26

UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN

CONTROL DE ACCESO Y SEGURIDAD EN LA INFORMACIÓN COMPUTACIONAL

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

CAROLINA GARCÍA PADILLA

ASESOR DE TESIS: **ING. GLADIS E. FUENTES CHÁVEZ**

CAMPUS ARAGON

MÉXICO 2001

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCION

VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

CAROLINA GARCÍA PADILLA
P R E S E N T E.

En contestación a la solicitud de fecha 22 de junio del año en curso, relativa a la autorización que se le debe conceder para que la profesora, Ing. GLADIS EMILIA FUENTES CHÁVEZ pueda dirigirle el trabajo de tesis denominado, "CONTROL DE ACCESO Y SEGURIDAD EN LA INFORMACIÓN COMPUTACIONAL" con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 7 de julio del 2000
EL DIRECTOR

M en R.I. CARLOS EDUARDO LEVY VÁZQUEZ

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON UNAM
DIRECCION

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería en Computación.
C p Asesor de Tesis.

CELV/AIR/BGC'vr

VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

JEFATURA DE INGENIERÍA EN COMPUTACIÓN

OFICIO: ENAR/JACO/0435/2001.

ASUNTO: Designación de Revisores.

MAT. LUIS RAMÍREZ FLORES

ING. SILVIA VEGA MUYTOY

ING. JUAN JOSÉ MARTÍNEZ COSGALLA

ING. RICARDO SÁNCHEZ MARTÍNEZ

ING. GLADIS EMILIA FUENTES CHAVEZ

Informamos a ustedes de la autorización que se le concede la alumna **CAROLINA GARCÍA PADILLA,** para que pueda desarrollar el trabajo de tesis titulado: **"CONTROL DE ACCESO Y SEGURIDAD EN LA INFORMACIÓN COMPUTACIONAL"** dirigida por la **Ing. Gladis Emilia Fuentes Chávez,** solicitando a ustedes sean tan amables de revisar el avance del mismo y hacer las observaciones que consideren pertinentes, o en su caso, indicar a la alumna si dicha revisión se hará a la conclusión del trabajo de tesis.

Sin otro particular, me es grato enviarles un cordial saludo

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
San Juan de Aragón Edo. de Méx., julio 2 del 2001.
EL JEFE DE CARRERA

M. EN C. JESÚS DÍAZ BARRIGA ARCEO

JDA/mav.

UNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

JEFATURA DE CARRERA DE INGENIERÍA EN COMPUTACIÓN

OFICIO: ENAR/JACO/0425/2001.

ASUNTO: Asignación de Jurado.

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P r e s e n t e .

Por este conducto me permito presentar a usted, nombre de los profesores que sugiero integren el Sinodo del Examen Profesional de la alumna **CAROLINA GARCÍA PADILLA**, que presenta el tema de tesis : **"CONTROL DE ACCESO Y SEGURIDAD EN LA INFORMACIÓN COMPUTACIONAL".**

PRESIDENTE:	**MAT. LUIS RAMÍREZ FLORES**
VOCAL:	**ING. SILVIA VEGA MUYTOY**
SECRETARIO:	**ING. GLADIS FUENTES CHÁVEZ**
SUPLENTE:	**ING. JUAN JOSÉ MARTÍNEZ COSGALLA**
SUPLENTE:	**ING. RICARDO SÁNCHEZ MARTÍNEZ**

Quiero subrayar que el director de tesis es la **Ing. Gladis Emilia Fuentes** Chávez, el cual está incluido con base en lo que reza el reglamento de Exámenes Profesionales de ésta Escuela.

Sin otro en particular, me es grato enviarle un cordial saludo.

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, Edo. de México, julio 2del 2001.
EL JEFE DE CARRERA

M. EN C. JESÚS DÍAZ BARRIGA ARCEO

c.c.p. Lic. Ma. Teresa Luna Sánchez.- Jefa del Departamento de Servicios Escolares.
Ing. Gladis Emilia Fuentes Chávez.-Asesor de tesis.

JDA/mav.

Dedico este trabajo, como todos los que he realizado y pueda realizar, **A MI PADRE**. Porque él ha sabido ser el mejor amigo, que ofrece su hombro para apoyarme cada vez que he sentido que puedo caer, y ha ofrecido su mano siempre para celebrar una alegría y hacerla aun mayor. Porque ha sabido ser el pilar del hogar, que ha dado SIEMPRE todo lo mejor de él y de su trabajo, para el bien y el progreso de su familia. Porque ha sabido ser la persona estricta en el momento preciso, y me ha corregido a tiempo. Porque siempre me ha brindado TODO su apoyo, confianza y comprensión.

Pero sobre todas las razones, le dedico a él lo que soy, porque ha sido precisamente mi padre quien me ha formado, soy el fruto de sus esfuerzos y sacrificios, y es lo menos que puedo hacer por él.

¡Muchas gracias papá, que DIOS te bendiga y te conserve bien!

Carolina García.

Cursar una carrera profesional, es una oportunidad de la cual no gozan muchas personas, y el poder llevarlo a cabo implica muchas experiencias agradables, pero también sacrificios por realizar. He sido afortunada, porque hoy me cuento entre la gente que ha podido ser parte de una generación más de estudiantes a nivel licenciatura, y porque he concluido la formación de esta etapa con el presente trabajo terminal. Pero, para que eso sucediera, afortunadamente han contribuido muchas personas que han sido parte importante de este equipo, y es por eso que les deseo dar un justo agradecimiento.

Por ocupar hoy el lugar que tengo, agradezco primeramente a DIOS, por haberme dado la oportunidad de llegar a este peldaño en la escalera de la vida, y por guiar a mi padre para ser un excelente amigo y padre a la vez. Agradezco a mi papá Andrés García Flores por todo el apoyo, motivación y comprensión incondicionales que SIEMPRE me ha brindado. A nuestra Universidad Nacional, por haberme abierto sus puertas y dejarme sentir con el corazón el privilegio y la responsabilidad que implica, ser parte de esta gran Institución. Al Sr. Miguel Angel Palma, que nos permitió trabajar cuando recién iniciaba mi carrera. A todos mis profesores de TODOS los niveles de estudio, que paso a paso me han conducido por el camino del saber compartiendo sus conocimientos, pero sobre todo aquellos que además de la Formación Académica, me han brindado su Amistad. A Ricardo Rugerio, por la paciencia que me ha tenido y por sus orientaciones, que nunca me han faltado. Al Ing. Irán Zadok Echávarry Gaytán por todas las facilidades, consejos y el apoyo ofrecidos para el desarrollo de mi trabajo. A la Ing. Gladis E. Fuentes Chávez por TODO el tiempo, apoyo, comprensión y paciencia que tuvo conmigo en la estupenda conducción de mi trabajo y por la ayuda que me brindó con los trámites del mismo. Al personal del Plan de Becas de la Dirección de Cómputo para la Administración Académica, principalmente a la Lic. Rosario Salinas, la Lic. Georgina Castelán y el Lic. Roberto Viveros, por haberme brindado la oportunidad de formar parte de su plantilla de becarios y complementar así mi formación académica. A la Sra. Maribel Diaz, por todo el apoyo que me ha dado y los ánimos que me transmitió para el mejor desarrollo de mi trabajo. Al Dr. César A. Colina Ramírez por la confianza que tiene en mi y en mi trabajo. A todo el personal secretarial del Departamento de Apoyo Operativo y de la Secretaría de Servicios Escolares de la Facultad de Medicina por su ayuda para la presentación y realización de mi trabajo. A todos mis familiares paternos, que aunque a la distancia, siempre han estado conmigo y me han hecho sentir el mejor de sus apoyos. Finalmente, quiero agradecer a TODOS MIS AMIGOS, los cuales no menciono por temor a omitir alguno, que siempre han estado conmigo y me han brindado su compañía y amistad sincera.

A TODOS ustedes y los que de alguna manera hicieron posible que alcanzara esta etapa:

De verdad, ¡**MUCHAS GRACIAS**!

Sinceramente.

Carolina García.

ÍNDICE

INTRODUCCIÓN

La razón de revisar un tema como *el control de acceso y la seguridad en la información computacional*, obedece a que la seguridad en cómputo es un tema que toma cada vez más importancia, tanto a nivel mundial como en el país.

La explosión tecnológica facilita las labores cotidianas, sin embargo, se deben tomar nuevas medidas en cuanto a la implementación de los sistemas de cómputo para que las personas no puedan acceder a información que no les pertenece.

En virtud de que todavía no existen procedimientos legales para ser aplicados contra criminales informáticos, es una obligación individual protegerse tanto de los atacantes externos como internos; para ello es necesario tener una base de conocimiento para comprender mejor qué es lo que está pasando, y saber cómo profundizar cada vez más y de mejor forma en el tema. Con la finalidad de contar con las bases que se mencionan, es que está pensado este trabajo, pues se considera de mayor importancia dar a conocer el tema al lector, para que después se encuentre en condiciones de localizar y entender los sistemas de protección que existen actualmente.

Uno de los problemas más graves que trae consigo el avance tecnológico, es la *Seguridad*. Los países industrializados y los que no lo son aún completamente, día a día se vuelven más dependientes de la tecnología informática: de las computadoras y de la red mundial que las conecta. Esta dependencia se ha convertido en amenaza al bienestar económico, a la seguridad ciudadana, y a la seguridad nacional de muchos países, aun de los más poderosos. Cabe señalar que, la amenaza va en aumento, y que por lo tanto, se demanda gente capacitada y de investigación de nuevas tecnologías.

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. La Seguridad de los Sistemas de Información (SSI) está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por las computadoras y las redes de comunicación.

Los sistemas de información son considerados parte fundamental de una organización, y se debe otorgar la misma importancia a la información que éstos procesan y almacenan.

Es notable el grado de dependencia que el mundo moderno ha desarrollado respecto a la informática; de acuerdo al documento oficial relativo a la instalación de la Comisión Nacional para la Conversión Informática Año 2000[1], en Julio de 1988, se apuntaba que en nuestro país existían poco más de 3.6 MM de computadoras; lo cual permite hacer un análisis acerca del crecimiento explosivo que se ha dado en esta industria, ya que a mediados de los 70 se contabilizaban poco mas de 100.0M de computadoras en operación, en todo el mundo [2]. Resulta fácil entender que una paralización general - deliberada o accidental -, de sistemas vitales para el funcionamiento de la sociedad, harían que ésta se colapse.

Con la infraestructura de comunicaciones que existe actualmente, las redes de cómputo han alcanzado gran auge, con el advenimiento de Internet, se han abierto a los usuarios posibilidades nunca imaginadas. Actualmente, una persona puede tener acceso a información localizada físicamente en otro lugar, incluso al otro lado del mundo, sin siquiera moverse de su lugar. Por otra parte, a pesar de que la mayor parte de las empresas prefieren abstenerse de dar parte cuando se suscita un incidente de seguridad, el índice de delitos informáticos realizados por medio de redes, crece exponencialmente año con año.

Los problemas técnicos, las amenazas ambientales, las condiciones de instalación desfavorables, los usuarios, la situación política y social, son otros tantos factores susceptibles de poner en peligro el buen funcionamiento de los sistemas de información. Las amenazas a éstos van desde desastres naturales tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos, virus, con un origen tanto interno como externo.

Las decisiones relacionadas con la seguridad informática no son triviales. Muchas veces no se sabe por donde empezar, ¿cómo conseguir un nivel de seguridad?, ¿cómo saber si se tiene un nivel mínimo de seguridad?, ¿qué beneficio habrá si se define un plan de contingencia?. En muchas organizaciones, estas responsabilidades recaen sobre una única persona, quien implícitamente las aplica sin una definición formal. Este hecho implica importantes conflictos, dado que los diferentes grupos o personas no entienden o interpretan de la misma forma los conceptos necesarios; y esto, por lo tanto, puede impedir tomar decisiones críticas de forma satisfactoria en situaciones de emergencia.

---

[1] Documento para la instalación de la Comisión Nacional para la Conversión Informática Año 2000, INEGI. Gobierno Federal de los Estados Unidos Mexicanos, (Julio 1998).
[2] Gordon, B. Davis, Computer Data Processing, McGraw-Hill International (2nd. Edition –1973).

Es por eso que en el presente trabajo se abordarán estos temas por medio de la siguiente organización:

⇒ En el capítulo uno, se verán antecedentes de la seguridad informática; así como los conceptos básicos relacionados con la misma y sus principios fundamentales.

⇒ En el capítulo dos, se revisará la seguridad en los sistemas operativos: la identificación y autentificación con el sistema, las formas de protección de memoria y lo que son los modelos y mecanismos de seguridad.

⇒ En el capítulo número tres, se tratará el tema de la criptografía; su historia, conceptos básicos y la importancia de ésta y los sistemas de cifrado dentro de la seguridad informática.

⇒ Finalmente, en el capítulo cuatro, se abordará de manera general el tema de la seguridad en las redes de información, y por lo tanto se revisará el protocolo más usado en las transmisiones de información a través de la INTERNET, TCP/IP.

OBJETIVOS

- ✓ Ayudar a crear una conciencia de la importancia de la seguridad informática.
- ✓ Conocer las diferentes formas de vulnerar la seguridad de los sistemas y las técnicas empleadas para solucionar estas deficiencias.
- ✓ Poner de manifiesto la necesidad y justificación de protección de la información, tanto almacenada como transmitida.
- ✓ Que el lector adquiera un grado de análisis y pueda planificar una política de seguridad, analizando los riesgos de exposición del sistema y conozca las medidas de solución existentes.
- ✓ Introducir al lector en las técnicas, herramientas y procedimientos de protección de los equipos y redes de comunicación.

Como resultado de esta investigación y de acuerdo a lo planteado, se deberá estar en la posibilidad de llegar a conclusiones propias acerca de la importancia que se le debe otorgar al tema de la *seguridad de la información computacional* dentro de cada una de las diversas organizaciones, ya sean de carácter educativo o empresarial.

1. TÉRMINOS GENERALES DE SEGURIDAD INFORMÁTICA

1.1 ANTECEDENTES

Desde la aparición del hombre, la información ha tenido gran importancia en cualquier actividad. Sin duda, cuando esta actividad tiene propósitos muy especiales, como el militar o personal, la información crece en importancia y requiere mayor atención en su resguardo. La información, como elemento indispensable en la comunicación, se puede clasificar en varios niveles dependiendo su valor; por ejemplo, existe información confidencial en las actividades militares, en las actividades comerciales importantes, en las transacciones financieras, etc., *una forma de poder dar seguridad a toda esta información es implementar y usar diversos métodos de control de acceso* a ella.

Los incidentes de seguridad en cómputo a nivel mundial aparecieron desde la invención de los primeros sistemas de cómputo. En aquellos años era muy difícil que quien quisiera penetrar dichos sistemas tuviera que ir personalmente y realizarlos desde la consola del sistema, por lo que se reducía el índice de probabilidad de que dicho ataque pudiera venir de personas de afuera o no pertenecientes a las empresas o ambientes académicos

Los sistemas de cómputo son herramientas muy poderosas que actualmente han adquirido una importancia insospechada hace tan sólo unas décadas. Se ha llegado a depender de las computadoras como nunca antes se hizo de ningún otro dispositivo electrónico, pues gran parte de los datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática.

