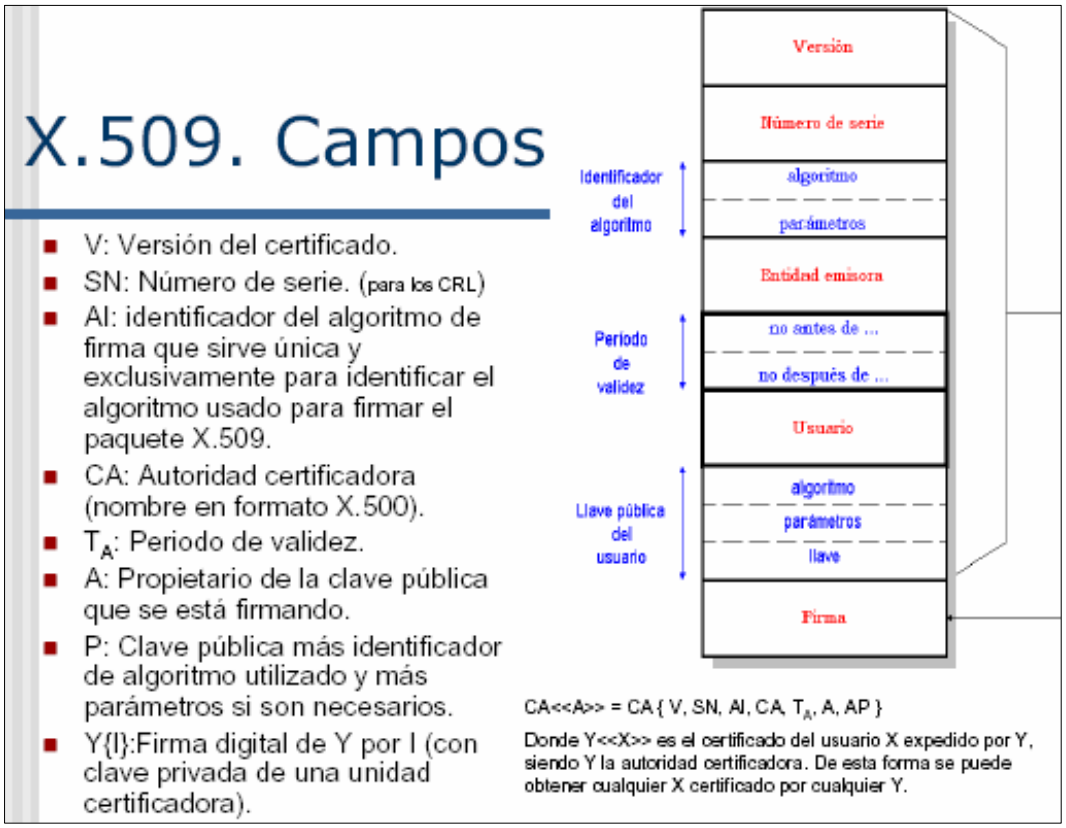


Figura 3.18 Estructura esquemática de un certificado X.509 típico.

[40] ***http://www.freesoft.org/CIE/RFC/1422/***

3.4.3.2 Tipos de certificados

Un certificado X.509v3 certifica que una llave privada fue firmada por una institución específica. Esta certificación se sella mediante una firma digital. En la actualidad se utilizan cuatro tipos de certificados digitales en Internet.

- **Certificados de autoridades certificadoras.-** Un certificado de autoridad certificadora es el que contiene el nombre y la llave pública de una autoridad certificadora. Estos certificados pueden ser auto-firmados: la autoridad certificadora dice que su propia llave es válida y el usuario debe confiar en ella. Alternativamente, puede formarlos otra organización. Las CA también pueden cruzar certificados, es decir, firmar mutuamente una llave maestra de la otra.
- **Certificados de servidores**.- Contienen la llave pública de un servidor SSL, el nombre de la organización que lo administra, su nombre de anfitrión en Internet y la llave pública del servidor (véase Figura 3.19).
- **Certificados personales**.- Contienen el nombre y la llave pública de un individuo. Pueden también tener información adicional, como la dirección de correo electrónico, dirección postal o cualquier otra cosa. Los certificados de clientes tienen muchos usos y beneficios:
  1. Pueden eliminar la necesidad de recordar nombres de usuario y claves de acceso. Solo es necesario signar utilizando la firma digital al entrar a un espacio restringido.
  2. En vez de desplegar una gran base de datos distribuida, las organizaciones pueden utilizar un certificado digital emitido por una CA específica como prueba de pertenecer a una organización.
  3. Puesto que para firmar mediante un certificado digital se requiere acceder a una llave secreta, es más difícil para grupos de individuos compartir una sola identificación digital que un nombre de usuario y clave de acceso, pues existen barreras técnicas que dificultan el compartir llaves secretas entre usuarios y porque estos tal vez no desearán compartir una llave secreta que se utiliza para más de una aplicación. Esto es interesante para los sitios que realizan cobros por usuario para la distribución de información a través de Internet.
  4. Como los certificados digitales contienen la llave pública de una persona, es posible utilizarlos para enviarle correo encriptado. Al crear sistemas estrictos de identificación de usuarios, los certificados ayudan a eliminar el anonimato y lo hacen en forma aún más efectiva que las cookies. Una cookie solo deja un rastro de por dónde se ha pasado dentro del sitio Web. Por su parte, un certificado digital deja el nombre, dirección de correo electrónico y otra información identificadora, la cual, por diseño, puede rastrearse hasta llegar al usuario.

- **Certificados de editor de software.-** Se utilizan para firmar software que va a distribuirse. Se supone que la firma de código debe dar al mundo de software distribuido vía electrónica la misma confiabilidad que brinda el software empaquetado. Esto se logra agregando dos cosas a un ejecutable:
  1. Una firma digital que signa al ejecutable con una llave secreta.
  2. Un certificado digital con la llave pública correspondiente, el nombre de la persona u organización a quien pertenece y una firma digital signada por una CA reconocida. Esto se muestra en la Figura 3.20.

Para ser útiles, las firmas deben ser verificadas. De manera ideal, todas las firmas de código deben revisarse al descargar cada fragmento de código y antes de cada vez que se ejecute el programa. De esta forma, las firmas de código pueden detectar tanto intentos hostiles de modificar el código como modificaciones accidentales resultantes de errores del sistema operativo o fallas de hardware. Esto se debe a que una vez que un programa ha sido modificado, su firma no pasará la verificación. Por ello, la firma de código puede mejorar considerablemente la confiabilidad de los sistemas de cómputo actuales, dando a los usuarios formas confiables de detectar modificaciones a los programas antes de su ejecución.

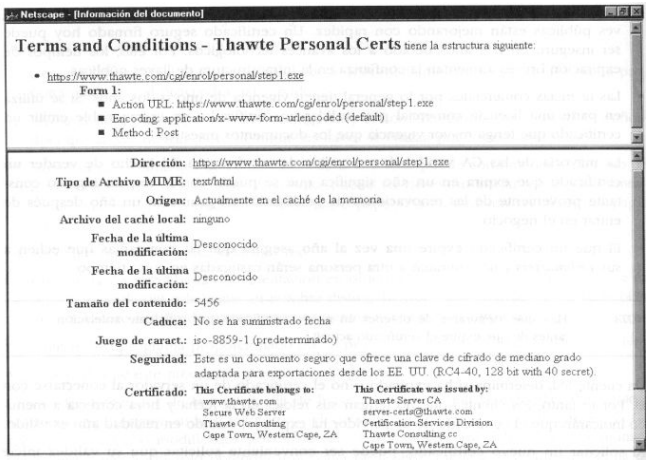


Figura 3.19 Certificado de un servidor.

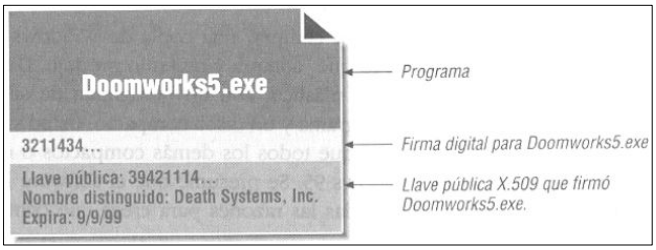


Figura 3.20 Un diagrama idealizado de una pieza de código signado, mostrando la firma digital del código y el certificado digital correspondiente.

3.4.3.4 Gestión de los certificados

Esta sección trata el tema de las operaciones necesarias para administrar certificados durante su ciclo de vida, desde la creación hasta su retiro. En ellos se incluye el reemplazo de claves cuando expiran, lo mismo que la revocación y validación de certificados.

3.4.3.4.1 Generación y certificación

La generación y certificación ocurre simultáneamente, y habitualmente se inician por un usuario que solicita un certificado a una CA. El usuario genera las claves, excepto para solicitud de tarjeta inteligente, usando uno de los proveedores de servicios de cifrado disponibles para su sistema.

3.4.3.4.2 Revocación de certificados

Revocar es el acto de cancelar un certificado, recuperando eficazmente la firma del emisor de la combinación clave pública/nombre del usuario. Técnicamente, la revocación se lleva a cabo publicando el número de serie del certificado en una CRL, con la firma de la CA que lo emitió. El certificado de una CA se revoca cuando se desvela su clave privada, ya que otros podrán emitir certificados en su nombre. Por ello todos los certificados, incluyendo los emitidos a CA subordinadas y los que éstas emitieran, también se consideran revocados. Podemos encontrarnos las siguientes causas de revocación:

- El usuario ha cambiado su nombre.
- Se ha revelado la clave privada del usuario; el mismo solicitará de nuevo un certificado con una nueva pareja de claves.
- Se ha descubierto la clave de firma del emisor. Todos los certificados emitidos serán inválidos, ya que existe un tercero que puede emitir certificados suplantando al emisor.
- El usuario deja de pertenecer a la organización, o a la parte de éste de la cual se responsabiliza la CA.
- El titular del equipo referido en el certificado (los titulares de equipos también pueden tener claves), es sustituido, está bajo sospecha o es trasladado.