Por consecuencia, la seguridad de las tecnologías de información, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de la sociedad, e incluso para su propia supervivencia. Motivo por el cual se hace de vital necesidad establecer políticas y lineamientos de acceso a estos dispositivos que manipulan y almacenan datos de relevada importancia para la mayoría de las personas actualmente; pues el problema reside casi siempre en nosotros mismos.

Paradójicamente nos hemos convertido en el enemigo más común (y más difícil de vencer) para los sistemas de cómputo actuales, por razones de naturaleza humana: la envidia, la falta de ética, los celos profesionales, la venganza, la avaricia, la inconformidad, etc., son las principales causas de los incidentes de seguridad en cómputo que suceden hoy en día.

Los avances tecnológicos que día a día se van logrando, no se han mantenido distantes del mundo del cómputo, por el contrario han ido a la par y constantemente se van logrando avances significativos que hacen posible tener computadoras más sofisticadas, equipos de cómputo mejores, redes de cómputo más veloces, etc. Hace tan sólo 20 años cuando las computadoras aun no estaban conectadas unas con otras y el Internet era solo un proyecto de unos cuantos, era prácticamente difícil creer en incidentes de seguridad. Llega 1983 y con él, el protocolo de comunicación TCP/IP que trajo consigo una posible comunicación entre sistemas de cómputo, las distancias se acortaron, los sistemas de cómputo cambiaron de ser simples redes de Área Local (LAN) se extendieron a uso Metropolitano (MAN) e incluso de alcance Mundial (WAN); surgió la tendencia Cliente - Servidor, los sistemas de cómputo se unieron y comenzó la integración del mundo gracias a la tecnología y a las redes de computadoras. En ese entonces no se pensaba en individuos que pudieran acceder a sistemas de cómputo remotos y mucho menos pensar que pudieran causar daño desde distancias lejanas. Con el paso del tiempo, cada vez fue más notable lo inseguro que eran los sistemas y que tanto hardware como software contenían fallas de elaboración y de programación respectivamente.

Los primeros incidentes de seguridad llegaron, y con ellos múltiples problemas; pero no había legislación, no existía algún organismo que fuera el responsable de denunciarlos ni que pudiese hacer algo al respecto. En aquellos años a finales de los 80´s la mayoría de los crackers[3] utilizaban técnicas tan triviales como el adivinar el login[4] y de saber el nombre del usuario, tratar de perpetrar el sistema con contraseñas fáciles de adivinar, siendo ésta una tarea trivial y que hoy en día aun la practican.

Posteriormente surgieron grandes incidentes de seguridad a nivel mundial; por ejemplo, el 28 de diciembre de 1998 un grupo de crackers norteamericanos, la "Legion of the Underground", declaró la "ciberguerra" contra Irak y China, amparándose en que en ambos países no se respetan los derechos y libertades fundamentales, llamaron a la destrucción masiva de todas las redes informáticas de estos países. Su primera víctima fue el servidor oficial del gobierno Iraquí, que sucumbió el 7 de enero.

[3] El que rompe la seguridad de un sistema ["The New Hacker's Dictionary", segunda edición, de Eric S. Raymond.].
[4] El login en un sistema, se refiere a la identificación de un determinado usuario, con el mismo.

Sin embargo, el resto de la comunidad de hackers[5] se opone frontalmente a este tipo de medidas. En el manifiesto que estos otros grupos publicaron, declararon "oponerse totalmente a cualquier intento de usar el poder del hacking para amenazar o destruir las infraestructuras de comunicación de cualquier país", por cuanto "las redes de comunicaciones son el sistema nervioso de nuestro planeta". También, a raíz del bombardeo de la embajada china en Belgrado (mayo 1999), los internautas chinos inundaron la Red con consignas en contra de Estados Unidos, entraron en la web de la embajada estadounidense y colapsaron las charlas en directo, condenando las acciones de la Alianza.

Este tipo de situaciones dieron pauta a la creación del máximo organismo de Seguridad en los EU, y en 1988 se creo el CERT (Computer Emergency Response Team), al cual se unieron el FIRST (Forum of Incident and Response Security Teams), y el CIAC (Computer Incident Advisory Capabilities).

También se dio la creación de sucursales de equipos de respuesta a los Incidentes de Seguridad en casi la mayoría de los países que no estaban aislados a los cambios tecnológicos constantes como lo fue en 1995 la creación en nuestro país de la sucursal del CERT, llamado MX-CERT. Se comenzaba a hacer conciencia de que había un problema y que dicho problema ocasionaba perdidas millonarias en empresas tanto privadas como gubernamentales, siendo su principal punta de lanzamiento los ambientes académicos y de ahí perpetrar a las industrias privadas, bancos, institutos de investigación, etc.

Desgraciadamente casi ninguna institución tiene políticas ni procedimientos, nadie sabe qué es permitido, ni qué es prohibido. Es muy alarmante encontrar que salvo las grandes corporaciones, la normatividad relativa a la tecnología de información es prácticamente inexistente; no hay lineamientos establecidos para administrar recursos como el correo electrónico, los mecanismos de seguridad, los niveles de servicio en redes y la atención de problemas.

La cultura de la seguridad informática es entonces un concepto que debe cubrir todos los niveles jerárquicos de la organización, así como todas las funciones que la conforman.

[5] Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible ["The New Hacker's Dictionary", segunda edición, de Eric S. Raymond.].

INTERNET

Internet es hoy en día una palabra reconocida por millones de personas en el mundo y su uso se ha convertido en un componente medular de la vida contemporánea. La gente se informa y se comunica a través de la Internet; conforme aumenta el uso por parte de las empresas y corporaciones, las oportunidades de negocio que se desarrollan son cada vez mayores y más interesantes; se anuncian, y venden sus productos a través de este medio. Sin embargo, el crecimiento de las amenazas de seguridad es igualmente acelerado; en este mundo cada vez más globalizado, con la Internet se mueven millones de datos financieros.

El web está formado por varios componentes:

- Los *servidores*, en los que sitios conectados al Internet pueden exportar datos al mundo;
- Los *clientes*, con los que los usuarios pueden navegar; y
- Los *proxies*[6], que se utilizan para facilitar la comunicación y proporcionar control de accesos para aquellos sitios que dependen de un host[7] intermediario para la comunicación con Internet, como pudieran ser sitios detrás de un firewall[8].

Se comunican decisiones y se efectúan transacciones a ritmos cada vez más acelerados. Un problema importante con los sistemas inalámbricos es que un gran número de usuarios comparte un canal común, lo que genera conflictos con los aspectos de privacidad y seguridad de la información.

La red Internet conecta a millones de computadoras en el mundo, abriendo nuevos canales de comunicación, nuevas oportunidades, nuevos negocios, pero abriendo también la posibilidad de invadir las redes corporativas. Para enfrentar este problema es vital contar con herramientas que den seguridad a toda prueba.

Las conexiones Internet dedicadas, requieren incorporar sistemas que:

- Den seguridad a la red interna de la empresa.
- Autentifiquen el ingreso de usuarios remotos.
- Optimicen el uso de Internet por parte de los usuarios internos, y
- Generen canales encriptados a través de la red para permitir el intercambio de información en forma confiable entre distintos grupos.

[6] Un proxy, es un servidor que centraliza el tráfico entre Internet y una red privada. Contiene mecanismos de seguridad que impiden el acceso no autorizado.
[7] Máquina con sistema operativo tal, que permite que varias computadoras accedan a ella al mismo tiempo. La información puede procesarse en el propio *host* , o bien descargarse a la máquina cliente, para su procesamiento.
[8] Un cortafuegos (*firewall*) está compuesto por hardware y software que protegen las partes de una red. Evitan que medios exteriores accedan a la información, e impiden que una fuente interior pueda sacar datos

["Redes informáticas", Ed. Paraninfo, de Michael J. Palmer].

1.2 CONCEPTOS BÁSICOS

Información y Sistema Informático

Entendemos por *información* el conjunto de datos que sirven para tomar una decisión. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un *componente vital* para el *control*.

Se puede ver el sistema informático como el conjunto de los recursos técnicos, financieros y humanos, cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de una organización.

Aspectos clave en la Seguridad de los Sistemas de Información (SSI)

En primer término, con la gran expansión del uso de computadoras personales se ha magnificado el problema de la SSI, debido sobre todo a la carencia de controles de seguridad básicos en este tipo de sistemas. En segundo lugar, la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones distintas, plantea retos importantes a la gestión de la seguridad.

Los riesgos fundamentales asociados con la incorrecta protección de la información son:

- ⇒ Revelación a personas no autorizadas.
- ⇒ Inexactitud de los datos.
- ⇒ Inaccesibilidad de la información cuando se necesita.

Estos aspectos se relacionan con las tres características que debe cubrir un sistema de información seguro: *confidencialidad*, *integridad* y *disponibilidad*. Así pues, preservar estas tres características de la información constituye el objetivo de la seguridad.

Seguridad Informática

No existe una definición estricta de lo que se entiende por seguridad informática, puesto que ésta abarca múltiples y muy diversas áreas relacionadas con los sistemas de información. Áreas que van desde la protección física de la máquina como componentes hardware de su entorno; hasta la protección de la información que contiene, o de las redes que lo comunican con el exterior.

Tampoco es único el objetivo de la seguridad. Son muy diversos tipos de amenazas contra los que se debe proteger; desde amenazas físicas, como los cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información.

No obstante, como ya se había mencionado anteriormente, sí hay tres aspectos fundamentales que definen la seguridad informática: la confidencialidad, la integridad y la disponibilidad.

Confidencialidad

Es el servicio de seguridad, o condición, que protege la información para que no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

⇒ El uso de técnicas de control de acceso a los sistemas.
⇒ El cifrado de la información confidencial o de las comunicaciones.

Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos.

Integridad

Es el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho, el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.

En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos. Es decir,

- Integridad de los datos: lo enviado es igual a lo recibido.
- Autenticidad de la información: quien lo envía es quien dice ser.

Disponibilidad

Se refiere al grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

1.3 OTROS CONCEPTOS RELACIONADOS

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar en sí mismos.

Autenticidad.

Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

Imposibilidad de rechazo (no-repudio)

Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

Esta característica y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

Consistencia

Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienza a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre. Por ejemplo, si el comando "*ls*" de UNIX comenzara a borrar los archivos listados, en lugar de solo listarlos.

Esta propiedad es amenazada por ejemplo, por el uso de los Caballos de Troya. Programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas.

Aislamiento

Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema que a la información que contiene.

Auditoria

Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han realizado. Una forma de lograr este objetivo es mantener un registro de las actividades del sistema; este registro debe estar altamente protegido contra modificación y ser accedido sólo por el personal indicado para ello.

Algunos ejemplos son, el uso de los denominados archivos de log en UNIX y en otros sistemas, y el uso de sistemas de accounting o contabilidad propia de cada sistema. Al conocer lo que ocurre en el sistema pueden detectarse comportamientos sospechosos.

Prevención

Se relaciona con el concepto de auditoria, pues al conocer los usuarios que se guarda registro de sus actividades, se abstienen de intentar dañar la información. Ello es debido al riesgo que corren de que sus acciones sean detectadas.

1.4 VULNERABILIDAD, AMENAZAS Y CONTRAMEDIDAS

Hay tres conceptos que entran en discusión cuando se habla de la seguridad de un sistema informático: vulnerabilidad o inseguridad (vulnerability), amenazas (threat) y contramedidas (countermesures).

Vulnerabilidad.

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

Amenaza.

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

Contramedida.

Técnicas de protección del sistema contra las amenazas.

La seguridad informática, se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que; *"No existe ningún sistema completamente seguro"*. Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

1.4.1 TIPOS DE VULNERABILIDAD

Algunos de los tipos de vulnerabilidad que se pueden presentar en un sistema son los siguientes:

Vulnerabilidad física.

Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.

Vulnerabilidad natural.

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañarlo; tales como, el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del hardware y del software.

Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, en ciertos sistemas es necesario contar con algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Ciertos fallos o debilidades del software del sistema, hacen más fácil acceder al mismo y lo hacen menos fiable.

Vulnerabilidad de los medios o dispositivos.

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, o cualquier otro medio que contenga la información.

Vulnerabilidad por emanación.

Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios encargados de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las comunicaciones.

La conexión de las computadoras a redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta en gran escala el riesgo a que está sometido, al ser mayor la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar al sistema a través de la red.
- Interceptar información que es transmitida desde o hacia el sistema.

Vulnerabilidad humana.

La gente que administra y utiliza el sistema, representa la mayor vulnerabilidad del mismo. Toda la seguridad del sistema descansa sobre el administrador que tiene acceso al máximo nivel y sin restricciones; y es por lo tanto, quien debe de protegerlo al máximo posible de los ataques de los usuarios tanto internos como externos, ya sean accidentales o intencionales.

Así, los usuarios del sistema también suponen un gran riesgo, ya que son ellos quienes pueden accederlo tanto físicamente como por medio de una conexión remota; la cual como ya se mencionó anteriormente, puede implicar una vulnerabilidad de las comunicaciones. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados, son debido a los usuarios mismos.

Con todo lo anterior, es posible apreciar la diferencia en cada uno de los niveles en los distintos tipos de vulnerabilidad y en las medidas necesarias a adoptar para protegerse de ellos.

1.4.2 TIPOS DE AMENAZAS

Las amenazas al sistema informático, pueden también clasificarse desde varios puntos de vista. En una primera clasificación, según el efecto causado en el sistema, las amenazas pueden englobarse en cuatro grandes tipos:

⇒ Intercepción
⇒ Modificación
⇒ Interrupción, y
⇒ Generación.

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 sí; son ejemplos de este tipo de amenaza:

- Escuchar de una línea de datos.
- Copiar de programas o archivos de datos no autorizados.

Modificación.

Se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino que además, se cambia en todo o en parte su contenido o modo de funcionamiento.

Ejemplos:

- Cambiar el contenido de una base de datos.
- Cambiar líneas de código en un programa.
- Cambiar datos en una transferencia bancaria.

Interrupción.

Interrumpir mediante algún método el funcionamiento del sistema ya sea intencionada o accidentalmente.

Ejemplos:

- Saturar la memoria o el máximo de procesos en el sistema operativo.
- Destruir algún dispositivo hardware.

Generación.

Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema.

Ejemplos:

- Añadir campos y registros en una base de datos.
- Añadir código en un programa (virus).
- Introducir mensajes no autorizados en una línea de datos.

Como se puede ver, la vulnerabilidad de los sistemas informáticos es muy grande, debido a la variedad de los medios de ataque o amenazas. Fundamentalmente los aspectos que se ven amenazados, son: el hardware (los dispositivos físicos del sistema), el software (programas de usuarios, aplicaciones, bases de datos, sistemas operativos, etc.), los datos y la información.

Desde el punto de vista del origen de las amenazas, éstas pueden clasificarse en:

⇒ Naturales
⇒ Involuntarias e
⇒ Intencionadas.

Amenazas naturales o físicas.

Son las que ponen en peligro los componentes físicos del sistema. En ellas podemos distinguir por un lado, los desastres naturales como las inundaciones, rayos o terremotos, y por otro lado, las condiciones medioambientales, tales como la temperatura, humedad, presencia de polvo, etc. Entre este tipo de amenazas, una de las más comunes es la presencia de un usuario ingiriendo alimentos cerca de la computadora.

Amenazas involuntarias.

Están relacionadas con el uso descuidado del equipo por falta de conocimiento o de adiestramiento acerca del tema de la seguridad. Entre las más comunes están:

- Borrar por descuido total o parcialmente la información.
- Dejar sin protección o sin respaldo determinados archivos básicos del sistema.
- Dejar el password o contraseña privada a la vista de todos u olvidar salir de sesión.

Amenazas intencionadas.

Son aquellas procedentes de personas que pretenden acceder al sistema para borrar, modificar o robar la información, para bloquearlo o por simple diversión; los causantes del daño pueden ser de dos tipos: internos y externos. Los atacantes externos pueden penetrar al sistema de múltiples formas; por ejemplo:

- Entrando a las instalaciones o accediendo físicamente a la máquina.
- Entrando al sistema a través de la red explotando las vulnerabilidades del mismo software.
- Consiguiendo acceder a través de personas que tienen autorización para hacerlo.

Los atacantes internos suelen ser alguno de estos tipos de empleados:

- Empleados despedidos o descontentos.
- Empleados coaccionados, y
- Empleados que obtienen beneficios personales.

1.4.3 TIPOS DE MEDIDAS DE SEGURIDAD O CONTRAMEDIDAS

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en la mayoría de las situaciones poco cuantificables y muy variadas. En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema; por ejemplo, la velocidad de las transacciones. Con relación a esto, también se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema; se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan su manejo. Por ejemplo, el uso de una política adecuada de passwords, con cambios periódicos, provoca molestia en los usuarios por el hecho de tener que estar memorizando sus claves constantemente.

Las medidas de seguridad que pueden establecerse en un sistema informático, son de cuatro tipos fundamentales:

⇒ Lógicas
⇒ Físicas
⇒ Administrativas y
⇒ Legales.

Medidas físicas

Se trata fundamentalmente de establecer un perímetro de seguridad en el sistema. Se aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También se le protege de desastres naturales o condiciones medioambientales adversas.

Los tipos de controles que se pueden establecer, incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc.). Por ejemplo, en un cuarto donde hay varias máquinas que trabajan constantemente, es necesario el servicio de aire acondicionado por toda la energía calorífica que se disipa constantemente.
- Prevención de catástrofes (incendios, tormentas, cortes de energía eléctrica, sobrecargas, etc.). Para prevenir los cortes de energía eléctrica, por ejemplo, se usan los llamados no-breaks o incluso el uso de una planta eléctrica alternativa dependiendo de la magnitud de la empresa o el lugar donde se trabaje la información.
- Vigilancia (cámaras, guardias, etc.). Este tipo de control se verá con mayor frecuencia en aquellos lugares en los cuales la información que se maneja es sumamente confidencial, por ejemplo en las instituciones bancarias.
- Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.). Para prevenir las variaciones de energía eléctrica, están por ejemplo, los llamados reguladores de voltaje, cuya utilidad es proteger al equipo de dichas variaciones y evitar así que se dañen sus componentes.
- Sistemas de recuperación (copias de seguridad, sistemas alternativos geográficamente separados y protegidos, etc.). Por ejemplo, en lugares de uso crítico como los bancos o las aerolíneas, es recomendable tener un espejo del sistema como alternativa para que en caso de que el principal falle, el secundario trabaje e impida que se suspenda el servicio que es tan importante. En la mayoría de las instituciones, es vital la realización de respaldos de información para prevenir que en caso de que algún usuario pierda alguna información importante, el administrador del sistema esté en posibilidades de recuperarla.

- Control de la entrada y salida de material. Esta es una medida de precaución que se toma en la gran mayoría de las instituciones para prevenir el hecho de que sea extraída clandestinamente tanto la información como los componentes físicos que la almacenan.

Medidas lógicas

Se refieren más a la protección de la información almacenada. Incluyen las medidas de acceso a la información, y a su uso correcto; así como a la distribución de las responsabilidades entre los usuarios. Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas, y que se pueden denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de los distintos usuarios potenciales del sistema; para ello se debe tomar en cuenta el tipo de usuario de que se trata, porque a cada uno se le aplicará una política de control de acceso diferente y se le imputará distinto grado de responsabilidad sobre el sistema.

Se diferencian cuatro tipos fundamentales de usuarios:

- El administrador del sistema y en su caso, el administrador de la seguridad.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema pero sin necesidad de usarlo.
- Las personas ajenas al sistema.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad, se pueden destacar los siguientes:

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autenticación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la criptografía para proteger los datos y las comunicaciones.
- Uso de cortafuegos para proteger una red local de Internet.
- Definición de una política de copias de seguridad.
- Definición de una política de monitoreo (logging) y auditoria (auditing) del sistema.

Medidas administrativas

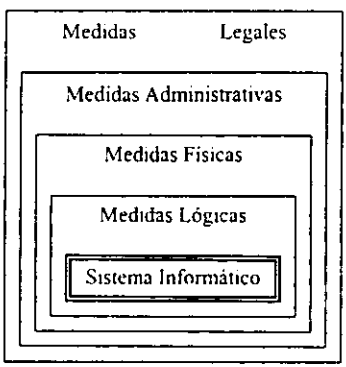
Son aquellas que deben ser tomadas por las personas encargadas de definir las políticas de seguridad para ponerlas en práctica, hacerlas viables y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- Documentación y publicación de las políticas de seguridad y de las medidas tomadas para ejercerlas.
- Debe quedar claro quién fija la política de seguridad y quién la pone en práctica.
- Establecimiento de un plan de formación del personal. Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda , y de esta manera evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.
- Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.
- Deben conocer las políticas y las medidas de seguridad tomadas para colaborar poniéndolas en práctica.
- Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso de éste.

Medidas legales

Se refiere a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo. Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales.

En resumen, las relaciones de estas medidas de seguridad dentro de un sistema informático, pueden observarse en la siguiente figura:



1.5 POLÍTICA DE SEGURIDAD

La política de seguridad es una declaración de intenciones de alto nivel, que cubre la seguridad de los sistemas de información y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada; con lo que los procesos más importantes recibirán más protección.

Para lograr el éxito en la realización e implantación de las políticas, la seguridad debe considerarse como parte de la operativa habitual y no como un extra añadido.

Algunas reglas básicas para establecer una política de seguridad, se mencionan a continuación.

⇒ Toda política de seguridad debe ser holística, es decir, debe cubrir todos los aspectos relacionados con el sistema:

- Debe proteger el sistema en todos los niveles: físico, humano y lógico.
- Debe tener en cuenta no sólo los distintos componentes del sistema, tales como el hardware, software, entorno físico y usuarios, sino también la interacción entre los mismos.
- Debe tener en cuenta el entorno del sistema, esto es, el tipo de compañía o entidad de que se trate (comercial, bancaria, educativa, etc.). De esta consideración surge la segunda regla básica.

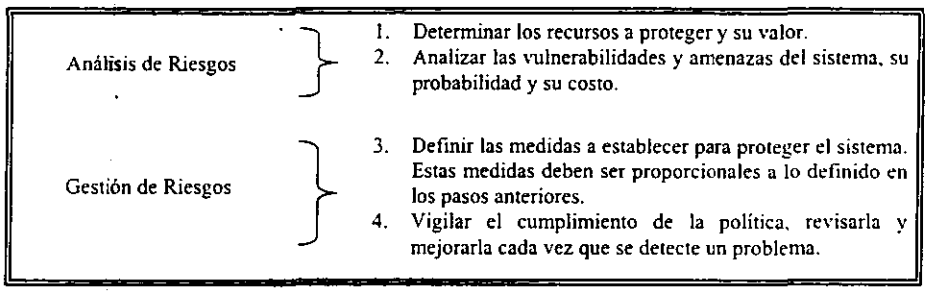
⇒ La política de seguridad debe adecuarse a las necesidades y recursos con que se cuente, al valor que se le da a los recursos y a la información, al uso que se hace del sistema en todos los departamentos:

- Deben evaluarse los riesgos, el valor del sistema protegido y el costo de atacarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.

⇒ Toda política de seguridad debe basarse fundamentalmente en el sentido común, para esto es necesario contar con:

- Conocimiento del sistema a proteger y de su entorno.
- Conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.
- Conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

La siguiente figura, muestra el resumen de los pasos básicos:



Las medidas deben establecerse a todos los niveles: físico, lógico, y humano. Además debe definirse una estrategia a seguir en caso de fallo.

Un ejemplo de política de seguridad en alguna organización, sería:
"Los empleados de cierto nivel pueden leer la información generada por niveles inferiores, pero no por niveles superiores".

1.5.1 TIPOS DE POLÍTICAS

Existen fundamentalmente tres tipos de políticas, cada una de las cuales actúa a distinto nivel y aborda distintos aspectos de la seguridad:

⇒ Políticas administrativas
⇒ Políticas de control de accesos
⇒ Políticas de control de flujo

Políticas administrativas

Este tipo de política se encarga de los procedimientos administrativos relacionados con la seguridad, no de los aspectos técnicos y de ejecución de ésta. Entre los puntos a ser tratados por las políticas administrativas se pueden destacar los siguientes:

- Análisis y gestión de riesgos.
- Política de actuación en caso de desastre.
- Monitoreo y audición del sistema y de los empleados.
- Capacitación y formación de los usuarios.
- Política de copias de seguridad.

Acceso discrecional y acceso obligatorio

A la hora de hablar del acceso a los datos existen dos tipos de políticas y modelos fundamentales:

⇒ Control de accesos discrecional (Discretionary Access Control - DAC)
⇒ Control de accesos obligatorio (Mandatory Access Control - MAC)

En el control de accesos discrecional, el propietario del objeto, de forma voluntaria, concede o deniega el acceso a éste a otros sujetos. En el control de accesos obligatorio, es el sistema el que establece una compartición obligatoria tanto de los objetos como de los sujetos; a partir de ésta se establecen reglas o políticas de acceso; por ejemplo, se podrían establecer niveles de confidencialidad en distintos grupos de objetos y sujetos, y permitir que un sujeto sólo accediera a un objeto con igual o menor nivel de confidencialidad que el suyo.

Cabe mencionar que ambos tipos de políticas, discrecional y obligatoria, no son excluyentes. Puede ocurrir, por ejemplo, que la política global de una empresa sea de acceso obligatorio pero que determinados departamentos establezcan una política interna discrecional. Así, los usuarios de determinados departamentos pueden fijar sus niveles de protección con respecto a sus compañeros de otras áreas, pero a la hora de compartir la información con el resto de usuarios de otros departamentos deben seguir la política de compartición fijada por la dirección.

Políticas de control de accesos

Las políticas de control de acceso a la información, establecen bajo qué condiciones cada sujeto puede acceder a cada objeto. Se entenderá en este caso por *sujeto* cualquier usuario, programa, computadora remota u otro dispositivo que pueda tener acceso al sistema. Se entenderá por *acceso* cualquier acción aplicada sobre los objetos, tal como leer, escribir, modificar o ejecutar. Finalmente, se entenderá por *objeto* cualquier archivo, directorio, proceso en memoria, dispositivo, etc. del sistema

Existen distintos criterios de clasificación de las políticas de control de accesos:

- ⇒ Política de menor privilegio o de necesidad de saber. Es la que establece que los sujetos sólo pueden acceder a aquellos objetos que necesitan para realizar su trabajo.
- ⇒ Política de compartición. La política de compartición o de máximo privilegio es lo contrario de la anterior. En ella todos los sujetos pueden acceder por defecto a todo el sistema.
- ⇒ Granularidad. Se define la granularidad como el tamaño mínimo de los objetos accesibles, y por tanto susceptibles de ser protegidos. Puede ser una granularidad muy fina, al nivel de direcciones individuales; o muy gruesa, al nivel de segmento de memoria o de dispositivo.
- ⇒ Políticas cerradas. Las políticas cerradas prohíben por defecto cualquier acceso. Para que un acceso sea posible debe estar explícitamente permitido. Este tipo de políticas es más seguro, ya que permite examinar cada objeto del sistema y definir si es accesible o no, cómo es accesible y para quién. En este punto es posible aplicar por ejemplo, una política de menor privilegio a la hora de definir los accesos. Obviamente, este tipo de políticas es más costoso, ya que requieren del administrador de la seguridad una comprobación completa de todos los aspectos del sistema y un conocimiento de sus características de seguridad.
- ⇒ Políticas abiertas. Las políticas abiertas permiten por defecto cualquier acceso. Para que no se pueda acceder a un objeto debe prohibirse explícitamente. Este tipo de políticas es más inseguro, ya que descuida el análisis de la seguridad de todo el sistema y tan solo se preocupa de determinados objetos. Por defecto, se presupone que todos los objetos son seguros, y tan solo se establecen medidas en algunos casos. Obviamente este tipo de políticas es menos costoso para el administrador de la seguridad.

Políticas de control de flujo.

Las políticas de control de flujo tratan sobre la difusión de la información una vez accedida, estableciendo cuales son los canales legítimos para su difusión. Al hablar de canales, no se hace referencia siempre a canales físicos de transmisión de información, sino a sistemas de transferencia, a las distintas formas en las que la información puede fluir de un sujeto origen a un sujeto destino.

Una de las primeras elecciones de toda política de control de flujo es la prioridad que se le da a los tres aspectos de la seguridad: confidencialidad, integridad y disponibilidad. El orden en que se tienen en cuenta estos tres aspectos depende del tipo de organización de la que se trate; por ejemplo, en el sector de la defensa, el orden establecido es el siguiente:

⇒ Confidencialidad.
⇒ Disponibilidad, e
⇒ Integridad.

Pues es más importante mantener el secreto de los datos incluso que tener acceso a los mismos o evitar su pérdida. En otros sectores gubernamentales distintos del de defensa, el orden de importancia es:

⇒ Integridad.
⇒ Confidencialidad y
⇒ Disponibilidad.

Supóngase por ejemplo, que se trate de los datos fiscales de los ciudadanos en hacienda, en primer lugar se trata de evitar la pérdida o modificación de los datos, por encima de la posibilidad de que éstos sean revelados, y en último lugar se tiene en cuenta la posibilidad de que los datos no estén disponibles en un momento dado. En los sectores privados, tanto el comercial como el bancario, el orden de prioridad de los factores es:

⇒ Integridad.
⇒ Disponibilidad, y
⇒ Confidencialidad.