3.4.3.4.3 Renovación de certificados

La renovación es el acto de emitir un nuevo certificado usando el mismo nombre, un número de serie nuevo y puede que una nueva pareja de claves, pero no necesariamente. La renovación no afecta a la validez del certificado antiguo. Se deberían renovar los certificados de usuarios y equipos poco antes de que expiren.

La renovación de certificados de la CA debería hacerse con mayor antelación, ya que para que un certificado sea válido en todo momento, los certificados de su CA emisora y los de sus ascendentes también

han de ser válidos. Sería lamentable que la expiración del certificado de una CA invalidara todos los certificados emitidos.

Es por ello que las CA implementan anidamiento temporal, que quiere decir que no emitirán certificados que expiren más tarde que sus propios certificados. Esta directiva de anidamiento temporal puede causar problemas cuando esté próximo a expirar el certificado de una CA. Por ejemplo, si una CA emitiera certificados un mes antes de la expiración, el tiempo de vida de dichos certificados tendrá que ser menor de un mes. Por tanto, se deben renovar los certificados de las CA cuando su tiempo de vida restante se aproxime al período máximo de validez de los certificados que emita. Por ejemplo, una CA que emita certificados de dos años de validez, debería tener un ciclo de vida de cuatro y renovar su certificado cada dieciocho meses. Tras la renovación, las entidades usan el nuevo certificado y la nueva pareja de claves, si la hubiera. El conjunto anterior se archiva para descifrar y verificar documentos antiguos e incluso nuevos. La Tabla 3.5 muestra algunos tiempo de vida que tienen los certificados.

Objeto del certificado	Tiempo de vida	Calendario de renovaciones
CA raíz (clave de 4.096 bits)	20 años	Renovarlo cada 9.5 años, para poder garantizar certificaciones de 10 años a las CA intermedias. Renueve además la pareja de claves al menos cada 20 años, apurando su tiempo de vida.
Certificación intermedia (clave de 3.072 bits)	10 años	Renovarlo cada 4.5 años, para poder garantizar certificaciones de 5 años a las CA emisoras. Renueve además la pareja de claves al menos cada 10 años, apurando su tiempo de vida.
Certificación de emisoras (clave de 2.048 bits)	5 años	Renuévelo cada 2.5 años, para poder garantizar permanentemente certificaciones de 2 años. Renueve además la pareja de claves al menos cada 5 años, apurando su tiempo de vida.
Usuarios normales (claves de 512 bits)	1 año	Renuévelo cada año, incluyendo la pareja de claves, apurando así su tiempo de vida.
Administradores (claves de 1024 bits)	2 años	Renuévelo cada 2 años, incluyendo la pareja de claves, apurando así su tiempo de vida.
Equipos (claves de 1024 bits)	2 años	Renuévelo cada 2 años, incluyendo la pareja de claves, apurando así su tiempo de vida.

Tabla 3.5 Plantillas de certificados emitidos por las CA

3.4.3.4.4 Validación de certificados

La validación del certificado es el proceso mediante el cual se determina que el certificado se puede usar con validez en algún momento y que se ajusta al propósito que el usuario pretende. Para lograr esto, es necesario validar múltiples aspectos de los certificados.

- El certificado debe contener una firma criptográficamente válida, que establezca que el contenido del certificado no ha cambiado.
- La clave pública del emisor se debe usar para verificar la firma que aparece en el certificado.

- El período de validez especificado para las fechas de iniciación y terminación debe mostrar que el certificado es actual.
- El certificado puede contener campos que están marcados como críticos o no críticos. El validador del certificado debe entender todos los campos marcados como críticos y certificar si el documento se considera válido.
- El certificado sólo se puede usar para el propósito para el cual se creó originalmente. Por ejemplo, claves y certificados que están marcados para usar sólo en aplicaciones de firmas, no se pueden usar para operaciones de cifrado.
- Otras restricciones establecidas por la directiva especifican condiciones de uso que se deben observar.
- Finalmente, el certificado no debe haber sido revocado. Incluso con toda la información interna del certificado que indica que éste es válido, se debe revisar si se ha presentado algún evento externo excepcional que exija invalidarlo. De modo que la revocación de validación se debe realizar usando una lista de revocación de certificados o alguna forma de prueba de verificación en línea.

3.4.4 Depósito de certificados y listas de revocación

Los depósitos se utilizan para el almacenamiento público de certificados y listas de revocación de certificados.

Las listas de revocación de certificados (CRL, Certificate Revocation List) se necesitan con el estándar X.509 como un esquema de notificación de la revocación. La forma más simple del CRL es una lista publicada sobre una base regular por la CA, que identifica todos los certificados que se han revocado durante la vida de ésta. Ello está limitado por el período de validez del certificado. Cuando ha expirado, se puede retirar de la lista (véase Figura 3.21). La CRL es una estructura firmada, de modo que el usuario del certificado confíe en que la información no se ha cambiado desde que la expidió la CA. Como la CA necesita ser de confianza para los propósitos de validación del certificado, probablemente el usuario tenga el certificado de la CA para permitir que se verifique la firma de esta en la CRL. Proteger el repositorio para evitar la eliminación de las CRL es una medida valiosa para garantizar que al usuario del certificado no se le niegue el acceso a la CRL. La forma simple de la CRL es un contenedor que alberga una lista de certificados revocados identificados por el número de serie. El contenedor mismo contiene información como la hora en que la CRL se publicó, cuándo se publicará la siguiente y cuál fue la CA que expidió dicha CRL. La CRL es simplemente un archivo secuencial que crece con el paso del tiempo para incluir todos los certificados que no han expirado, pero que han sido revocados. Cada entrada contiene información, como la razón por la que el certificado se revocó. Esto incluye el compromiso de clave, compromiso de la CA expedidora, retiro de los

privilegios identificados en el certificado o cambio de otra información de éste (se conoce como afiliación cambiada).

También se puede incluir la fecha cuando se cree que el certificado ha sido invalidado debido al compromiso de clave. Se han propuesto varias alternativas para que las CRL sean más útiles. La mayoría de ellas se concentra en suministrar el subconjunto más relevante de la información de revocatoria para el usuario del certificado. Dos de estos esquemas se describen a continuación:

1. **CRL delta.-** Las CRL delta están diseñadas para reducir el tamaño de la CRL que se transmite hacia una entidad destino. Inicialmente, y luego sobre una base periódica planeada, se publica una CRL completa con todas las noticias de revocación conocidas; esto es lo que se conoce como la CRL base, la cual permite que las entidades destino establezcan una lista correcta conocida de todos los certificados revocados por una CA en una fecha en particular. Desde ese punto, se cuenta con una serie de actualizaciones que muestran los cambios o deltas que se han hecho a la lista de certificados revocados mediante esa CA, desde la expedición de la última CRL base o delta. Cada actualización se distribuye como una CRL y la emite y firma la CA de la misma manera que una CRL normal.
2. **Puntos de distribución de CRL.-** Los puntos de distribución de CRL están diseñados para concentrarse en el conjunto de CRL que se deben buscar para un subconjunto de información de revocatoria disponible. El concepto de un punto de distribución CRL es que las noticias de revocación del certificado se pueden organizar en categorías por el tipo de certificado que se está procesando, el tipo de CRL publicada o el tipo de noticia de revocación que se va a expedir. El tipo de certificado incluye certificados de usuario o de una CA. El tipo de CRL incluye CRL indirectas. El tipo de revocatoria incluye *conservación de certificado, compromiso de clave de la CA, cambio en la afiliación* y así sucesivamente. Los puntos de distribución de CRL pueden soportar sólo un subconjunto de certificados y tipos de CRL o de razones de revocatoria. Como resultado, el conjunto de noticias de revocatoria que se devuelven debe ser mucho más pequeño.

Para terminar este análisis de la revocación, vale la pena mencionar que las variaciones que se han implantado en las CRL estándar poseen muchos de los mismos beneficios de las CRL, pero cuentan con mejores características operativas. Por lo general, en las tecnologías más interesantes y bien desarrolladas de esta área se encuentran categorías de los esquemas basados en hash. En el caso de los esquemas hash de revocación, la meta es reducir el conjunto de información con respecto a los certificados revocados, para que sea una muy pequeña representación de toda las noticias de revocatoria. Por lo general, esta información va firmada, de modo que tiene las mismas características de protección de una CRL y no requiere el uso de un servidor seguro o de transporte seguro[41].

[41] *La versión comercial mejor conocida de esta clase de sistemas es la que suministra ValiCert: http://www.itsecurity.com/show/val24.htm*

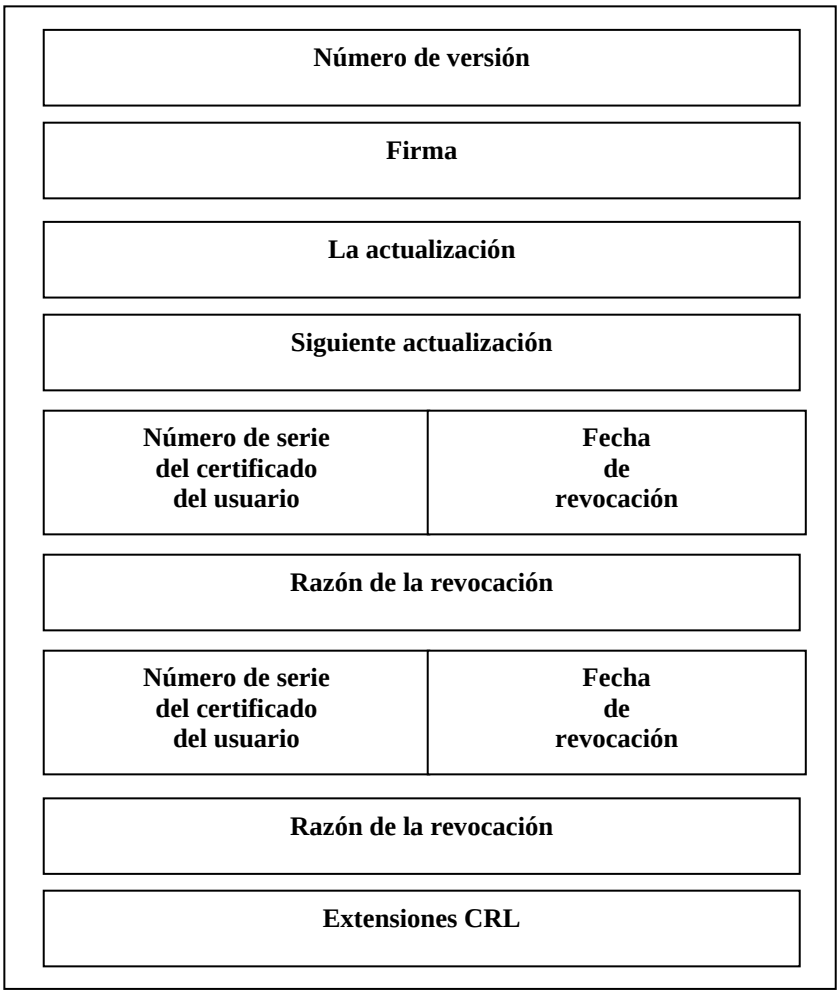


Figura 3.21 Formato de lista de revocación de certificados.