Por ejemplo, en un banco en los datos de las cuentas de los clientes, el primer elemento a considerar es que sean correctos, esto es, que no puedan ser modificados, en segundo lugar es necesario poder acceder a ellos en todo momento, y en último lugar, aunque no por ello se le reste importancia, es necesario mantener el secreto de los mismos. En principio no es tan importante que alguien conozca los datos de la cuenta de otra persona, como que sea capaz de modificarlos y engañar al banco.

Planes de contingencia

Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación. La mayor parte de las medidas que se han tratado hasta este momento se refieren a la prevención ante posibles amenazas. Sin embargo, y como ya se ha mencionado, ningún sistema es completamente seguro, y por tanto hay que definir una estrategia a seguir en caso de fallo o desastre. De hecho los expertos de seguridad afirman sutilmente que hay que definir un plan de contingencia para cuando falle el sistema, no por si falla el sistema.

La clave de una buena recuperación en caso de fallo es una preparación adecuada. Por recuperación se entiende tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo de los recursos y de la información.

Adicionalmente existen otros aspectos relacionados con la recuperación como son la detección del fallo, la identificación del origen del ataque y de los daños causados al sistema y las medidas a tomar posteriormente contra el atacante. Todo ello se basa en buena medida en el uso de una adecuada política de monitoreo y auditoria del sistema.

La recuperación de la información se basa principalmente en el uso de una política de copias de seguridad adecuada; mientras que, la recuperación del funcionamiento del sistema se basa en la preparación de recursos alternativos.

Una buena política de copias de seguridad debe contemplar los siguientes aspectos:

- Qué tipos de respaldos se realizan: completos o incrementales.
- Con qué frecuencia se realiza cada tipo de respaldo.
- Registrar en una bitácora los respaldos realizados.
- Cuántas copias se realizan y dónde se guardan.
- Durante cuánto tiempo se guardan las copias.

Dependiendo del tipo de empresa o dependencia de que se trate, puede ser necesario recuperar el funcionamiento en un plazo más o menos breve. A un banco por ejemplo, le interesa volver a funcionar en unas pocas horas, mientras otros tipos de empresas pueden esperar un plazo mayor. Todo depende del uso que se haga del sistema y de las pérdidas que suponga no tenerlo en funcionamiento.

Las compañías pueden mantener o contratar dos tipos de instalaciones alternativas: frías (cold site) o calientes (hot site). Una instalación fría consiste en un lugar con las medidas de seguridad física disponibles donde se pueda instalar el hardware y el software y funcionar en menos de una semana. Una instalación caliente incluye además computadoras, periféricos, líneas de comunicaciones y otros medios e incluso personal para volver a funcionar en unas pocas horas.

1.6 PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA

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. Algunos de los fundamentales, son:

Principio de menor privilegio

Este es quizás el principio más fundamental de la seguridad, y no solamente de la informática. Básicamente, el principio de menor privilegio afirma que cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener tan sólo los privilegios de uso necesarios para desarrollar su tarea y ninguno más.

Esto quiere decir que cualquier usuario solamente debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

Al diseñar cualquier política de seguridad es necesario estudiar las funciones de cada usuario, programa, etc., definir los recursos a los que necesita acceder para llevarlas a cabo, identificar las acciones que necesita realizar con estos recursos, y establecer las medidas necesarias para que tan solo puedan llevar a cabo estas acciones.

Por ejemplo, en un sistema UNIX el usuario necesita acceder al archivo /etc/passwd, donde normalmente se guarda su password, para poder entrar al sistema. Sin embargo, durante el resto de su trabajo en el sistema no necesita acceder a los passwords. Siguiendo el principio de menor privilegio, se evita este acceso, pues los passwords cifrados están situados en otro archivo, el cual no tiene otorgados los permisos de lectura.

La seguridad no se obtiene a través de la oscuridad

El hecho de mantener posibles errores o vulnerabilidades en secreto, no evita que existan, en cambio si evita que se corrijan. No es una buena medida basar la seguridad en el hecho de que un posible atacante no conozca las vulnerabilidades del sistema.

No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad; educar a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas, suele ser mejor método para protegerlo.

No obstante tampoco se trata de hacer público un nuevo fallo del sistema o un método para romperlo. En primer lugar hay que intentar resolverlo, obtener un medio para eliminar la vulnerabilidad y luego publicar el método de protección.

Principio del eslabón más débil

En todo sistema de seguridad, el máximo grado de seguridad es aquel que tiene su eslabón más débil. Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Al diseñar una política de seguridad o establecer los mecanismos necesarios para ponerla en práctica, se deben contemplar todas las vulnerabilidades y amenazas. No basta con establecer unos mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

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 en el sistema se utiliza la red ethernet para conectar las máquinas, y no se protege la conexión, no servirá de nada la política de passwords establecidas, (por defecto, por ethernet 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 sistema el punto débil sería la red, por mucho que se haya reforzado la seguridad en otros puntos, el sistema sigue siendo altamente vulnerable.

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 sólo 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 cualquiera 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.

A lo largo del desarrollo del primer capítulo de este trabajo, se ha podido apreciar cómo es que han ido evolucionando y agravándose los ataques informáticos; y que incluso, algunos de sus orígenes obedecieron a problemas políticos. Ahora se tiene un punto de vista un tanto más completo de la importancia que tiene la información, y que en muy diversas actividades, en su gran mayoría, tiene un valor especial. Como consecuencia de este hecho, se aprecia también más claramente lo relevante que es el tema de la *seguridad en la información*, y el aspecto de conocer diferentes métodos que controlen el acceso a la misma.

Así, se conocen ya los elementos básicos que forman parte de un sistema informático, es importante ahora aprender a integrarlos correctamente para el óptimo funcionamiento y resguardo del propio sistema.

Es posible concluir entonces, que la finalidad de la seguridad en la información es preservar la confidencialidad, la integridad y la disponibilidad de la misma, y que para que esto tenga buenas bases, es necesario adquirir el concepto de seguridad informática como una cultura que debe cubrir TODOS los niveles de una determinada organización, y que generar en los usuarios buenos hábitos de seguridad con su información confidencial, como es el cambio periódico de contraseñas, por ejemplo; hará que en su conjunción se logre el mejor nivel de seguridad posible en la información general de dicha organización. Es decir, que si se logra un verdadero trabajo de equipo, seguramente la situación de la seguridad, verá resultados muy positivos.

En el capítulo 2 se verán diferentes formas de autenticación de los usuarios con el sistema operativo, diversos métodos de protección a la memoria de las computadoras; así como algunos modelos y mecanismos de seguridad. Se explicarán las características de las formas de protección de memoria y los criterios de evaluación para los sistemas operativos.

2. SEGURIDAD EN SISTEMAS OPERATIVOS

En el capítulo 1, se ha iniciado al lector en el tema de la seguridad y protección a la información que se almacena y procesa en los equipos de cómputo. Se han aprendido los conceptos más primordiales al respecto; entre los que destacan: información, sistema informático, seguridad informática, confidencialidad, integridad y disponibilidad. También se han explorado los tipos de vulnerabilidades que con mayor probabilidad pueden afectar al sistema que sea de particular interés, se contemplaron las reglas o políticas de seguridad que pueden ser implantadas para iniciar los controles y contramedidas pertinentes; además de tomar en cuenta las posibles amenazas que pudieran presentarse dentro del mismo personal que maneja el sistema.

En este capítulo se verán los métodos de protección de memoria, con el objetivo de resaltar la importancia que tienen en el resguardo de los sistemas operativos. Pues como se ha empezado a ver, hay carencia de controles de seguridad básicos en las computadoras personales; y esto es también debido a la falta de protección del mismo sistema operativo. Es muy conveniente también saber cómo es que está trabajando el sistema operativo que se esté usando para poder decidir de qué manera es posible protegerlo.

Actualmente, la información normalmente se almacena en equipos de cómputo; y el sistema operativo, es la parte fundamental de todo sistema de cómputo; pues son los encargados de la interacción entre el usuario de la máquina y los recursos e informaciones almacenados, es claro entonces que son un punto importante tanto para la administración de los recursos, como de la propia información. Y, por lo tanto, también constituyen la primera línea de protección y seguridad lógica.

Hasta hace poco los sistemas operativos se habían venido construyendo basándose en criterios de eficacia, economía, facilidad de manejo, etc. Sin embargo; no hace mucho, que se ha hecho necesario prestar una mayor atención a la seguridad de los mismos a la hora de abordar su diseño.

El principal problema en la construcción de un sistema informático seguro, es el diseño, desarrollo e implementación de sistemas operativos que satisfagan estrictas políticas de seguridad. Este aspecto es más visible en el caso de las computadoras aisladas de la red. No obstante, aunque se trate de una computadora conectada con otras a través de Internet, además de mecanismos específicos de protección como los firewalls, la existencia de un sistema operativo seguro es una medida fundamental a la hora de proteger al sistema de cualquier tipo de ataque desde el exterior.

Algunos de los aspectos que deben ser contemplados por un sistema operativo seguro son:

- ⇒ La identificación y autenticación de los usuarios.
- ⇒ El control de acceso a los recursos e informaciones almacenados.
- ⇒ El monitoreo y contabilidad de todas las acciones realizadas por usuarios o por procesos invocados por ellos, sobretodo aquellas que puedan constituir un riesgo para la seguridad.
- ⇒ La auditoria de los acontecimientos que puedan representar amenazas a la seguridad.
- ⇒ La garantía de la integridad de los datos almacenados.
- ⇒ El mantenimiento de la disponibilidad de los recursos y la información.

Todos estos aspectos han sido estudiados con interés creciente en las últimas dos décadas, creándose modelos teóricos de gran importancia que recientemente han empezado a implementarse en sistemas operativos comerciales.

2.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

Normalmente para acceder a un equipo con sistema operativo multiusuario, éste procede a identificar y autentificar al usuario, con el fin de comprobar si se trata de alguien autorizado para ocupar los recursos del sistema o no. Sin embargo, si se quiere proteger la información almacenada en una máquina personal; aún teniendo un único usuario, es conveniente establecer algún mecanismo de identificación y autenticación.

En un entorno en el que cada vez son más las computadoras conectadas en red, la identificación y autenticación debe producirse tanto con personas como con otras máquinas que intenten establecer una conexión.

Etapa de identificación

En todos los sistemas multiusuario, cada usuario posee un identificador (ID) que define quién es y que lo identifica unívocamente en el sistema diferenciándolo del resto. Usualmente este identificador es un código o nombre de usuario, apellido, iniciales+apellido, nombre+número o cualquier cadena alfanumérica designada por el administrador del sistema.

La etapa de identificación consiste en proporcionar al sistema el identificador del usuario.

Etapa de autenticación

Una vez identificado al usuario, es necesario que éste demuestre de algún modo que es quien dice ser. Con este propósito existen tres métodos fundamentales:

1. Algo que sólo el usuario sabe.
2. Algo que sólo el usuario tiene.
3. Algo que el usuario es.

Algo que sólo el usuario sabe.

Este es el método más común de autenticación, y consiste en asociar al identificador de usuario una palabra de paso, contraseña o password.

La autenticación se basa en que sólo el usuario identificado conoce la contraseña asociada. Por lo tanto, esta palabra demuestra que el usuario es quién dice que ser.

Obviamente la validez de este método descansa sobre el hecho de que el usuario no confíe su contraseña a ningún otro, o que ésta no sea descubierta mediante algún medio. De ahí la importancia de establecer un buen sistema de contraseñas y de protección de las mismas.

Por ejemplo el sistema operativo UNIX, utiliza por defecto este mecanismo de contraseña para autentificar a los usuarios. La unión del identificador de usuario más su contraseña o password definen cada cuenta.

La contraseña no es el único tipo de conocimiento que puede usarse para autentificar a un usuario, aunque si es el más usual. También es posible basarse en datos culturales, aficiones, frases contraseña, etc., pero no son métodos comúnmente usados.

Algo que sólo el usuario tiene.

Este método también se denomina *autenticación hardware*. En este caso el usuario posee algún objeto que demuestra su identidad. De nuevo la utilidad de este sistema se basa, en que solo el usuario con un determinado identificador puede tener el objeto, es decir, que no se lo ha prestado a nadie o que no ha sido robado.

El objeto utilizado para autentificar puede ser una llave, una placa, una tarjeta inteligente o cualquier otro dispositivo hardware que permita acceder al sistema.

Este método de autenticación no es necesario que sea utilizado frente a la computadora, sino que puede utilizarse, por ejemplo al entrar en el cuarto donde se encuentra el equipo. De hecho este sistema suele combinarse con cualquiera de los otros dos para proporcionar un mayor grado de seguridad.

Algo que el usuario es.

Este método se basa en autentificar al usuario mediante alguna característica física que lo identifica unívocamente. Estas características suelen denominarse *bioantropométricas* o *biométricas*, y son propias de cada individuo y por tanto lo diferencian del resto de los usuarios. Entre las características biométricas más usuales se encuentran las huellas dactilares, las imágenes de la palma de la mano, patrones de voz, patrones retinales, etc.

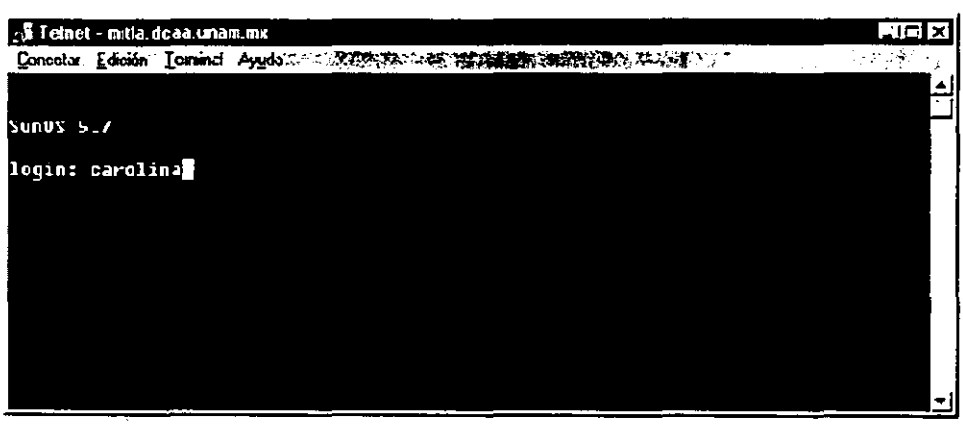
Algunas de estas características se basan más en aptitudes o hábitos del usuario, tales como los patrones dinámicos de la firma (tiempo, aceleraciones, inclinaciones), los estilos de pulsación en el teclado o los rasgos de uso del ratón.