- **Versión number (número de versión).** La versión más reciente definida para actualizar es la v2. Las CRL que contienen extensiones críticas se deben a marcar como versión 2.
- **Signature (firma).** Identifica el tipo de función hash y algoritmo de firma usado para firmar la lista de revocación.
- **Issuer (expedidor).** El nombre de la autoridad que expidió y firmó la lista de revocación.
- **This Update (esta actualización).** Define la fecha y hora en que se publicó la lista de revocación.
- **Next Update (siguiente actualización).** Define la fecha y hora en que se publicará la siguiente lista de revocación.

3.5 Planificación de la PKI

Luego del análisis y evaluación realizada en los capítulos anteriores, se propone un modelo de PKI que incluye: una CA centralizada, políticas y prácticas básicas de seguridad, certificación adaptadas para los programas específicos, una RA para asumir la responsabilidad de la validación de la identidad de los usuarios. Todo esto aplicándolo por medio de modelos jerárquicos que son los mejores que se adaptan a la naturaleza organizacional de los usuarios de estas infraestructuras, proporcionando a su vez, un sistema de confianza sólido y robusto para definir una plataforma de seguridad para los sistemas de redes basado en la utilización de firmas y certificados digitales, todo ello utilizando software libre o comercial. Es necesario tener bien claro para que se diseña este tipo de infraestructura, teniendo en cuenta principalmente el tipo de aplicaciones que se montarán sobre de ellas. Esto nos permitirá determinar el tamaño de las claves, así como los algoritmos básicos a utilizar. Una PKI para autenticidad, integridad y no repudio utilizan funciones de firmas digitales, mientras que para confidencialidad necesita funciones de encriptado. También deben definirse los diferentes usos de las llaves, por ejemplo podríamos tener solamente un par de llaves pública/privada, una para firma y otra para codificación. No existe un diseño genérico para la PKI, por que cada red y cada lugar que lo necesita tiene sus propios requerimientos, restricciones y características. Es necesario analizar si existen impedimentos en los usos de algoritmos y estándar criptográficos, requerimientos en cuanto al tiempo de vida de las llaves, niveles de usuarios, exigencias del manejo de entrega de certificados (puede ser que se exija una entrega centralizada o en ciertas zonas de la red), exigencias del manejo de la base de datos de los certificados, adaptabilidad, interoperabilidad con externos, restricciones de costo, de velocidad, entre otras que pueda imponer las características detallada tanto física como lógica de la red en cuestión. A continuación de describen los requerimientos que se proponen como base para la planificación de una PKI.

3.5.1 Elección de los componentes para el modelo propuesto

- **Políticas de seguridad**.- Para que el entorno de certificación funcione correctamente es necesario definir una serie de reglas que indiquen la forma de cómo se va a diseñar la PKI. Este conjunto de reglas que constituyen las política de seguridad (véase Figura 3.22) tienen que estar definidas por las autoridades reconocidas (como por ejemplo, instituciones de gobierno, universidades, departamentos, etc.) todo con el fin de definir el entorno, alcance y medios de las políticas de seguridad en la plataforma**.** A continuación proponemos las siguientes políticas (véase la Tabla 3.6)

Políticas	Descripción
Identidad de la PS	Se deben dar a conocer el DN (Distinguided Name) de la PS, información que permita establecer contacto personal (código postal, teléfono, fax y dirección de e-mail), fecha de publicación de su informe de política y duración prevista.
Privacidad y seguridad	Deberá especificar las medidas técnicas y los procedimientos de seguridad que seguirán en la generación y protección de sus claves. También podrá imponer requisitos de seguridad sobre las CA´s certificadas y deberá dictar medidas de seguridad para proteger la información recogida en los procesos de certificación de las CA´s subordinadas.
Mecanismos de protección	Se deben definir los requerimientos de hardware y software necesarios para proteger la infraestructura de una CA.
Políticas de certificación	Cada PS deberá indicar la política y procedimiento que gobiernan la certificación de las CA´s subordinadas y transitivamente también a los usuarios o CA´s que sean certificados por las anteriores. Por ejemplo, se debe especificar el procedimiento del registro, el periodo de validez de los certificados, tamaño de las claves, etc.
Gestión de CRL´s	Se especificara la frecuencia de emisión de CRL´s para su sub-árbol bajo la PS, la dirección en la que las CA´s subordinadas deberán depositar las CRL´s emitidas, la dirección de consulta de CRL´s, los procedimientos adicionales como almacenamiento de CRL´s antiguas y las posibles ayudas que pueda tener de las CA´s para mantener y gestionar las CRL´s
Otras políticas	Se puede añadir cualquier otra información que deban conocer los usuarios, teniendo en cuenta que los documentos de política se consideran casi inmutables y de larga duración.

Tabla 3.6 Políticas de seguridad

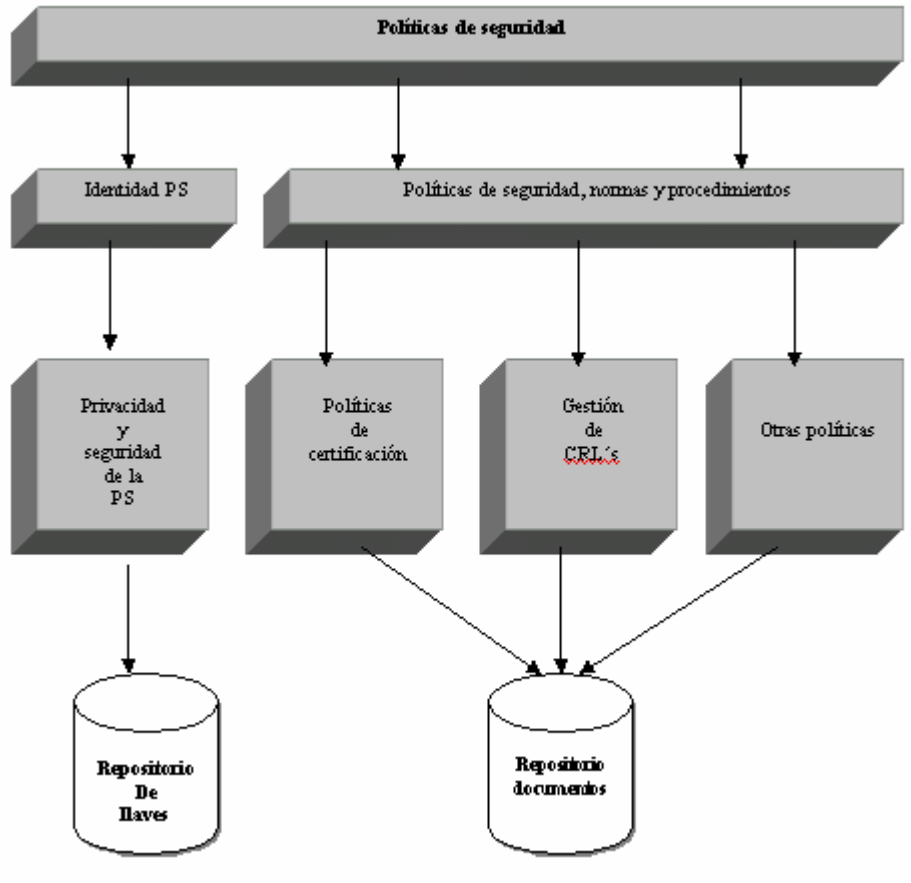


Figura 3.22 Políticas de seguridad para el modelo.

- **Autoridades de certificación.-** Su función principal es el de avalar los datos de cualquier certificado emitido por la PKI, para nuestro modelo, si bien se puede partir de una entidad fiable y la creación de certificados raíz autofirmadas, esto no es recomendable, lo correcto y buen camino es ser avalada por una entidad que tenga reconocido prestigio y confianza (el departamento de informática por ejemplo). Cada certificado emitido por una CA debe de estar firmada por una CA de mayor grado en el esquema jerárquico de autoridades certificadoras, formándose así una cadena de certificados, en los que una CA se avalan a otras hasta llegar a la CA superior, que se avala a si misma. El certificado digital vincula pues indisolublemente a una persona o entidad con una llave pública, y mediante el sistema de firma digital se asegura que el certificado que recibimos es realmente de la persona que consta en el mismo (véase Figura 3.23).