Modelo de contraseña simple

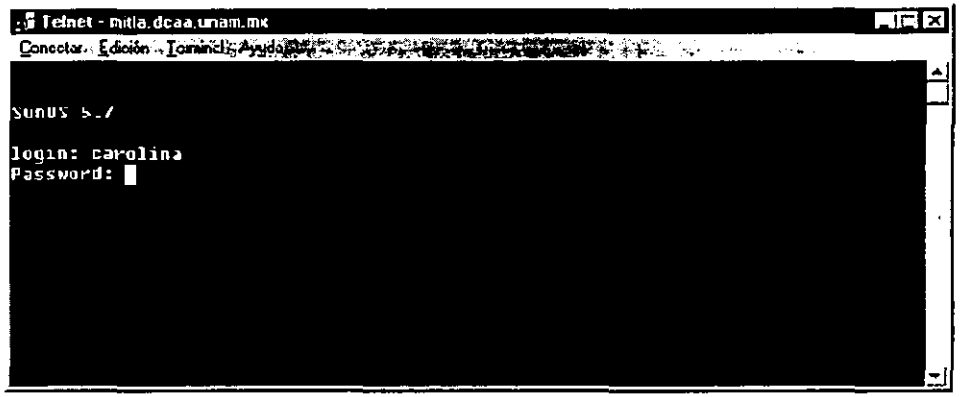
Este método de autenticación es el más usual y se basa en asociar una contraseña única en forma de una palabra con o sin sentido a cada identificador de usuario.

El proceso utilizado en el sistema operativo UNIX para aplicar este modelo es el siguiente:

- En primer lugar se pide el identificador o nombre del usuario.



- Una vez que se introdujo dicho identificador, y sin realizar ningún tipo de comprobación aún, se le solicita al usuario que introduzca su contraseña secreta. Cabe señalar que el password por ser confidencial NO aparece en pantalla al ser tecleado.



- Tras introducir la contraseña, el sistema comprueba la validez de la identidad total del usuario, es decir, tanto login como password; si la contraseña corresponde con el nombre del usuario, se permite el acceso. Si por el contrario alguno de los pasos fue erróneo, se permite al usuario reintentar su identificación un número limitado de veces.

- Si después de estos reintentos el usuario no ha conseguido introducir su identificación correctamente, el sistema, por seguridad da por finalizada la sesión, y almacena un registro de lo ocurrido en un archivo debidamente protegido para que éste sea revisado únicamente por el administrador del sistema.

Debido a la importancia de mantener en secreto las contraseñas, el sistema no las almacena directamente en algún lugar visible para todos los usuarios, sino que mantiene una copia cifrada de las mismas dentro de un archivo destinado para ello, y que está resguardado por el sistema.

Elección y gestión de contraseñas

Las contraseñas son la primera y principal línea de defensa contra los intrusos. Para proteger al sistema y a los datos que contiene es necesario elegir una contraseña adecuada y protegerla cuidadosamente. Para la selección de contraseñas existen diversos métodos que, fundamentalmente son:

- Es el mismo usuario quien la escoge.
- Es generada aleatoriamente por la máquina.
- Es asignada por el administrador del sistema.
- Elegida por el usuario y comprobada por el administrador del sistema o por algún software específico para hacerla encajar dentro de las restricciones mínimas.

Para elegir la clave de la mejor manera posible es bueno recordar el denominado dilema de la contraseña: *"Cuanto más fácil de recordar es una contraseña, más fácil es de adivinar, mientras que cuanto más difícil es de descubrir, más difícil es de recordar"*.

Cuando es el usuario quien elige su clave, el problema consiste en que normalmente no la selecciona aleatoriamente, más aún, existen algunas elecciones típicas, como:

- No seleccionar alguna contraseña.
- Elegir como contraseña el nombre de usuario, los apellidos, alguna fecha significativa o una variación mínima de éstos.

Menos peligroso, aunque no exento de riesgo es elegir:

- Palabras comunes y con sentido.
- Nombres de personas conocidas o personajes de ficción.
- Nombres de lugares, etc.

Debido a esta debilidad en las contraseñas elegidas por muchos usuarios, existe un método muy extendido para atacarlas denominado *"ataque mediante diccionario"*; con este sistema se consigue una copia del archivo en el que se almacenan los passwords cifrados, a partir de ella se cifran una serie de palabras que son passwords probables. Por ejemplo, se usan los criterios de selección definidos anteriormente y además se cifran todas las palabras contenidas en uno o varios diccionarios. Las palabras cifradas se comparan con los passwords del archivo, si alguna de ellas coincide, entonces el atacante descubre una de las contraseñas del sistema y está en posibilidades de acceder a él. De esta manera es fácil observar la enorme debilidad del sistema de contraseña simple sin ninguna medida adicional de selección y administración de éstas.

Es por todo esto que se han ido sugiriendo métodos alternativos de autenticación que conjuguen la facilidad de recordar con la dificultad de adivinar. Dentro del modelo de contraseña simple es posible destacar los siguientes tipos:

⇒ **Contraseña variable**
El usuario posee una contraseña de gran longitud de la que el sistema sólo comprueba algunos caracteres, situados en posiciones que, aleatoriamente, elige en cada intento de acceso.

⇒ **Lista de contraseñas**
El usuario posee varias contraseñas que va usando consecutivamente. Las distintas contraseñas suelen ser generadas por el sistema y guardadas por el usuario en una lista.

Con este sistema si alguien logra adivinar la siguiente contraseña y entrar al sistema, ésta tan solo le servirá en una ocasión; además el usuario podrá saber que se ha producido una "invasión" a su cuenta al comprobar que no puede entrar con la contraseña que le corresponde.

⇒ **Frase - contraseña**
La contraseña es una frase larga fácil de recordar por el usuario, pero difícil de adivinar debido a su longitud.

Algunos aspectos para elegir una buena contraseña

- Elegir contraseñas que no sean palabras (aunque sean extranjeras), o nombres (especialmente el del usuario, personajes de ficción, miembros de su familia, una mascota, la marca del coche, el lugar de nacimiento, etc.).
- Elegir una contraseña que mezcle caracteres alfabéticos y numéricos. No usar nunca contraseñas completamente numéricas con algún significado (teléfono, fecha de nacimiento, etc.).
- Elegir contraseñas largas, de más de 8 caracteres.
- Elegir contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

Las mejores contraseñas contienen tanto letras mayúsculas como minúsculas, y tanto letras como números. Deben ser fáciles de recordar para no escribirlas.

Algunas normas para proteger las contraseñas

La protección de la contraseña recae tanto en el administrador del sistema como en el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema; por lo tanto, algunos consejos a seguir, son:

- No permitir ninguna cuenta sin contraseña. El administrador del sistema debe repasar este hecho periódicamente.
- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de root, system, test, demo, guest, etc.
- No dejar nunca a nadie la contraseña. Si se hace, cambiarla inmediatamente.
- No escribir la contraseña en ningún sitio, en especial cerca de la máquina. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
- No teclear la contraseña si hay alguien observando.
- No enviar la contraseña por correo electrónico, y en todo caso no escribir la palabra "password" en el correo.
- No mantener la contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente.

Muchos sistemas incorporan algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

- Número de intentos limitado. Tras un número de intentos fallidos (3 a 5), pueden tomarse distintas medidas:
  - ⇒ Obligar a reescribir el nombre de usuario o el password (lo más común).
  - ⇒ Bloquear el acceso durante un tiempo.
  - ⇒ Enviar un mensaje al superusuario o mantener un registro especial.
- Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres.
- Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números y no pueden contener el nombre del usuario.
- Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir la anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.
- Ataque preventivo. Muchos administradores utilizan ciertos programas (crackers) para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

Contraseñas de un solo uso

Las contraseñas de un solo uso (*one-time passwords*) son uno de los mecanismos de autenticación más seguros, debido a que su descubrimiento tan solo permite acceder al sistema una vez. Además, en muchas ocasiones se suelen utilizar dispositivos hardware para su generación, lo que las hace mucho más difíciles de descubrir.

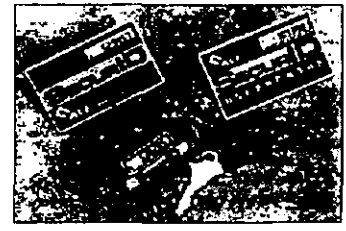
Básicamente se distinguen tres tipos de contraseñas de un solo uso:

- Las que requieren algún dispositivo hardware para su generación, tales como calculadoras especiales o tarjetas inteligentes.
- Las que requieren algún tipo de software de cifrado especial.
- Las que se basan en una lista de contraseñas sobre papel.

El mecanismo basado en el uso de tarjetas es uno de los que están siendo más usados actualmente, y consiste en que el usuario posee una tarjeta o pequeña calculadora que funciona como generador de contraseñas. Esta tarjeta contiene una serie de funciones preprogramadas y un número de serie único grabado en memoria. El usuario combina una palabra clave con la tarjeta para obtener el password de un solo uso, lo que le protege en caso de robo o pérdida.

El modo de funcionamiento de este sistema, es como sigue; la tarjeta genera periódicamente valores mediante una función secreta basada en el tiempo y en el número de identificación de la misma. El usuario combina el número generado por la tarjeta con su palabra de paso para obtener el password de entrada.

Un ejemplo práctico de este tipo de mecanismo son las tarjetas SecurID de Security Dynamics.



Otro método que hace uso de tarjetas, aplica un sistema denominado de pregunta-respuesta. Al introducir el nombre de usuario en la máquina, ésta muestra un valor. El usuario introduce este valor en la tarjeta junto con su número de identificación (PIN: Personal Identification Number). La tarjeta genera un valor que constituye el password de un solo uso para entrar en el sistema.

La tarjeta es usada con una máquina remota como parte de un sistema pregunta-respuesta.

Contraseñas cognoscitivas

Se basan en conocimientos o respuestas del usuario a una serie de preguntas.

Al generarse una cuenta se realiza una encuesta inicial al usuario donde se le proponen una serie de preguntas típicas. Las distintas relaciones pregunta - respuesta se almacenan para cada usuario. Cuando el usuario quiere acceder a la cuenta se le repiten algunas de las preguntas y si las respuestas son coincidentes con las originales se le permite el acceso.

Si las preguntas están bien elegidas, las respuestas serán fáciles de recordar por el usuario y lo caracterizarán unívocamente.

Cifrado de contraseñas

Para poder comparar las contraseñas introducidas por el usuario con las originales, el sistema debe guardar una copia de las mismas. Obviamente no es conveniente guardar la copia sin ningún tipo de protección. Así pues, en UNIX se guarda una copia cifrada de las contraseñas en el sistema dentro del archivo */etc/shadow*. Cuando un usuario entra al sistema, el programa */bin/login* cifra la contraseña introducida y la compara con la almacenada. Si coincide, deja entrar al usuario.

Con el fin de dificultar el uso de un ataque mediante diccionario, los creadores del UNIX introdujeron un condimento adicional (salt) en el proceso de cifrado de contraseña. A la hora de realizar el cifrado se utiliza tanto la contraseña como un código adicional de 12 bits. De este modo se evita que una misma contraseña siempre resulte en un mismo código cifrado, y se hace que cada contraseña elegida pueda dar lugar a 4096 cifrados distintos.

2.2 PROTECCIÓN DE MEMORIA

Otra forma de protección ofrecida por el sistema operativo es la protección de memoria. Se trata de que los distintos procesos en ejecución no interfieran en la memoria utilizada por otros. En particular la memoria ocupada por el sistema operativo debe ser protegida para garantizar la salvaguarda de los datos e instrucciones que contiene.

La protección de memoria está estrechamente relacionada con el direccionamiento, es decir, con la forma en que el sistema operativo genera las direcciones de memoria de los distintos procesos.

Existen diversos mecanismos de protección de memoria:

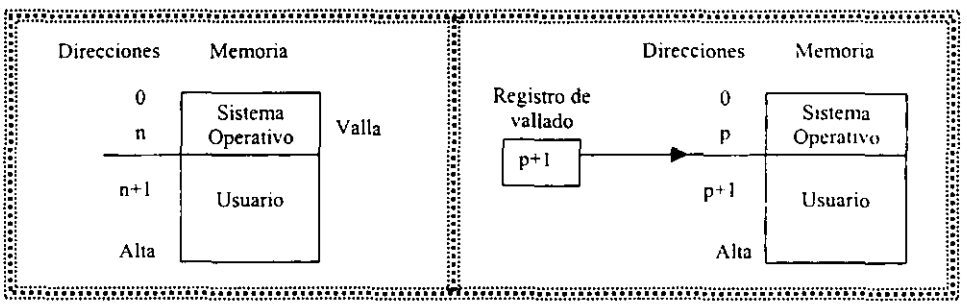
⇒ Vallado
⇒ Registros de reubicación
⇒ Arquitectura etiquetada
⇒ Segmentación
⇒ Paginación

Vallado

Este sistema se utiliza en sistemas monousuario, para evitar que los procesos del usuario puedan afectar a la porción residente del sistema operativo. Para ello se divide la memoria en una zona de usuario y una de sistema mediante el establecimiento de una valla de división. Esta valla es en realidad una dirección, que puede ser fija o que se guarda en el denominado registro de vallado, y que señala el límite superior de la zona de memoria ocupada por el sistema operativo.

Cada vez que algún proceso del usuario genera una dirección, ésta se compara con el contenido del registro de vallado. Si la dirección se encuentra dentro de la zona del sistema, se considera una dirección inválida y se impide que el programa acceda a ella.

El esquema de protección de vallado, se encuentra representado en la siguiente figura:



Las funciones básicas para el manejador de la memoria para este método de asignación, son:

- *Guardar información*, lo cual es una tarea sencilla. Pues se reduce a saber si la zona asignada para el usuario está ocupada o disponible.
- *Decidir a quién asignar el recurso*, esto es también muy fácil, ya que hay un solo usuario que ocupa todo el espacio disponible.
- *Asignar y retirar el recurso;* estas son de igual manera tareas elementales.

En resumen, la gran ventaja de este método es, entonces, la simplicidad.

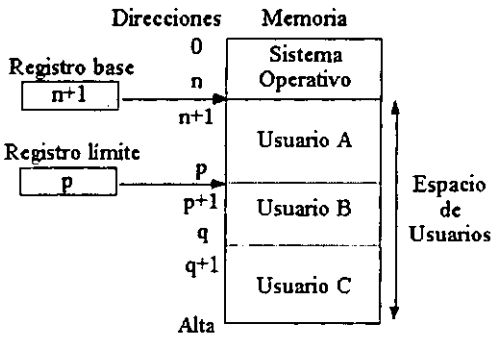
Como desventaja, es posible observar que, este método tan solo protege al sistema operativo de los procesos del usuario, y no protege a los procesos del usuario entre sí; con este fin pueden utilizarse los registros de reubicación.

Registros de reubicación

Este sistema puede utilizarse en entornos multiproceso y multiusuario. Utilizando este mecanismo la memoria se divide en distintas zonas asociadas a los distintos procesos en ejecución. Se utilizan una serie de registros de reubicación protegidos en los que tan solo puede escribirse en modo privilegiado.

Un par de registros por proceso guardan la dirección base y la dirección límite que ocupa en memoria, de modo que las direcciones generadas por cada proceso deben encontrarse siempre entre ambos límites. La ventaja de este mecanismo es que impide que los distintos procesos de usuario interfieran entre sí.

La siguiente figura ejemplifica la organización que tendrían los procesos de tres usuarios diferentes y el sistema operativo, en una máquina determinada, usando el sistema de registros de reubicación:



Ventajas:

- El contenido del registro de reubicación, se suma automáticamente a toda dirección utilizada para referenciar la memoria.
- Incluso puede establecerse una versión de este sistema en la que se separen las zonas de datos de las de instrucciones para cada proceso. De este modo se impide que se puedan sobrescribir las instrucciones de un proceso en memoria.

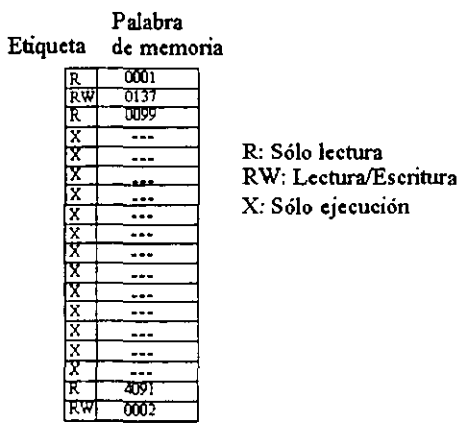
Finalmente, este esquema presenta dos inconvenientes. El primero, se refiere al costo de reubicación, al terminarse una tarea, el sistema debe reubicar a todas las demás para compactarlas. El segundo, es la fragmentación o desaprovechamiento de la memoria.

Arquitectura etiquetada

Este mecanismo puede implementarse por software o por hardware:

Por hardware, se utilizan una serie de bits adicionales (extra-bits) asociados a cada palabra de memoria. Estos bits contienen una etiqueta (tag) indicando el tipo de operaciones permitidas sobre la palabra, por ejemplo, si es de solo lectura, de lectura/escritura o de solo ejecución (contiene instrucciones).

En la siguiente figura, se observa un ejemplo de una cierta cantidad de palabras de memoria, con sus correspondientes etiquetas; así como el significado de cada etiqueta.



Por software se reserva una zona especial de memoria altamente protegida donde se guardan las etiquetas asociadas a cada palabra de memoria.

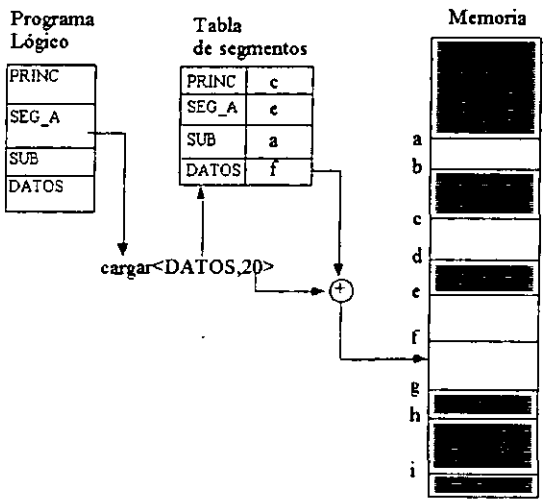
Segmentación

Tanto la segmentación como la paginación son mecanismos destinados fundamentalmente a la gestión de memoria, a su asignación y reserva. No obstante permiten adicionalmente establecer algunas medidas de seguridad.

La segmentación puede considerarse un mecanismo de registros de reubicación llevado al límite. El código de cada programa se divide en segmentos separados. Cada segmento contiene un código relacionado (procedimientos, datos de un vector, etc.). A cada segmento se le asigna un nombre único; y una instrucción o un dato en el segmento se direcciona mediante el par *<nombre, desplazamiento>*.

El sistema operativo mantiene una tabla de segmentos, con sus nombres y direcciones de memoria. Cuando un programa genera una dirección virtual de la forma *<nombre, desplazamiento>* se obtiene la dirección absoluta consultando la tabla de segmentos. De hecho, se puede mantener una tabla de direcciones de segmentos por cada programa en ejecución, de modo que varios procesos en ejecución pueden compartir segmentos, como es el caso de las librerías.

La siguiente figura, representa un ejemplo del funcionamiento del método de segmentación.



Cada segmento posee un nombre simbólico; para la localización de una dirección o dato, será necesario especificar (a nivel sistema operativo, obviamente), el nombre del segmento y la dirección dentro de éste.

Las direcciones absolutas son transparentes al usuario, lo que proporciona 3 ventajas al sistema operativo:

1. El sistema operativo puede resituar los segmentos cambiando solamente su dirección base en la tabla correspondiente. Esto sin afectar al código y de modo transparente al usuario.
2. Los segmentos pueden salvaguardarse en memoria auxiliar si no se utilizan.
3. Cada referencia a memoria pasa a través del sistema operativo, lo que permite verificarla si se quiere establecer alguna medida de protección.

Las ventajas ofrecidas por el mecanismo de segmentación en relación con la seguridad de la información son las siguientes:

⇒ Cada dirección referenciada puede comprobarse.
⇒ Pueden asignarse distintos niveles de protección a diferentes segmentos.
⇒ Varios usuarios pueden compartir un segmento, pero con distintos derechos de acceso.
⇒ Los segmentos pueden estar protegidos según la semántica de su contenido. Por ejemplo, un segmento que contiene código, puede especificarse como sólo para ejecución, y nadie puede copiarlo, no sobrescribirlo; un arreglo puede especificarse como lectura y escritura, pero no ejecución.
⇒ Un usuario no puede generar una dirección para acceder a segmentos no permitidos.

Sin embargo utilizar la segmentación también genera dificultades:

⇒ Necesidad de almacenar el tamaño de los segmentos y comprobar cada dirección para que no sobrepase el límite.
⇒ Los accesos a memoria se vuelven más lentos al tener que realizar cálculos y comprobaciones adicionales.
⇒ Posible fragmentación de la memoria y mala utilización del espacio disponible. Esto es porque la memoria sigue siendo, físicamente, un solo arreglo de bytes, que debe contener los segmentos de todos los procesos; a medida que se van creando y eliminando proceso, se va a ir produciendo, inevitablemente fragmentación externa.

Paginación

La paginación es una alternativa a la segmentación como mecanismo de gestión de memoria. En este caso la memoria se divide en páginas de igual tamaño (page frames). Los programas se dividen en secciones de igual dimensión que pueden almacenarse en las páginas de memoria. Así pues, la información contenida en cada página de memoria no tiene porque ser homogénea, sino que puede contener por ejemplo una parte de un programa y una parte de sus variables.

Cada dirección virtual de memoria tiene la forma *<página, desplazamiento>* y, al igual que ocurre en el caso de la segmentación, existe una tabla de páginas que permite realizar un proceso de conversión entre la dirección virtual y la dirección física.

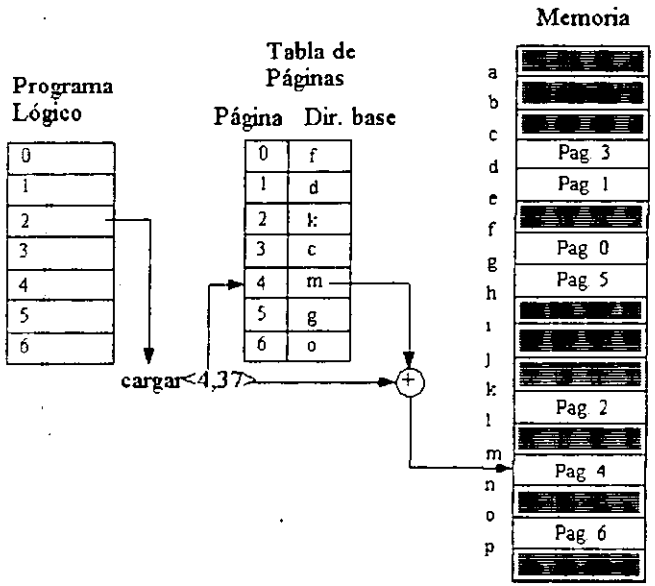
Una ventaja del uso de la paginación de memoria, es que, debido a que las páginas son de igual tamaño, no se produce el fenómeno de la fragmentación, pues ésta será sólo interna. Otra ventaja es que permite que los procesos compartan páginas; por ejemplo, varios procesos ejecutando el miso código: las primeras páginas lógicas, apuntan a las mismas páginas físicas, que contienen el código.

En cuanto a la seguridad de la información en memoria, la paginación no es un mecanismo adecuado para su gestión. Al no haber una unidad lógica de contenido en cada una de las páginas, no tiene sentido establecer distintos derechos de acceso sobre páginas diferentes. No obstante, el uso de la paginación sigue permitiendo comprobar cada dirección generada y evitar que unos procesos intenten acceder a la memoria ocupada por otros.

Una de las desventajas es, dado que cada proceso tiene su propia tabla; cuando el CPU se concede a otro proceso, es necesario cambiar la tabla de páginas a la del nuevo proceso. La paginación, en general, encarece los cambios de contexto.

En la práctica, en muchos sistemas operativos, no se utiliza un mecanismo de paginación o de segmentación puro, sino que se usa un mecanismo híbrido de segmentación paginada, mediante el cual se intentan aunar las ventajas de ambos.

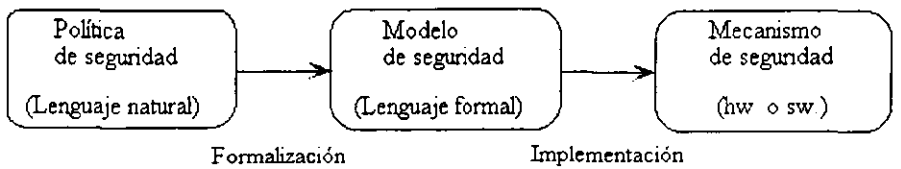
Un ejemplo de paginación, se observa en la siguiente figura; la cual esquematiza cómo es paginada por bloques una tarea determinada, su organización en la tabla de páginas y su ubicación dentro del espacio de memoria.



2.3 MODELOS Y MECANISMOS DE SEGURIDAD

Las políticas de seguridad se expresan en lenguaje natural y son ambiguas. Para evitar esta ambigüedad, antes de implementarlas se transforman en un modelo de seguridad que se expresa en un lenguaje matemático, formal y por tanto no ambiguo.

La materialización o implementación del modelo por hardware o software se denomina *mecanismo de seguridad*. La figura siguiente muestra un esquema general de un mecanismo de seguridad.



Una de las razones de la estructura *política–modelo-mecanismo* es su flexibilidad. Es posible retocar la política sin rehacer el mecanismo. Esto es, un mismo mecanismo puede ser utilizado para poner en práctica distintas políticas.

Modelos de seguridad

Un modelo de seguridad es la formulación teórica formal, es decir matemática, de una política de seguridad. La política de seguridad, debe contemplar la capacitación de:

- Los usuarios para comprender sin ambigüedad el funcionamiento eficaz del sistema.
- Los diseñadores para comprender cuales son los controles de seguridad a construir para respetar el modelo.
- Los evaluadores y certificadores para determinar si un sistema es consistente con la política y si implementa correctamente el modelo.

Todo modelo divide los componentes del sistema en dos tipos: activos y pasivos. Los componentes activos, conocidos como sujetos, son los que pueden acceder a otros componentes. En esta categoría entran por ejemplo los usuarios, los procesos en ejecución o las máquinas remotas.

Los componentes pasivos, u objetos, son los accedidos por los sujetos. En esta categoría se pueden incluir los archivos, directorios, tablas del sistema operativo, segmentos de memoria, dispositivos, etc.

Un modelo debe definir sin ambigüedad un conjunto de restricciones que prevengan la realización de acciones que puedan comprometer la seguridad. Las restricciones toman la forma de axiomas y controlan los tipos de accesos que pueden hacer los sujetos sobre los objetos.

En el siguiente diagrama general, se observa que en el modelo de seguridad están establecidos los filtros necesarios para controlar el acceso de los sujetos sobre los objetos del sistema.

Tipos de modelos

Al igual que ocurre con las políticas de control de accesos, existen dos grandes grupos de modelos:

⇒ Modelos Discrecionales y
⇒ Modelos Obligatorios.

En los modelos discrecionales se deja al sujeto la posibilidad de conceder el acceso a los objetos de su propiedad. Cada sujeto fija las restricciones sobre sus objetos. En este tipo de modelo el sistema no puede fijar restricciones especiales sobre el flujo de la información. Dado que cada sujeto determina quién y cómo accede a los objetos que le pertenecen, es imposible regular como se transfieren los objetos entre los usuarios.

Los modelos discrecionales se expresan mediante modelos de matriz de accesos, en los que se distinguen sujetos, objetos y tipos de acceso (lectura, escritura, ejecución, etc.). Son ejemplos de matriz de accesos el HRU (Harrison, Ruzzo y Ullman), y el GD (Graham y Denning).

Para establecer un control de flujo de la información es necesario utilizar modelos de acceso obligatorios. En ello el sistema especifica globalmente los canales validos a través de los que puede fluir la información. En este tipo de modelos se distinguen sujetos, objetos y retículos o niveles de seguridad.

Modelos de seguridad obligatoria

En este tipo de modelos, el control de accesos se encuentra centralizado, y se establecen una serie de medidas generales de obligado cumplimiento por parte de todos los sujetos.

El uso de estos modelos, a diferencia de los discrecionales, añade una serie de medidas para prevenir la difusión de la información mediante canales no autorizados, tanto ilegales como ocultos.

Existen dos tipos fundamentales de modelos de seguridad obligatoria:

⇒ Modelos multinivel.
⇒ Modelos de flujo de información.

Modelos multinivel

En estos modelos los objetos se caracterizan por dos parámetros que constituyen su clasificación:

- Un nivel de confidencialidad.
- Un compartimento o conjunto de compartimentos.

Los niveles de confidencialidad se ordenan de mayor a menor grado. Por ejemplo, en el ámbito de la defensa podemos distinguir los siguientes niveles de confidencialidad:

- Alto secreto
- Secreto
- Confidencial
- No clasificado

Los compartimentos pueden ser departamentos, secciones, proyectos de investigación, etc. De este modo, la clasificación de un objeto puede verse como el par:

(nivel de confidencialidad, [lista de compartimentos])

Los sujetos también tienen una clasificación dada por dos parámetros:

- Nivel de autoridad. Supone la aplicación del nivel de confidencialidad aplicado a los sujetos siguiendo el principio de menor privilegio.
- Compartimentos a los que pertenece.

Así, la clasificación de un sujeto puede expresarse como:

(nivel de autoridad, [lista de compartimentos])

En resumen, los objetos y sujetos del sistema se clasifican en distintos niveles, de ahí el nombre del modelo.

Modelos de flujo de información

En este tipo de modelos se describen los canales autorizados para el flujo de información en un sistema, especificando qué sujetos pueden acceder a qué objetos y de qué forma, según sus clasificaciones.

Los objetos y sujetos se clasifican en distintos niveles. Además existen tres modos de acceso a los objetos: lectura, escritura y lectura/escritura.

Los dos modelos de flujo de información más difundidos, son el modelo Bell-LaPadula (BLP) y el modelo Biba.