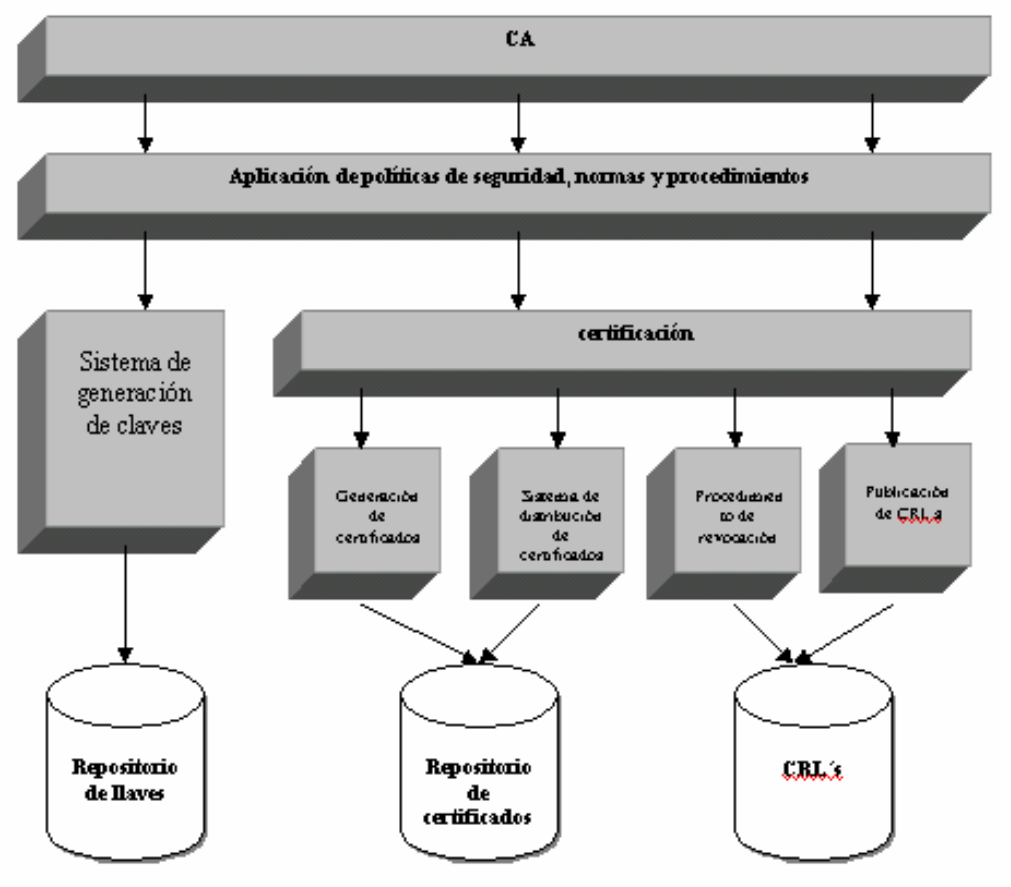


Figura 3.23 Autoridad de certificación.

- **Autoridades de registro.-** Para garantizar la validez del procedimiento de registro, cada RA debe de tener un par de claves asimétricas, con la clave publica certificada por una CA que sea un punto de confianza de todas las CA´s para las que realiza funciones de registro. Cuando una RA y una CA coincidan físicamente, la RA podrá considerar el par de claves de la CA y su certificado como propios. El modelo incluirá una o varias RA para certificar la identidad de los usuarios; una o varias CA que emitan los certificados de clave pública; un repositorio de certificados accesible vía Web u otro medio, donde se almacenen los certificados; las CRL, donde se listan los certificados suspendidos o revocados y por supuesto los propios certificados (véase Figura 3.24).

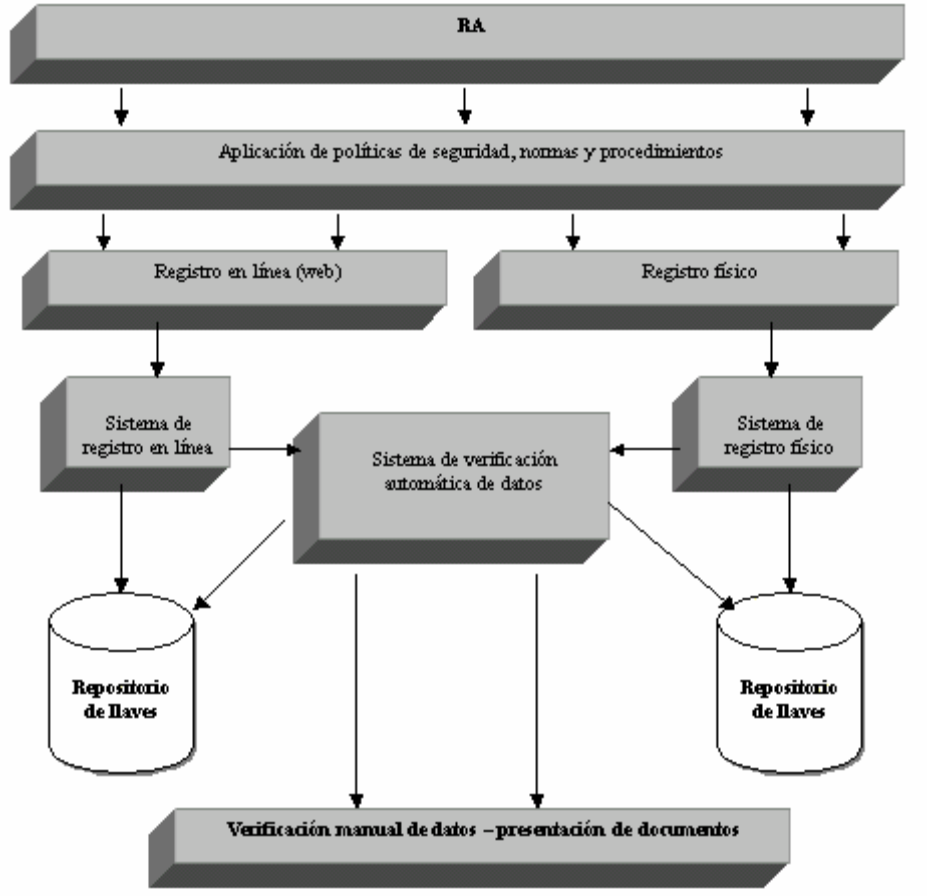


Figura 3.24 Autoridad de registro para el modelo.

3.5.2 Funciones del modelo

- **Generación y registro de claves**. El modelo considera la disponibilidad de que las entidades puedan generar sus claves a través de un portal o pagina Web (lógicamente con elementos o componentes que se ejecuten en el equipo del cliente). En cualquier caso, las claves privadas nunca deben viajar por la red y habrán de ser distribuidas a través de canales no telemáticos de seguridad y confidencialidad probadas (por ejemplo un token). Una vez completado la solicitud y generación de las claves, la entidad final debe registrar su clave publica ante la CA a través de la RA aceptada dentro del escenario. Para la inscripción se tiene que enviar su clave publica y el documento digital de solicitud firmado con dicha clave. Tiempo de vida de las llaves: a) no más de un año, b) no más de 3 años, c) no más de 2 años.
- **Generación de certificados de usuarios.** Se generaran a través de formularios Web provistos por la CA. Este servicio no estará en la misma máquina de la CA. Cuando un usuario es inscrito recibirá dos certificados y un fichero de claves privadas protegido por clave asimétrica. La CA para inscribirte deberá comunicarle a la CA central el nuevo nombre. Esta verificara si no existe y dará su aprobación o rechazo.
- **Expiración de certificados.** Debe solicitarse por red antes del tiempo límite, la información pasará protegida y firmada por el certificado viejo que aún no ha dejado de tener validez. Existirá una aplicación que estará corriendo en cada PC incluida en el sistema que verificara si el certificado público de los usuarios está por vencer, le dará una alarma y le brindará un mecanismo casi transparente para hacer este proceso, de no ocurrir esto antes del tiempo límite el usuario deberá ir personalmente a inscribirse otra vez. Existirá un tiempo en que todavía el usuario estará usando los dos certificados, eso lo deben tener en cuenta todas las entidades que se encargan de verificar certificados.
- **Revocación de certificados.** Debe hacerse de manera personal la solicitud del nuevo certificado. Por los diversos motivos que se puede invalidar un certificado, la revocación podrá realizarse por red (pues suponemos que si hubo un robo de llave privada, esa persona no desea revocar el certificado). Pudiera suceder que se modificara el mensaje de revocación (si se intercepta). El usuario una vez que revoca su certificado, deberá ir personalmente a crear uno nuevo, si el mensaje de revocación nunca llegó, se comprobará en ese momento. También el usuario podrá comprobar personalmente si su certificado ya no está público.
- **Distribución de certificados de usuarios.** Los certificados estarán publicados en un sistema de directorio. Pero cada aplicación puede decidir, si envía o no los certificados en cada mensaje, ya que el modelo resuelve ambas variantes.
- **Servicios de directorio**. El modelo esta pensado para operar tanto en entornos en los que se utiliza el directorio X.500 como en aquellos en los que no se utiliza, el mecanismo de

almacenamiento y obtención de certificados y CRL´s se simplifica. En el modelo se propone que cada CA tenga asociado un servidor de certificados y CRL´s que permita la obtención por parte de cualquier usuario, del certificado de la propia CA, de las CRL´s que tenga asociadas y de cualquier certificado que haya sido emitido por ella. Este servidor obtendrá los certificados de una base de datos local asociada a la CA, o bien del directorio X.500

- **Servicios de publicación y almacenaje de llaves, certificados y CRL**. Es el servicio de nos permite la distribución de certificados, así como otros datos de las personas u otras entidades funcionales que estén dentro de la PKI. Este servicio debe permitir que existan entradas en las base de datos para obtener los diferentes certificados con sus datos, asegurarse que existe un solo nombre para cada objeto en la PKI, brindar servicio de directorio confidencial con entrada autorizada (que no tiene sentido con la CRL) pero si con alguna información personal, brindar un directorio externo para que personas fuera de la PKI puedan obtener información y además debe mantener un control estricto sobre la modificación de la información, garantizando siempre que sea el personal autorizado.
- **Verificación de certificados de usuarios.** El servicio de verificación de certificado tendrá dos implementaciones, una on-line y otra off-line.

3.5.3 Selección de la plataforma de trabajo

Se proponen tres soluciones de tecnologías actuales del mercado: Microsoft Windows 2000 Certificate Service, OpenCA y SunONE Certificate Server. Las ventajas que ofrecen estas soluciones es que SunONE es la más robusta y completa, Windows 2000 Certificate Service es una solución excelente para los sistemas que están diseñados para la familia Microsoft y la solución de código abierto OpenCA es recomendable para Linux.

CONCLUSIÓN

La meta principal de esta investigación fue proporcionar los conocimientos necesarios para el diseño, implementación y puesta a punto de las Infraestructuras de Claves Públicas, con lo cual se ha procurado dejar sentadas las bases para que se puedan adquirir los conocimientos y las habilidades necesarias para ello, aunque quede aún mucho camino por recorrer.

Como se puede observar el aspecto de la seguridad en las redes informáticas es un tema de suma importancia que debe estar sobre la mesa de cualquier organización que esté interesada en proteger y usar eficientemente su información; las razones son muchas, la ubicuidad es una, la escalabilidad es otra y, por supuesto, la accesibilidad en costo, lo que permite que las organizaciones se conecten con socios de negocios, clientes, proveedores y ubicaciones remotas de campo, sucursales y empleados móviles directamente en línea a la red de la empresa.

La Infraestructura de Clave Pública (PKI) es una herramienta novedosa dentro de la industria de seguridad. Implica conocimientos criptográficos, conocimientos de los Protocolos SSL, TCP/IP, etc; así como el funcionamiento de una autoridad de certificados. Con lo anterior se ha puesto de manifiesto la importancia que tiene el uso de algoritmos y técnicas de criptografía asimétrica para la provisión de los servicios de seguridad. También se ha definido el concepto de certificado de la clave pública y se ha analizado con cierto detalle la estructura interna del certificado X.509 y de las listas de revocación de certificados. En este trabajo se ha podido comprobar que el certificado es una pieza clave para la obtención de la seguridad en las redes informáticas. Si tan importante es el certificado, no menos han de serlo las garantías y medidas de seguridad necesarias para la implantación de la tercera parte de confianza que lo genera, que es la Autoridad de Certificación. Cuando el entorno telemático en el que se usan los certificados crece en extensión geográfica y complejidad organizativa resulta necesario el concurso de diversas Autoridades de Certificación para garantizar la provisión de estas credenciales. Además de las ya citadas autoridades, es necesaria la existencia de otras, tales como las de registro, agentes autorizados para emitir listas de certificados revocados, repositorios para el almacenamiento y recuperación de certificados, etc. Una red de entidades y agentes de estas características constituyen la infraestructura de certificación de ese entorno.

Dicha infraestructura está acrecentando su popularidad debido a que se presenta como una de las mejores soluciones que se pueden implementar debido al uso conjunto de claves públicas y privadas. La implementación de una PKI en cualquier ambiente que necesite seguridad ofrece una solución muy eficiente gracias a que cada uno de los usuarios tendrá una clave asignada, que no será compartida por ninguna otra persona lo que nos da como consecuencia una mayor facilidad para llevar a cabo el control y registro de las actividades que se llevan a cabo dentro de una red. Ahora, al implementar una PKI, si dicha información lograse ser desviada, haría falta que quien logró esta intercepción tuviera la llave privada del destinatario al cual iba dirigida ésta para lograr interpretarla en el mensaje, ofreciendo un nivel muy alto de seguridad en las operaciones de cualquier empresa o institución.

Sin embargo, esta complejidad no necesariamente debe ser reducida a una serie de formatos y estándares igualmente sofisticados. La búsqueda de la PKI perfecta no debería imponer límites al desarrollo de una buena PKI. Existen muchos usuarios y aplicaciones que precisan de un menor grado de complejidad a cambio de mayor versatilidad. Un importante criterio de diseño de arquitectura aplicado a las redes define que cuando la complejidad no puede ser eliminada, esta debe ser confinada a aquellas partes de la red que sean capaces de soportarla.

Por otra parte, y aun siendo este punto conocido y repetido constantemente en la literatura sobre la materia no se puede dejar de insistir en la importancia de las prácticas y procedimientos, que en su diseño y en su ejecución exigen un cuidado exquisito. Su valor como elemento crucial de la seguridad, la exigencia de que sean comprensibles por todos los participantes para lograr un funcionamiento óptimo y seguro del sistema de certificación y firma digital, y la dificultad que supone su transmisión a los usuarios son factores que condicionan decisivamente la utilidad de las PKI y de las aplicaciones que tienen en ellas su fundamento.

Por último se hace notar que un plan de seguridad debe tener varias capas para que pueda ser eficaz, dirigiéndose a todas las principales áreas de importancia. Entre ellas se incluirán la seguridad física, la seguridad del perímetro (por medio de la instalación de firewalls en los puntos de entrada a la red), el almacenamiento de los datos en discos (gracias a la encriptación de discos y archivos), la seguridad de los datos transportados por la red (con la seguridad de IP) y un medio para verificar las identidades de los usuarios, ordenadores y otras entidades que disponen de acceso a otros recursos de la red, al mismo tiempo, cimentarlas en la identificación de riesgos, vulnerabilidades, impactos y costos organizacionales a los que se expone a través de sus redes de comunicaciones.

APÉNDICE 1

En este Apéndice, se ofrece información sobre dos conceptos a los que hace referencia esta investigación: los números primos y la aritmética modular.

Números primos

El conjunto de los números primos es un subconjunto de los números naturales que engloba a todos los elementos de este conjunto que son divisibles exactamente tan sólo por dos números naturales 1 y p (el 1, que sólo tiene un divisor natural, no es primo ni compuesto).

Hay infinitos números primos, es decir, existen números primos tan grandes como se quiera. La distribución de los números primos es muy irregular. Hay algunos que son números impares consecutivos, como 3 y 5; estos se llaman primos gemelos.

Decimos que b ≠ 0 divide a *a* si $a = mb$ para algún *m*, donde *a, b* y *m* son enteros. Es decir, *b* divide a *a* si no hay ningún resto en la división. La notación $b \mid a$ se usa comúnmente para expresar que *b* divide a *a*. También, si $b \mid a$, decimos que *b* es un divisor de *a*. Por ejemplo, los divisores positivos de 24 son 1, 2, 3, 4, 6, 8, 12 y 24.

Se cumplen las siguientes relaciones:

- Si $a \mid 1$, entonces $a = 1$.
- Si $a \mid b$ y $b \mid a$, entonces a = b.
- Cualquier $b \neq 0$ divide a 0.
- Si $b \mid g$ y $b \mid h$, entonces $b \mid (mg + nh)$ para cualquier entero *m* y *n*.

Para entender este último punto, obsérvese que

- Si $b \mid g$, entonces *g* es de la forma $g = b \times g_1$ para algún entero g_1.
- Si $b \mid h$, entonces *h* es de la forma $h = b \times h_1$ para algún entero h_1.

Así.

$$mg + nh = mbg_1 + nbh_1 = b\ x\ (mg_1 + nbh_1 = b\ x\ (mg_1 + nh_1)$$

Y por lo tanto, *b* divide a $mg + nh$.

La propiedad más importante de los números primos es que constituyen las piezas básicas en las que se descompone cualquier número. Más exactamente, el Teorema fundamental de la Aritmética establece que todo número mayor o igual que 2 puede ser expresado como producto de números primos (independientemente del orden de los factores)., de la siguiente manera:

$$n = p_1^{a_1} p_2^{a_2} \ldots . p_n^{a_n}$$

donde las $p_1, p_2, \ldots, p_n$ son primos tal que: $p_1 < p_2 < \ldots < p_n$ y $a_1, a_2, \ldots, a_n$ son enteros.

Propiedades de los números primos

- Si p es un número primo y divisor del producto de números enteros ab, entonces p es divisor de a ó de b. (Lema de Euclides).
- Si p es primo y a es algún entero, entonces a^p – a es divisible por p (Teorema de Fermat).
- Un número p es primo si y solo si el factorial (p – 1)! + 1 es divisible por p. (Teorema de Wilson).
- Si n es un número natural, entonces siempre existe un número primo p tal que

  n < p < 2 (Postulado de Bertrand)
- En toda progresión aritmética $a_n = a + n * q$, donde los enteros positivos a, q ≥ 1 son primos entre si, existen infinitos números primos. (Teorema de Dirichlet).
- El número de primos menores que un x dado sigue una función asintótica a

$$f(x) = \frac{x}{\ln x}$$ (Teorema de los números primos)

Mínimo común múltiplo (MCM) Y Máximo común divisor (MCD)

En ocasiones es conveniente conocer el menor de los múltiplos comunes (MCM), y el mayor de los divisores comunes (MCD) de varios números enteros. La regla de obtener dichos números es:

- Para encontrar el MCM de varios enteros se multiplican los factores primos comunes y no comunes de los números tomados con sus mayores exponentes.
- Para encontrar el MCD de varios números enteros se multiplican los factores primos comunes de los números tomados con sus menores exponentes.

Si m es el MCD de a y b esto se denotará por m = (a, b); otra manera de calcular el MCD es usando el algoritmo de Euclides, el cual se basa en la siguiente propiedad:

Si m = (a, b) y a = bq + r con 0 £r < b, entonces m = (b, r)

Y consiste en lo siguiente: Dividimos a / b obteniendo un residuo r1, después dividimos b / r1 y obtenemos un residuo r2, a continuación dividimos r1 / r2 obteniendo un residuo r3, y así sucesivamente hasta llegar a un residuo cero, el MCD de a y b será el último residuo diferente de cero.

El MCD de dos enteros a y b es el mayor entero positivo que divide a a y b con resto cero. Si el MCD de dos enteros es 1, se dice que los dos números son primos relativos o primos entre sí. A los números que son el producto de dos o más primos les llamaremos compuestos.