Modelo Bell-LaPadula (BLP)

Este modelo describe las rutas de flujo de información permitidas cuando se quiere mantener la confidencialidad.

Los objetos se clasifican en niveles de confidencialidad. Denotándose mediante *C(o)* el nivel de confidencialidad de un objeto *o*.

Los sujetos se clasifican en los mismos niveles, pero en este caso se denominan de autoridad. El nivel de autoridad de un sujeto *s* se expresa como *A(s)*.

Se define una relación de orden *?* entre los niveles de los objetos y sujetos. Se dice que *C(o) ? A(s)* si la confidencialidad de *o* es menor o igual que la autoridad de *s*.

Basándose en todas las definiciones anteriores, el flujo de información permitido viene definido por 2 propiedades:

1. **Propiedad de seguridad simple.**
   "Un sujeto *s* puede leer un objeto *o* si y sólo si *C(o) ? A(s)*"

   Los sujetos sólo pueden leer objetos con un nivel de confidencialidad igual o menor que su nivel de autoridad. Se dice entonces que "la lectura es hacia abajo".

2. **Propiedad estrella.**
   "Un sujeto *s* sólo puede escribir un objeto *o* si *A(s) ? C(o)*"

   Los sujetos sólo pueden escribir en objetos con un nivel de confidencialidad mayor o igual que su nivel de autoridad. Se dice entonces que "la escritura es hacia arriba".

Utilizando este modelo los sujetos podrán leer y escribir en los objetos con su mismo nivel, tan solo podrán leer objetos con menor nivel que el suyo, y tan solo podrán escribir en objetos con mayor nivel que el suyo. El flujo de la información siempre será hacia arriba, hacia mayores niveles de confidencialidad. Dicho de otro modo, un sujeto nunca podrá leer información con mayor nivel de confidencialidad que el suyo y escribirla, transferirla y desvelarla a niveles inferiores de confidencialidad.

Modelo Biba

Se trata del modelo dual del BLP. En este se pretende primar la integridad de la información. Si se observa, en el modelo BLP, los sujetos pueden escribir sobre objetos de mayor nivel que ellos mismos, es decir, pueden "atentar" contra la integridad de estos objetos.

En el modelo Biba los sujetos siguen teniendo un nivel de autoridad *A(s)*, pero los objetos se clasifican según su nivel de integridad *I(o)*.

Las propiedades que definen el flujo de información en este modelo son:

1. **Propiedad de integridad simple**
   " Un sujeto *s* sólo puede escribir en un objeto *o* si *I(o) ? A(s)*"

   Los sujetos sólo pueden escribir en objetos con igual o menor nivel de integridad que su nivel de autoridad. En este caso "la escritura es hacia abajo".

2. **Propiedad estrella**
   " Un sujeto *s* puede leer en un objeto *o* si y sólo si *A(s) ? I(o)*"

   Un sujeto sólo puede leer objetos con igual o mayor nivel de integridad que su nivel de autoridad. Así pues "la lectura es hacia arriba".

En este modelo el flujo de información siempre es hacia menores niveles de integridad, es decir, se lee de mayores niveles y se escribe en menores. De este modo, no es posible escribir, modificar o dañar objetos de mayor nivel de integridad.

Mecanismos de control de accesos

Los mecanismos son la materialización o implementación práctica de los modelos. Estos mecanismos deben monitorear todos los accesos a los objetos, así como el desarrollo de todos los comandos que otorgan, transfieren o revocan los derechos sobre los mismos.

Existen una serie de principios para el diseño de mecanismos de control de accesos que pueden resumirse del siguiente modo:

1. Menor privilegio.
2. Economía de mecanismos. Se trata de utilizar el mínimo número de mecanismos y de que éstos sean lo más sencillos posible. Esto hace más fácil su diseño, utilización y mantenimiento. Además los hace más fiables al existir menos posibilidad de defectos o "agujeros" en los mismos.
3. Diseño abierto. Su diseño debe ser público y su seguridad debe depender de unos pocos parámetros. No debe buscarse la seguridad mediante la oscuridad o la dificultad.
4. Mediación completa. No puede soslayarse el mecanismo. Todo acceso debe ser verificado y permitido por él.
5. Separación de privilegios. Los accesos deben satisfacer varias condiciones para ser permitidos. Deben pasar varios filtros y aplicarse el principio de defensa en profundidad. Por ejemplo, el acceso a la información puede depender de un mecanismo de identificación + autenticación, y adicionalmente del conocimiento de una clave criptográfica.
6. Menor número de mecanismos comunes. Debe reducirse el grado de compartición de la información.
7. Sencillez de uso. Cuanto más fácil sea de usar un mecanismo más cómodo se hará el trabajo de los usuarios y menos tentados estarán estos a intentar esquivarlo.

Algunos de los mecanismos de control de acceso más extendidos, son:

Directorio

Utilizando este mecanismo, cada sujeto tiene un directorio que lista los archivos a los que tiene acceso con sus correspondientes derechos. El propietario tiene todos los derechos de acceso sobre sus archivos, así como la capacidad de otorgarlos y revocarlos. Cualquier modificación en los directorios debe ser realizada a través del sistema operativo.

El mecanismo de permisos (r,w,x)[9] utilizado en UNIX es una variación del mecanismo de directorio.

Matriz de accesos

Se trata de implementar por software el modelo de matriz de accesos, cuando un sujeto desea acceder a un objeto debe consultar la entrada correspondiente de la matriz para ver si posee el derecho a hacerlo.

[9] El sistema operativo UNIX, se rige básicamente por estos tres tipos de permisos, que pueden ser negados o permitidos en los archivos. El significado de cada uno, es: *r*=lectura, *w*=escritura y *x*=ejecución.

La implementación directa de este modelo supone el uso de mucha memoria y tiempo de búsqueda debido a la gran dispersión de la matriz. Para solucionar este problema se utilizan listas de control de accesos o listas de potestades.

Lista de control de accesos

En las listas de control de accesos, cada objeto tiene asociada una lista conteniendo los sujetos que tienen algún derecho de acceso sobre el mismo, así como cuáles son los derechos de acceso que posee dicho sujeto.

Su uso puede ser ineficiente si cada acceso (por ejemplo, cada lectura y escritura) supone explorar la lista.

En algunas versiones de UNIX (HP-UX) se implementa este mecanismo además del de protección clásica mediante permisos.

Lista de potestades

En este mecanismo cada sujeto tiene asociada una lista de potestades. Cada potestad es un par *objeto-derechos de acceso*, y puede equipararse a una etiqueta que da a un sujeto unos determinados derechos sobre el objeto.

Cuando un sujeto quiere acceder a un objeto o archivo, consulta su lista de potestades y comprueba si este objeto está incluido en la misma y si posee los derechos necesarios para realizar las operaciones que pretende.

Algunos sistemas operativos como el MULTICS combinan ambos tipos de listas. En principio tan solo existen las listas de control de accesos. Cuando un sujeto accede al sistema su lista de potestades se encuentra vacía. Cada vez que el sujeto accede a un objeto al que tiene derecho, se añade una potestad a su lista que se mantiene en memoria y desaparece cuando el sujeto sale del sistema.

En principio las listas de potestades tienen cierta similitud con el mecanismo de directorio. Sin embargo su modo de uso es totalmente distinto.

El directorio contiene siempre todos los objetos accesibles por el sujeto y se almacena en memoria, lo que lo hace bastante inmanejable.

La lista de potestades es mucho más reducida:

- Para usuarios, tan sólo contiene en cada momento las potestades de objetos que se hayan intentado acceder desde que se entró en la máquina.
- Para procesos, contiene las potestades de los objetos que vaya a acceder durante su ejecución.

Así, pueden añadirse potestades dinámicamente desde la matriz de accesos o la lista de control de accesos. Éstas se guardan en memoria secundaria, mientras que la lista de potestades puede guardarse en una zona protegida de memoria. Esta forma de funcionar la hace mucho más eficiente que el mecanismo de directorio.

Mecanismo llave - cerradura

En este mecanismo cada sujeto tiene asociada una lista de pares (*objeto, llave*). Cada objeto tiene asociada un lista de pares (*cerradura, derechos de acceso*).

Cuando un sujeto quiere acceder a un objeto:

1. Presenta el par (*objeto, llave*) y el tipo de acceso deseado.
2. Si la llave coincide con la cerradura del objeto, y el derecho pedido se encuentra en el par, se permite el acceso.

2.4 EVALUACIÓN DE SISTEMAS OPERATIVOS SEGUROS

Además de su diseño, implementación y mantenimiento, los sistemas operativos seguros deben poder evaluarse, con el fin de estudiar su nivel de seguridad y los requisitos que cumplen.

Uno de los criterios de evaluación más extendidos es el establecido por la NCSC (National Computer Security Center) dependiente del Departamento de Defensa de los Estados Unidos. Estos criterios se plasman en el documento publicado en 1985 denominado TCSEC (Trusted Computer Systems Evaluation Critera) y también conocido como el libro naranja debido al color de su portada.

Los objetivos perseguidos al desarrollar el libro naranja, son fundamentalmente tres:

- Suministrar normas a los fabricantes sobre las funciones de seguridad a incluir.
- Proporcionar una métrica estándar para la evaluación y clasificación de sistemas seguros.

- Proporcionar una base para la inclusión de requisitos de seguridad en la adquisición de equipos.

El libro define como sistema seguro (trusted system) "Un sistema que emplea suficientes medidas de integridad hardware y software para permitir su uso para procesar simultáneamente un rango de información con distintos niveles de confidencialidad por parte de un conjunto de usuarios distintos sin violar los privilegios de acceso".

El libro naranja establece una clasificación de los distintos sistemas en función del cumplimiento de ciertos criterios de seguridad. Estos criterios se refieren a cuatro categorías básicas:

⇒ Políticas de seguridad.
⇒ Contabilidad.
⇒ Seguridad.
⇒ Documentación.

Basándose en los criterios anteriores se definen 4 niveles de seguridad o divisiones; que de menor a mayor nivel de seguridad, son:

División D: Protección mínima.

El nivel D1 es la forma más elemental de seguridad disponible, o sea, que el sistema no es confiable. Este nivel de seguridad se refiere por lo general a los sistemas operativos como MS-DOS, MS-Windows y System 7.x de Apple Macintosh. Estos sistemas operativos no distinguen entre usuarios y tampoco tienen control sobre la información que puede introducirse en los discos duros.

División C: Protección discrecional. El nivel C tiene dos subniveles de seguridad:

Clase C1: Protección mediante seguridad discrecional.

El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad disponible en un sistema típico Unix. Los usuarios deberán identificarse a sí mismos con el sistema por medio de un nombre1 de registro del usuario y una contraseña para determinar qué derechos de acceso a los programas e información tiene cada usuario.

Clase C2: Protección mediante control de accesos.

Junto con las características de C1, el nivel C2 tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso de algunos archivos basados no sólo en permisos, sino en niveles de autorización. Además requiere auditorías del sistema. La auditoría se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema. La auditoría requiere autenticación y procesador adicional, así como también recursos de disco del subsistema.

División B: Protección obligatoria. El nivel B de seguridad, tiene tres niveles:

Clase B1: Protección de seguridad etiquetada.

Es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultrasecreta. Parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

Clase B2: Conocido como protección estructurada.

Requiere que se etiquete cada objeto como discos duros y terminales. Este es el primer nivel que empieza a referirse al problema de comunicación de objetos de diferentes niveles de seguridad.

Clase B3: Dominios de seguridad.

Refuerza a los dominios con la instalación de hardware. Requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

División A: Protección verificada.

El nivel de diseño verificado, es el nivel más elevado de seguridad. Todos los componentes de los niveles inferiores se incluyen. Es de distribución confiable, o sea que el hardware y el software han sido protegidos durante su expedición para evitar violaciones a los sistemas de seguridad.

Cabe señalar que los criterios establecidos por el libro naranja están básicamente orientados a los sistemas operativos; y que debido a su origen militar se orienta hacia la preservación de la confidencialidad de la información.

Para solucionar el primer problema se han publicado toda una serie de libros adicionales relacionados con otros ámbitos de la seguridad. Estos libros constituyen la denominada serie arcoiris.

La comunidad europea también está haciendo un esfuerzo para estandarizar la evaluación de sistemas informáticos seguros, para ello, en 1990 la CEE[10] publicó el ITSEC (Information Technology Security Evaluation Criteria).

El ITSEC define 10 clases de funcionalidades de seguridad. Las 5 primeras coinciden con las del libro naranja, mientras las 5 últimas se encuentran orientadas hacia aplicaciones no jerarquizadas: bases de datos, control de procesos, intercambio de datos, dispositivos criptográficos y redes seguras.

Al evaluar los sistemas, el ITSEC los encaja en 7 niveles de seguridad, que van del E0 al E6 en función de su mayor o menor nivel de confianza.

[10] Comisión Europea, formada por: Reino Unido, Alemania, Francia y los Países Bajos.

Como se pudo apreciar en el desarrollo de los temas de este segundo capítulo; es un punto sumamente importante el hecho de procurar el mejor resguardo posible del sistema operativo, ya que es el encargado a nivel interno, de la administración de los dispositivos con los que cuenta el equipo; así como de los procesos que se originan dentro de éste. La revisión de estos temas, permitió observar las ventajas que ofrecen los métodos de protección de memoria; por ejemplo, en virtud de que contribuyen a un funcionamiento mejorado del sistema operativo, pues permiten organizar y controlar más los procesos, evitando que interfieran entre sí, tanto los trabajos solicitados por el usuario, como los propios procesos del sistema operativo.

Se revisó también la forma de generalizar las políticas de seguridad, que en un momento dado se hayan podido establecer, para una mejor aplicación y reconstrucción de éstas, en caso necesario. Esto se logra por medio de los modelos y mecanismos de seguridad. Como se puede observar, es muy importante la comprensión de cada uno de los temas que se van revisando, ya que están estrechamente relacionados, y todos se dirigen hacia el mismo objetivo: *lograr la mejor seguridad posible en la información.*

Finalmente, se mencionaron los documentos oficiales que existen para tener una referencia del grado de seguridad que ofrece un determinado sistema operativo, lo cual, como ya se vio, repercutirá en la propia seguridad del sistema, y, por lo tanto, de la información.

De esta manera, se concluye que, además de la protección física del equipo que contiene la información a resguardar, debe estar lógicamente protegida; es decir, se debe cuidar también el sistema operativo, para prevenir que el sistema de información se vea invadido por usuarios ajenos que pretendan realizar acciones mal intencionadas para dañar o sustraer información. Es importante recordar que los ataques pueden darse desde un nivel interno como desde uno externo, y es precisamente cuando el equipo tiene comunicación al mundo exterior (Internet), cuando se deben contemplar otro tipo de medidas para mantener al máximo posible, la seguridad de la información que se transmite. En el siguiente capítulo, se revisarán algunas formas de evitar que la información sea interceptada, e incluso alterada por terceras partes.