EJEMPLO. Usando el algoritmo de Euclides, encontrar el MCD de:

a) 328 y 1804

b) 105 y 385

a) 1804 / 328 = 5 y resto = 164

328 / 164 = 2 y resto = 0 por lo tanto (1804, 328) = 164

b) 385 / 105 = 3 y resto = 70

105 / 70 = 1 y resto = 35

70 / 35 = 2 y resto = 0 por lo tanto (385, 105) = 35

Congruencias

Decimos que los enteros a y b son congruentes módulo m, m > 0 si al dividirse entre m dejan al mismo residuo, y lo denotaremos como

$$a \equiv b \pmod{m}$$

Teorema 1.- $a \equiv b \pmod{m}$ si y sólo si $m \mid b - a$

Teorema 2.- La relación congruencia módulo m tiene las siguientes propiedades:

- $a \equiv a \pmod{m}$
- Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
- Si $a \equiv b \pmod{m}$ y $b \equiv a \pmod{m}$ entonces $a \equiv c \pmod{m}$

Es de esperarse, en vista del teorema anterior, que las congruencias se comporten en muchos aspectos como igualdades. Esta semejanza queda ilustrada en el siguiente teorema:

Teorema 3.- Sean a, b, c enteros y m entero positivo.

- Si $a \equiv b \pmod{m}$ entonces:
  a) $a + x \equiv b + x \pmod{m}$ para todo entero x.
  b) $ax \equiv bx \pmod{m}$ para todo entero x.
- Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces:
  a) $a + c \equiv b + d \pmod{m}$.
  b) $a - c \equiv b - d \pmod{m}$.
  c) $ac \equiv bd \pmod{m}$.
  d) $a^n \equiv b^n \pmod{m}$ para todo entero positivo n.

EJEMPLO.- Al dividirse los números 3, 13, 23, 33 ÷ 10, sobra 3 por lo que decimos que ellos son congruentes modulo 10. Para ilustrar una parte del teorema 3 utilizamos 3 13 (mod 10) y 23 33 (mod 10). Entonces podemos sumar las congruencias como lo indica el teorema y resulta otra congruencia. Sumando obtenemos 3 + 23 13 + 33 (mod 10).
Esto es lo mismo que 26 46 (mod 10). Podemos ver que 26 y 46 son congruentes módulo 10, ya que al dividirse entre 10 dejan residuo 6.

Primalidad de números primos

El problema de la primalidad consiste en determinar, de forma aleatoria, números primos grandes. El problema surge, entre otras razones, porque el criptosistema RSA necesita, para ser implementado, dos números primos p y q, de longitud grande (de alrededor de 200 dígitos). En general, para resolver este problema se recurre a los test de primalidad y de pseudoprimalidad.

Un test de primalidad es un criterio para decidir si un número dado es o no primo. Supongamos que n es un entero impar grande. El test de primalidad más sencillo es el test de las divisiones sucesivas. El método consiste en tomar un número entero impar m y ver si divide o no a n. Si m no es ni 1 ni n, entonces n es compuesto; en caso contrario, n pasa el intento de división por m. Es claro que los valores de m para asegurar todos los posibles casos debe ir desde 3 hasta el entero más cercano a $\sqrt{n}$, es decir, m es impar con $2 < m < \lfloor \sqrt{n} \rfloor$.

El tiempo de computación necesario para llevar a cabo el test anterior es demasiado elevado para llevarlo a la práctica, por lo que generalmente se recurre a otro tipo de pruebas, los llamados test de pseudoprimalidad. Un test de pseudoprimalidad es un criterio para decidir, con un alto grado de probabilidad, si un número dado es o no primo.

Si el número n pasa el test de pseudoprimalidad, entonces puede que sea primo; en caso contrario, es seguro que el número no es primo. Con este tipo de test se asegura si un número no es primo, mientras que la propiedad de ser primo es probabilística; es decir, el test puede no proporcionar resultados seguros si el número es primo, pero proporciona resultados seguros si el número no es primo. En general, hay dos procedimientos para obtener números primos de forma más o menos rápida. El procedimiento depende, fundamentalmente, del tamaño del número que se desea. Si el número primo no es grande, basta recurrir a alguna de las tablas de números primos publicadas, pero el inconveniente es que estos números son muy pequeños para objetivos criptográficos. Así, habitualmente el procedimiento seguido para obtener números primos de tamaño grande consiste en generar, aleatoriamente, enteros impares y aplicarles un test de pseudoprimalidad.

Teorema de Tchebycheff. La cantidad de números primos menores o iguales que x, π(x), es asintóticamente equivalente a $\frac{x}{\ln x}$; es decir, $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$

Ejemplo. Según este resultado, la proporción de números primos entre el total de números impares de 100 cifras sería:

$$\frac{\pi(10^{100}) - \pi(10^{99})}{impares\,de\,100\,cifras} \approx \frac{1}{115}$$

y, por tanto, es de esperar que el número de tests de primalidad necesarios para encontrar un número primo de 100 dígitos sea de 115. Veamos algunos de los más conocidos tests de pseudoprimalidad. El primero de ellos se basa en el Teorema (pequeño) de Fermant. Ya sabemos que si n es primo, entonces para cualquier b con mcd (b, n) = 1, se tiene que:

$$b^{n-1} \equiv (\text{mod } n) \qquad (1)$$

Sin embargo, puede que no sea primo y que se siga verificando la congruencia (1). Si n es un número compuesto impar y b es un número entero con mcd (b, n) = 1 de modo que se verifica (1), entonces n se llama un pseudoprimo de base b. Puede suceder que un número n sea compuesto y verifique la propiedad (1). Los números que verifican la propiedad anterior para cualquier b se llaman números de Carmichael. Los primeros números de Carmichael son 565, 1105 y 1729. Estos números son bastantes raros de encontrar; baste decir que hay 255 números de Carmichael menores de 100 millones.

Ejemplo. Consideremos el número n = 91. Este número es un pseudoprimo de base b = 3, puesto que $3^{90} \equiv 1$ (mod 91); sin embargo, p1 no es un pseudoprimo de base 2, puesto que $2^{90} \equiv 64$ (mod 91).

Un primer test de pseudoprimalidad para determinar si un número n es primo consiste en hacer pasar a n por el test anterior para t valores de b elegidos independientemente. La probabilidad de que el número n no primo pase los t test es de 2^{-t}.

Test de Solovay-Strassen

Pasemos a describir a hora el test de Solovay-Strassen. Supongamos que n es un entero positivo impar y queremos saber si n es un número primo o compuesto. Para ello se eligen k enteros $0 < b < n$ aleatoriamente. Para cada uno de estos números b se calculan los valores de $b^{(n-1)/2}$ y de $\left(\frac{b}{n}\right)(\mathrm{mod}\, n)$.

Si estos dos valores no son congruentes módulo n, entonces n es un número compuesto y el test se detiene. En otro caso, se prueba el siguiente valor de b. Si los valores anteriormente calculados son congruentes para k valores de b, independientemente elegidos, entonces hay una probabilidad menor a 2^{-k} de que n no sea primo. Así pues, el test de Solovay-Strassen es un algoritmo probabilístico que lleva a la conclusión de que o bien n es compuesto o bien es un primo probable.

Si n es un número entero impar y b es un entero con mcd (n, b) = 1 y se verifica la congruencia anterior, es decir, si $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right)(\mathrm{mod}\, n)$, entonces n se llama un pseudoprimo de Euler de base b.

Test de Miller-Rabin

Vamos a ver otro test de primalidad, que está basado en los pseudoprimos de Euler y que es mejor que el de Solovay-Strassen; es el test de Miller-Rabin. Supongamos que n es un entero positivo impar grande, que b es de Z_n^* y que n es un pseudoprimo de base b; es decir, que $b^{n-1} \equiv 1 \pmod n$. La idea del test consiste en extraer raíces cuadradas a la congruencia anterior; es decir, si se calculan las potencias (n-1)/2, (n-1)/4, ..., $(n-1)/2^s$ (donde $t = (n-1)/2^s$ es impar), entonces la primera clase de residuos distinta de 1 debe ser -1 si n es primo, puesto que ± 1 son las únicas raíces cuadradas de 1 módulo un número primo.

En la práctica se procede del modo contrario; es decir, se escribe $n = 2^s \times t$ con t impar; luego se calcula $b^t \pmod n$, entonces (si no es congruente con 1 módulo n) se determinan los cuadrados $b^{2t} \pmod n$, $b^{2^2 t} \pmod n$, etc., hasta que se obtenga el primer residuo 1. En el paso anterior a obtener 1, debemos obtener -1, o en caso contrario sabemos que n es compuesto. Si n es un número compuesto impar y escribimos $n = 2^s \times t$ con t impar, y si b pertenece a Z_n^*, entonces si n y b satisfacen o bien la condición $b^t \equiv 1 \pmod n$ o bien existe un número r, $0 \le r < s$, tal que $b^{2^r t} \equiv -1 \pmod n$, entonces a n se le llama pseudoprimo fuerte de base b.

APÉNDICE II

RFC DE INTERNET		
Número	**Título**	**Fecha**
RFC 822	Estándar para el formato de mensajes de texto de Internet ARPA	1982
RFC 1321	Algoritmo de resumen de mensaje MD5	1992
RFC 1510	Servicio de autentificación de red Kerberos v5	1993
RFC 1636	Seguridad en la arquitectura de Internet	1994
RFC 1928	Protocolo SOCKS versión 5	1996
RFC 2026	Proceso de normalización de Internet	1996
RFC 2040	Algoritmos RC5, RC5-CBC,RC5-CBC-PAD y RC5-CTS	1996
RFC 2045	MIME Primera Parte: formato del cuerpo de mensajes en Internet	1996
RFC 2046	MIME Segunda Parte: tipos de medios	1996
RFC 2047	MIME Tercera Parte: ampliaciones de la cabecera de mensaje para texto no ASCII	1996
RFC 2048	MIME Cuarta Parte: procedimientos de registro	1996
RFC 2049	MIME Quinta Parte: criterios de conformidad y ejemplos	1996
RFC 2104	HMAC: Hash con claves para autentificación de mensajes	1997
RFC 2401	Arquitectura de seguridad para el protocolo de Internet	1998
RFC 2402	Cabecera de autentificación IP	1998
RFC 2408	Asociación de seguridad de Internet y protocolo de gestión de claves	1998
RFC 2459	Define lo que debe contener el certificado	1999
RFC 2828	Glosario de seguridad en Internet	2000
X.509	Marcos de clave pública y certificado de atributos	2000
X.800	Arquitectura de seguridad para la interconexión de sistemas abiertos	1991
FIPS 46-3	Estándar de cifrado de datos (DES)	1999
FIPS 81	Modos de operación del DES	1980
FIPS 113	Autentificación de datos computacionales	1985
FIPS 180-1	Estándar hash seguro	1995
FIPS 181	Generador automático de contraseñas	1993
FIPS 186-2	Estándar de firma digital	2000
PKCS # 1	Proporciona las recomendaciones para la implementación de criptografía de clave publica basada en el algoritmo RSA, cubriendo aspectos como: primitivas criptográficas, esquemas de cifrado, esquemas de firma y sintaxis ASN.1 para la representación de claves y para identificar los esquemas.	2002
PKCS # 3	Describe un método para implementar el acuerdo de claves por Diffie-Hellman utilizado en los protocolos para establecer comunicaciones seguras.	1993
PKCS # 5	Proporciona las recomendaciones para la implementación de criptografía basada en contraseñas, cubriendo aspectos como: derivación de claves, esquemas de cifrado y esquemas de autenticación de mensajes.	1999
PKCS # 6	Describe la sintaxis para certificados extendidos, consistentes en un certificado y un conjunto de atributos, firmados por el emisor del certificado.	1993
PKCS # 7	Describe la sintaxis general para los datos que pueden tener criptografía aplicada a ellos mismos, tal como firmas digitales y sobres digitales.	
PKCS # 8	Describe la sintaxis para la información de la clave privada, incluyendo una clave privada para algún algoritmo de la clave pública y un conjunto de atributos. También describe la sintaxis para las claves privadas cifradas.	1993
PKCS # 9	Define los tipos de atributos seleccionados para el uso en certificados extendidos (PKCS #6), mensajes firmados digitalmente (PKCS #7), información de la clave privada (PKCS #8), y requerimientos de certificación (PKCS #10).	2000
PKCS # 10	Describe la sintaxis para un requerimiento de certificación de una clave pública, de un nombre, y posiblemente de un conjunto de atributos.	2000

PKCS # 11	Especifica una API, llamada Cryptoki, por medio de la cual los dispositivos que contienen información criptográfica realizan funciones criptográficas.	2004
PKCS # 12	Especifica un formato portable para almacenar o transportar las claves privadas de un usuario, los certificados, etc.	1999
PKCS # 13	Es el estándar de la criptografía de curvas elípticas que todavía está en desarrollo. Tratará muchos aspectos, incluyendo parámetros, generación y la validación de la llave, firmas digitales, el cifrado público, y la sintaxis dominante ASN.1.	2005
PKCS # 15	Es una especificación definida por RSA Data Security que pretende estandarizar el acceso a la información PKI y del método o métodos de autenticación almacenada en una tarjeta inteligente.	2000
RFC 2196	Guía creada por el IETF para desarrollar normas y procedimientos de seguridad para sitios que tengan sistemas en Internet.	1997
RFC 2559	Define los protocolos operacionales para la PKI	1999
RFC 2585	Define el uso de FTP y HTTP para el transporte de las operaciones de la PKI	1999
RFC 2510	Protocolos de gestión para los certificados X.509	1999
RFC 2560	Protocolo de verificación online de certificados X.509 (OCPS)	1999
RFC 2797	Define un protocolo de administración de certificados utilizando CMS	1999
RFC 2511	Formato de mensaje de petición de certificados X.509	1999
RFC 2527	Declaración de prácticas de certificación para los servicios de certificación	1999

GLOSARIO

Amenaza. Toda circunstancia o evento con el potencial de causar daños en un sistema de red. Una amenaza puede adoptar formas dañinas, como los intrusos de red, y peligros no dañinos, como los rayos.

Appletalk. Es una arquitectura para LAN construida para las computadoras de Apple Macintosh. Appletalk apoya el esquema que cablegrafía de LocalTalk de Apple, así como Ethernet y token ring de la IBM . Puede conectar las computadoras y las impresoras de Macintosh , e incluso las PC si se equipan del hardware y del software especiales de Appletalk .

Arcnet. Es una red en banda base que utiliza una topología mixta estrella/bus con protocolo de paso de testigo. Transmite a una velocidad de 2.5 Mbps y todos los computadores han de estar conectados a un concentrador (Hub activo). La distancia máxima entre el computador y el Hub activo no puede sobrepasar los 660 metros.

Ataque de Negación de Servicio. Cualquier acción que impide que alguna parte de una red o sistema de hosts funcione de acuerdo a su finalidad.

Autentificación. Se llama así al proceso de validación de la conexión del usuario que determina el permiso de acceso a los recursos del servidor.

Autoridad de Certificados (CA). Una entidad en la que se confía para la firma de certificados digitales, y que certifica la identidad.

Certificado. Un mensaje firmado digitalmente con la clave privada de una tercera parte de confianza, que declara que una clave pública específica pertenece a alguien o a algo que tenga un nombre y un conjunto de atributos específico.

Clave Privada. Es un código digital que se usa para descifrar información y proporcionar firmas digitales. Esta clave deberá ser mantenida en secreto por su propietario; tiene su clave pública correspondiente.

Clave Pública. Es un código digital que se usa para cifrar información y verificar firmas digitales. Esta clave puede ser puesta a disposición de todo el mundo; tiene su clave privada correspondiente.

Confidencialidad. Garantía de que la información no es revelada a personas que no deben recibirla.

Control de Acceso. Limitación del flujo de información de los recursos de un sistema a las personas, programas, procesos u otros sistemas autorizados de una red.

Cracker. Es un usuario informático que invade en secreto el computador de otro usuario para inspeccionar, alterar o incluso dañar la información y programas que se encuentre en él.

Criptografía. Es la ciencia de escribir o leer mensajes codificados.

Datagrama. Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el ordenador receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ordenador destino.

Disponibilidad. Un estado de los sistemas y redes de computación en el que el sistema está operativo y puede ejecutar los servicios que está obligado a prestar.

DNS. Sistema de nombre de dominio (Domain Name System), es un esquema para la traducción de direcciones internas de Internet en cadenas de caracteres y palabras con significado de nombres de usuarios y lugares de conexión.

Encriptación. Se llama así al proceso de hacer indescifrable la información para proteger su uso o su visualización no autorizada durante el proceso de transmisión o cuando se guarda en un medio magnético transportable.

Ethernet. Es un estándar para redes de área local en banda base a 10 Mbits/s que emplea CSMA/CD para control de acceso. Más tarde adoptado como estándar IEEE 820.3.

Firewall. Es una barrera establecida en hardware o software (o en ambas) que permite que el tráfico de la red sólo fluya hacia fuera para protección de la red.

Firma Digital. Una cadena de bits adjunta a un mensaje (un hash cifrado) que proporciona la autentificación y la integridad de los datos.

FTP. Protocolo de transferencia de archivos (File Transfer Protocol), es una aplicación de Internet que permite transferir archivos de un computador a otro. Las siglas FTP también pueden hacer referencia al propio protocolo.

Función Hash. Un cálculo matemático que resulta en una cadena de bits de longitud fija (código digital) de una entrada de tamaño arbitrario; la función no se puede invertir para que genere la entrada original.

Hacker. Es un usuario informático que además de programar su computador, se introduce en sistemas operativos y programas de otros computadores para descubrir su funcionamiento.

HTTP. Es un protocolo relativamente simple que utiliza los servicios proporcionados por el protocolo TCP del nivel de transporte para transferir archivos desde los servidores a los clientes.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers), es la organización más grande del mundo. Además de publicar revistas y organizar numerosas conferencias cada año, el IEEE tiene un grupo de estandarización que elabora estándares en las áreas de ingeniería eléctrica y computación. El estándar 802 del IEEE para redes de área local es el estándar clave para las LAN.

IETF (Internet Engineering Task Force). Es una organización existente dentro del Consejo de la Arquitectura Internet cuya finalidad es discutir y dar solución a los posibles problemas técnicos que pueda tener Internet.

Infraestructura de Clave Pública (PKI). Una clave de confianza y eficiente, así como un sistema de administración de certificados.

Integridad. Es el proceso de garantizar que los datos no han sido alterados más que por las personas cuyo cometido legítimo sea precisamente el de modificarlos.

IP (Internet Protocol). Es el protocolo de nivel de red usado en Internet. Mediante el protocolo IP cualquier paquete puede viajar a través de las distintas redes de Internet hasta llegar a su destino final. Registra las direcciones de nodos, encamina los mensajes que se envían y reconoce los mensajes recibidos.

IPv4. IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primer versión del protocolo que se implemento extensamente, y forma la base de Internet.

Irrebatibilidad. Es una propiedad de un sistema de cifrado que impide a un emisor negar con posteridad que ha enviado un mensaje o llevado a cabo una determinada acción.

Kerberos. Es un protocolo de autentificación de red de clave secreta, desarrollado en el Massachussets Institute of Technology (MIT), que utiliza el algoritmo de cifrado DES para el cifrado y una base de datos de claves centralizada para la autentificación.

Lista de Revocación de Certificados (CRL). Es una lista firmada digitalmente de todos los certificados creados por una autoridad de certificados determinada que todavía no ha expirado, pero que ya no es válida**.**

NNTP. Network News Transport Protocol (NNTP), o protocolo de transferencia de noticias. Es el Protocolo de red utilizado por el Usenet Internet Service. Es un Protocolo de red basado en tiras de textos envíados sobre canales TCP de 7 bit ASCII . Es usado para subir y bajar así como para transferir artículos entre servidores.

OSI (Open System Interconnection). Es un modelo de referencia o estructura lógica en torno al cual se construye la arquitectura de un sistema abierto. El modelo de referencia ISO 7489 especifica una arquitectura de red de siete capas utilizada en la definición de estándares para protocolos que permiten a cualquier dispositivo compatible OSI conectarse con cualquier otro dispositivo.

PCMCIA. Es un dispositivo normalmente utilizado en computadoras portátiles para expandir las capacidades de estas. Reciben su nombre del estándar (Personal Computer Memory Card International Association, asociación de la industria de fabricantes de hardware para ordenadores o computadoras portátiles encargada de la elaboración de estándares) y pueden ser de muy distintos tipos: memoria, disco duro, tarjeta de red, etc. Las tarjetas PCMCIA de 16 bits reciben el nombre de PC Card y las de 32 bits el de CARD BUS.

Proxy. El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Red de Área Ancha. Es una red formada por nodos conectados en un área geográfica extensa. También se le puede denominar RED DE ÁREA EXTENSA o AMPLIA.

Red de Área de Almacenamiento. Es una red de recursos de almacenamiento compartidos que pueden asignarse a diferentes sistemas.

Red de Área Local. Es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar con los ordenadores correspondientes, tarjetas de red, los cables de conexión, los dispositivos periféricos y el software conveniente.

Red de Área Metropolitana. Es una red formada por nodos conectados en un área geográfica localizada dentro de una ciudad.

Red X.25. Es un protocolo de transmisión de red de paquetes ISO utilizado en muchas redes de área extensa. Forma parte del modelo OSI.

Red. Grupo de ordenadores y otros dispositivos periféricos conectados unos a otros para comunicarse y transmitir datos entre ellos.

RFC (Request for Comments). Son una serie de documentos o informes técnicos que edita la IAB (*Internet Architecture Board* - Consejo de Arquitectura de Internet), con el propósito de regular los estándares y procedimientos de estandarización en el Internet.

Rivest, Shamir, Adelman (RSA). Es un algoritmo de cifrado de clave pública que puede cifrar o descifrar los datos y que puede aplicar o verificar una firma digital.

Router. Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o bien una combinación de ambos.

Seguridad en Redes. Son las medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación de las redes.

SMTP. Protocolo simple de transferencia de correo (Simple mail Transfer Protocol), se basa en el servicio de correo electrónico en Internet. Define el formato que deben tener los mensajes y cómo deben ser transferidos. Gracias a SMTP distintos fabricantes de software pueden desarrollar programas completamente compatibles entre sí.

SSH. Es un protocolo de seguridad del nivel de transporte que se usa para realizar una conexión segura con un computador remoto, ejecutar comandos y mover archivos a o desde dicho computador.

SSL. Es un protocolo de seguridad del nivel de transporte que proporciona codificación de datos, autentificación de servidor e integridad de mensajes para una conexión TCP/IP.

Switch. O conmutador es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TCP. Es un conjunto de protocolos de los niveles de red y transporte del modelo OSI que permite el intercambio de datos de computadores conectados a Internet.

Telnet. Es una aplicación de Internet usada para acceder a otros computadores de la red. Mediante ella se puede utilizar una gran variedad de servicios.

Token Ring. Es un mecanismo de acceso para redes de área local y una topología. Un testigo (token) pasa de una estación a otra a lo largo del anillo. Las estaciones pueden emitir sólo cuando están en posesión del anillo. Los datos pasan de estación en estación hasta que vuelve a la estación originaria.

Token. Palabra utilizada en la industria de la seguridad para referirse a un *hardware* o a objetos físicos que se utilizan para proteger la información o la identidad. A diferencia de las soluciones de seguridad basadas en *software*, las tarjetas inteligentes se consideran como un "token tipo *hardware"*.

Trama. Es una unidad de transmisión de red en el nivel de enlace de datos. Se refiere a la unidad que se envía fuera de la estación origen en una red física.

UDP. Acrónimo de User Datagram Protocol (Protocolo de datagrama a nivel de usuario), perteneciente a la familia de protocolos TCP/IP. Este protocolo no es tan fiable como TCP, pues se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar el éxito de la transferencia, UDP hace que la máquina de destino envía un mensaje de vuelta. Si no es así, el mensaje se envía de nuevo. Con este protocolo no se establece una conexión entre las dos máquinas.

Virus. Pequeño programa adjuntado a otro legítimo y que provoca una acción no deseada por los usuarios cuando éstos acceden a dicho programa. Algunos pueden actuar de forma inofensiva, pero otros pueden causar daños como borrar o modificar archivos.

FUENTES DE INFORMACIÓN

BIBLIOGRAFÍA

Brown, Steven: **"Implementación de Redes Privadas Virtuales"**., México, Edit. McGraw – Hill, 2001.

Carracedo, G. Justo: **"Seguridad en Redes Telemáticas"**., España, Edit. McGraw-Hill, 2004.

Carreto P. Jesús: **"Sistemas Operativos: Una visión Aplicada"**., España. Edit. McGraw-Hill, 2001.

Farley, Marc; Stearns, Tom; Hsu, Jeffrey: **"Guía LAN TIMES de Seguridad e Integridad de Datos"**., España, Edit. Osborne McGraw – Hill, 1998.

Gallo, A. Michael; William, M. Hancock**: "Comunicación entre Computadoras y Tecnologías de Redes".,** México, Edit. Thomson, 2002.

Garfinkel, S.; Spafford, G.: **"Seguridad y Comercio en el Web"**., México, Edit. McGraw – Hill, 1999.

Heywood, D: **"Redes con Microsoft TCP/IP"**., España, Edit. Prentice Hall, 1999.

Hinrichs, J. Randy: **"Intranets, Usos y Aplicaciones"**., México, Edit. Prentice Hall, 1997.

Karanjit, Siyan; Hare, Chris: **"Firewalls y la Seguridad en Internet"**., México, Edit. Prentice– Hall Hispanoamericana, 1997.

Leon, C. David: **"Guía para el Administrador de Redes Privadas Virtuales (RPV)".,** México, Edit. McGraw – Hill, 2000.

Littlejohn, S. Debra: **"Prevención y Detección de Delitos Informáticos"**., España, Edit. Anaya Multimedia, 2003.

Maiwald, E: **"Fundamentos de Seguridad de Redes"**., México, Edit. McGraw-Hill, 2004.

Mariño. E. Perfecto: **"Las Comunicaciones en la Empresa, Normas, Redes y Servicios".**, España, Edit. Rama, 1995

Merike, Kaeo: **"Diseño de Seguridad en Redes"**., España, Edit. Cisco Systems, 2003.

Milenkovic, Milan: **"Sistemas Operativos: Conceptos y Diseño".,** España. Edit. McGraw-Hill, 1988.

Nash, Andrew; Duane, William; Joseph, Celia; Brink, Derek: **"Infraestructura de Claves Públicas".,** Colombia, Edit. Osborne McGraw – Hill, 2002.

Raya C. Jose, Raya P. Cristina: **"La Seguridad de una Red con Netware 5".,** México, Edit. Alfaomega-Rama, 2000.

Stallings, W: **"Fundamentos de Seguridad en Redes, Aplicaciones y Estándares".,** España, Edit. Prentice Hall

Stallings, W: **"Sistemas Operativos".,** España, Edit. Prentice Hall, 1997.

Tanenbaum, S. Andrew: **"Redes de Computadoras"**., México, Edit. Prentice Hall, 1991.

Vaca, R. John: **"Los Secretos de la Seguridad en Internet"**., España, Edit. Anaya Multimedia, 1997.

Zacker, C: **"Manual de Referencia de Redes"**., España, Edit. McGraw-Hill, 2002.

REFERENCIAS ELECTRÓNICAS

FIPS PUB-191. Creado por el NIST., aunque está escrito específicamente para las LAN, esta publicación es aplicable a cualquier entorno computarizado. El uso de la gestión de riesgos se presenta para ayudar al lector a determinar los activos LAN, identificar las amenazas y puntos débiles, determinar el riesgo de tales amenazas sobre la LAN, y determinar los posibles servicios y mecanismos de seguridad que se pueden usar para ayudar a reducir el riesgo para la LAN.
http://www.itl.nist.gov/div897/pubs/fip191.htm

Información sobre Telecomunicaciones (Comisión Federal de Telecomunicaciones)
http://www.cft.gob.mx/html/la_era/info_tel/it3.html
http://www.cofetel.gob.mx/

Infraestructura de Clave Pública (X.509). Detalla los estándares internet que soportan una PKI X.509
http://www.irtf.org/html.charters/pkix-charter.html

Libro Electrónico de Seguridad Informática y Criptografía versión v 3.2
http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Libro Naranja
http://www.radium.ncsc.mil/tpep/library/rainbow/

Lista de Estándares de Seguridad Informática
http://www.unal.edu.co/seguridad/estandares_de_seguridad_internacionales.pdf

Protocolo de Seguridad IP
http://www.ietf.org/html.charters/ipsec-charter.html

RFC 2196.- Guía creada por el IETF para desarrollar normas y procedimientos de seguridad para sitios que tengan sistemas en Internet
http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2196.txt

RSA
http://www.rsa.com

Seguridad de la Capa de Transporte
http://www.ietf.org/html.charters/tls-charter.html

Seguridad Informática
http://cfbsoft.iespana.es/cfbsoft_es/seguridad/

Seguridad Informática, Criptografía, Criptoanálisis
http://www.htmlweb.net/seguridad/seguridad.html

Seguridad WWW
http://www.genome.wi.mit.edu/WWW/faqs/www-security-faq.html

Seguridad y Protección de la Información
www.evidalia.com/tutoriales/categoria.php

THE SITE SECURITY HANDBOOK (libro sobre la seguridad de los sitios). Libro destinado a que los usuarios creen normas específicas del sitio y procedimientos que traten con problemas relativos a la seguridad computacional y su prevención
http://www.ietf.org/html.charters/ssh-charter.html

CSI/FBI
http://www.gocsi.com