3. CRIPTOGRAFÍA

En el capítulo 2, se revisaron temas esenciales para la seguridad en la información; tales como, la identificación y autenticación de los usuarios dentro de un sistema, se explicaron además en qué consisten cada una de sus respectivas etapas, dejando muy en claro la importancia que representan, el entendimiento y aplicación de estos conceptos. Se revisaron también diversos métodos de protección de memoria, como son: vallado, registros de reubicación, arquitectura etiquetada, segmentación y paginación. Se explicaron los conceptos de modelo y mecanismo de seguridad, y la utilidad que éstos tienen en la aplicación de las políticas de seguridad. Finalmente, se plantearon parámetros de evaluación de los sistemas operativos; así como, los objetivos que éstos persiguen.

Después de revisar el panorama vital que tiene la seguridad en los sistemas operativos; es importante considerar también las medidas mínimas recomendables al momento de realizar una transferencia de información; pues a pesar de que se hayan considerado los aspectos de confidencialidad interna de la empresa y la seguridad en el sistema operativo, de nada servirán, si la información no se protege al momento de enviarla a través de la red. Para ello, es muy recomendable, hacer uso de la *criptografía*, tema que será tratado en este tercer capítulo. Se iniciará al lector en los conceptos básicos, se revisará el papel que juega la criptografía en el campo de la seguridad informática; todo esto con el objetivo de entender cómo se aplican estos conceptos, y las ventajas que en un momento determinado pueden ofrecer, al realizar una transferencia por medio de la red, para ello, se mencionarán los sistemas de cifrado clásicos y modernos.

Los mecanismos de protección que se han revisado hasta ahora, muchas veces no son suficientes para mantener información confidencial adecuadamente resguardada. Con el uso masivo de las redes de computadoras, más y más información se transmite a través de ella, y nadie puede estar seguro de que no hay *mirones* en el alambre. Los métodos criptográficos son los más comúnmente usados para proteger información confidencial. Lo que se envía por la red no es la información original, sino la información codificada, que carece de sentido salvo para el receptor, que puede decodificarla.

Se entiende por criptología el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor. La criptografía es la parte de la criptología que estudia cómo cifrar o esclarecer efectivamente los mensajes. Etimológicamente la palabra criptografía proviene del griego *kryptos* (oculto) y *grafía* (escritura):*Escritura oculta*. La criptografía es pues la ciencia que estudia la escritura secreta, es decir, la forma de escribir ocultando el significado.

Por otro lado, su oponente, el criptoanálisis, es la ciencia que se ocupa de esclarecer el significado de la escritura ininteligible. No hay que confundir el criptoanálisis con el descifrado de la información. El descifrado de la información es por medios lícitos, utilizando la clave y el sistema adecuado, y forma parte de la criptografía, mientras que el criptoanálisis pretende descifrar el mensaje sin conocer la clave.

La criptología engloba tanto a la criptografía como al criptoanálisis; el éxito de un criptoanalista supone el fracaso de un criptógrafo y viceversa.

3.1 ANTECEDENTES

Se puede decir que la criptografía es tan antigua como la civilización; cuestiones militares, religiosas o comerciales impulsaron desde tiempos remotos el uso de escrituras secretas; los antiguos egipcios usaron métodos criptográficos, mientras el pueblo utilizaba la lengua demótica, los sacerdotes usaban la escritura hierática (jeroglífica) incomprensible para el resto. Los antiguos babilonios también utilizaron métodos criptográficos en su escritura cuneiforme. El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta, el cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar la lista en un rodillo llamado hesítala, el mensaje quedaba claro cuando se enrollaba la tira de papel alrededor del rodillo de longitud y grosor adecuados. Carlomagno sustituía ya las letras por símbolos extraños. En la época de los romanos se utilizó el cifrado César que consistía en cambiar cada letra por la que ocupaba tres lugares más adelante en el abecedario.

En la Edad Media San Bernardino evitaba la regularidad de los signos (con lo que el criptoanálisis por el método de las frecuencias no era efectivo) sustituyendo letras por varios signos distintos, así tenía un símbolo para cada consonante, usaba tres signos distintos para cada una de las vocales y utilizaba signos sin ningún valor. El libro más antiguo del que se tiene constancia y que trata sobre criptografía es el Liber Zifrorum escrito por Cicco Simoneta en el siglo XIV. En el siglo XV destaca León Battista Alberti que es considerado por muchos el padre de la criptología; crea la primera máquina de criptografiar que consiste en dos discos concéntricos que giran independientes consiguiendo con cada giro un alfabeto de transposición. En el siglo XVI, Girolamo Cardano utilizó el método de la tarjeta con agujeros perforados, que se debía colocar sobre un texto para poder leer el mensaje cifrado; en ese mismo siglo Felipe II utilizó una complicada clave que el francés Viete logró descifrar. En ese mismo siglo, Blaise de Vigenére publica Traicté des Chiffres donde recoge los distintos métodos utilizados en su época, el método Vigenére es un método clásico de cifrado por sustitución que utiliza una clave.

Carlos I de Inglaterra usó en el siglo XVII códigos de sustitución silábica. Napoleón, en sus campañas militares y en los escritos diplomáticos, usó los llamados métodos Richelieu y Rossignol y para evitar la regularidad de los símbolos asignaba números a grupos de una o más letras.

En el siglo XIX se utiliza ampliamente el método de transposición, consistente en la reordenación según distintos criterios de los símbolos del mensaje. Kerckhoffs escribe el libro La Criptografía Militar en el que da las reglas que debe cumplir un buen sistema criptográfico. En la Primera Guerra Mundial los alemanes usaron el sistema denominado ADFGX, en el que a cada combinación de dos letras del grupo ADFGX se le hace corresponder una letra del alfabeto y a la que posteriormente se le hacía una transposición en bloques de longitud 20. El presidente americano Jefferson diseñó un cilindro formado por varios discos que se utilizaba como máquina criptográfica. El mayor desarrollo de la criptografía se dio en el periodo de entreguerras por la necesidad de establecer comunicaciones militares y diplomáticas seguras.

En 1940 se construyó la máquina Hagelin C-48, consistente en seis volantes unidos por el eje y con distinto número de dientes. En la Segunda Guerra Mundial se construyó por parte alemana la máquina Enigma, que se basaba en un perfeccionamiento del cilindro de Jefferson, pero la máquina británica Colossus consiguió descifrar los mensajes cifrados con Enigma. Los americanos construyeron la máquina Magic utilizada para descifrar el código púrpura japonés ; los americanos a su vez usaron a los indios navajos con su difícil lenguaje para la transmisión de mensajes.

Con el desarrollo de la informática en la segunda mitad de este siglo y con el uso cada vez más extendido de las redes informáticas y del almacenamiento masivo de información se ha dado paso a un gran salto en el estudio de sistemas criptográficos. En 1975 Diffie y Hellman establecieron las bases teóricas de los algoritmos de llave pública, hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta. En la actualidad se usan distintos métodos criptográficos, el DES[11] (de llave secreta), método RSA[12], método de Merkle y Hellman[13], etc.

3.2 CONCEPTOS BÁSICOS

En la práctica, la criptografía se ocupa del cifrado y el descifrado de mensajes. Cifrar información consiste en transformar un mensaje en claro (plaintext) en un mensaje cifrado (ciphertext) mediante el uso de una clave.

El texto en claro es inteligible (si se conoce el lenguaje utilizado), mientras el texto cifrado es ininteligible, es decir, tiende a parecerse a una sucesión de caracteres aleatorios a los que no es posible otorgar ningún significado.

[11] (DES) Data Encryption Standard.
[12] Criptosistema de clave pública, cuyo nombre proviene de sus creadores Rivest, Shair y Adleman.
[13] Criptosistema de clave pública que se utiliza para secreto, y no para preservar la autenticación de la firma.

La operación inversa al cifrado es el descifrado, y consiste en obtener el texto en claro a partir del texto cifrado.

Es necesario hacer una distinción entre código y cifra, con un código se sustituye una palabra o frase del texto original por otra palabra o frase en el texto cifrado. La traducción a una lengua extranjera es un buen ejemplo de código, asi podemos transformar el mensaje original "estoy contento" por "☺" o "emprender la guerra" por "to go to war". La cifra suele actuar antes sobre caracteres que sobre palabras, utilizando un sistema de signos en el que se transcriben guarismos, letras o símbolos según una clave acordada; es posible, por ejemplo, cifrar el mensaje "emprender la guerra" escribiendo "merpneedlrgaeurra" donde la clave utilizada ha sido: eliminar los espacios en blanco, tomar las letras de dos en dos y cambiando su orden escribirlas.

Componentes de un criptosistema

Todo sistema criptográfico o criptosistema consta de cinco componentes básicos:

1. El *espacio de mensajes*, que es el conjunto de los posibles textos en claro. Los elementos de este conjunto se denominan mensajes, teniendo en cuenta que nos referimos a mensajes inteligibles. Los mensajes se forman a partir de un alfabeto, mediante unas reglas sintácticas y semánticas del idioma en que se originan.

2. El *espacio de cifrado* o de textos cifrados, es el conjunto de todos los posibles mensajes cifrados. El alfabeto de los textos cifrados puede ser el mismo o ser distinto del utilizado para los mensajes en claro.

3. El *espacio de las claves*, es el conjunto de las posibles claves utilizadas en los procesos de cifrado y descifrado.

4. Una *familia de transformaciones de cifrado*, donde un parámetro, denominado clave de cifrado, define la transformación concreta realizada.

5. Una *familia de transformaciones de descifrado*, donde la clave de descifrado define la transformación utilizada.

MÉTODOS CRIPTOGRÁFICOS BÁSICOS.

Sustitución.

El método de sustitución consiste básicamente en sustituir los caracteres del mensaje inicial por otros; los nuevos caracteres pueden ser de cualquier tipo: letras, símbolos, dígitos, etc... Los caracteres iniciales siguen estando en el mismo orden pero salvo que se conozca la equivalencia entre los nuevos caracteres y los antiguos el mensaje es ilegible.

Se pueden considerar dos tipos de sustitución:

1) Equivalencia entre alfabetos carácter a carácter. A cada letra del alfabeto ordinario se le hace corresponder un símbolo y el mensaje se cifra cambiando las letras iniciales por su equivalente; por ejemplo, si a la letra A se le asigna el símbolo "@" en el mensaje cifrado tendremos siempre @ en lugar de A.

2) Utilización de cifra o clave. Distinto del anterior porque una vez establecida la correspondencia entre alfabetos (que en este caso pueden ser el mismo) la asignación de caracteres se realiza teniendo en cuenta la posición del carácter en el mensaje y el dígito que le corresponde según la clave, . Por ejemplo: sea el mensaje "SECRETO" y la cifra "23" el mensaje cifrado se consigue (utilizando el mismo alfabeto) adelantando 2 letras la primera que se encuentre, 3 la segunda, 2 la tercera, 3 la cuarta y así sucesivamente, el mensaje cifrado será pues: "UHEUGWQ", como se ve la letra "e" del mensaje inicial aparece una vez como h y otra como g, ya no hay una correspondencia uno a uno entre el alfabeto inicial y los símbolos del mensaje cifrado. Este método se conoce con el nombre Vigenere.

Para descifrar un mensaje cifrado debemos (en principio) conocer la correspondencia entre alfabetos y en su caso conocer también la clave.

Transposición.

El método de transposición consiste en una reordenación de los símbolos del mensaje original de modo que éste resulte ilegible. Si un mensaje consta de n letras se podrá transponer de n! (n factorial) formas. La reordenación se puede realizar desde un modo simple: escribiendo el mensaje letra a letra pero al revés, o utilizando complicados esquemas matriciales.

Los métodos básicos de sustitución y transposición se pueden combinar para formar métodos mixtos más seguros ante un ataque criptográfico. Los métodos clásicos han demostrado su ineficacia ante la potencia de cálculo de las máquinas modernas, por lo que no se usan en aplicaciones que necesiten una mínima seguridad, sistemas de cifrado como los usados por algunos procesadores para cifrar textos que han sido rápidamente criptoanalizados.

Método de las frecuencias.

El método de las frecuencias consiste en usar la permanencia estadística de los símbolos utilizados después de una sustitución; así, si el símbolo $ es el que más aparece en el criptograma, es posible pensar que con bastante probabilidad dicho símbolo corresponderá a alguna vocal (si el mensaje está en castellano).

Por lo tanto, cuando se tiene un criptograma lo suficientemente largo (póngase por ejemplo 100 caracteres) y se sospecha que está cifrado por sustitución simple, el primer paso del criptoanálisis debe ser realizar una tabla con las frecuencias de cada uno de los símbolos, ordenar dicha tabla de mayor a menor; después se deberán asociar los símbolos con los correspondientes (en el mismo orden de mayor a menor) a los que aparecen las letras en español, dicha tabla se puede componer a partir de un texto cualquiera lo suficientemente largo; por ejemplo, se tiene: E=17%, A=12%, 0=9%, L=8%, S=8%, N=7%, D=7%, etc.

Para mayor información se puede estudiar también la frecuencia con que se dan las letras iniciales y finales de cada palabra o la frecuencia de los grupos de 2 letras, etc.

Si se usa el método Vigenére, en el que la sustitución es polialfabética, el primer paso consistirá en descubrir la longitud de la clave, para ello se puede usar entre otros métodos el del estudio de las repeticiones en el texto cifrado, así si se repite un mismo bloque varias veces cada seis símbolos podemos deducir que la longitud de la clave es seis, separando ahora el texto en seis partes se procede como se ha visto en el párrafo anterior. En general todos los métodos clásicos por sustitución son atacables por métodos estadísticos pues con esos métodos no se pierde la redundancia de la fuente (la frecuencia de las letras en el texto original).

Un criptosistema sencillo

A continuación se muestra un ejemplo de criptosistema. Se denomina cifrado César y fue utilizado por Julio Cesar en sus campañas militares. Se trata de un sistema de sustitución simple en el que cada letra del alfabeto del mensaje es sustituida por una letra situada 3 posiciones más adelante para obtener el mensaje cifrado. Por ejemplo, la A es sustituida por la D, la B por la E, la C por la F y así sucesivamente; como se muestra en la siguiente figura:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

En este caso, la transformación de cifrado consiste en sustituir cada carácter por uno situado *k* posiciones más adelante. No solo eso, sino que la clave *k* está fijada con un valor 3 en el caso del cifrado César.

La transformación de descifrado es muy sencilla, ya que consiste en sustituir cada carácter por uno situado *k* posiciones por detrás. Como vemos se cumple que la transformación de descifrado es la inversa del mensaje cifrado.

Base teórica de la criptología

La criptología descansa sobre tres importantes campos teóricos:

⇒ La teoría de la información.
⇒ La teoría de los números.
⇒ La teoría de la complejidad algorítmica.

La fundamentación matemática de la teoría de la comunicación y su posterior aplicación a los sistemas criptográficos puede encontrarse en los trabajos de C.E. Shannon. A partir de las investigaciones de este autor, la criptografía deja de ser un arte y pasa a convertirse en una ciencia.

La seguridad de los sistemas criptográficos descansa sobre dos conceptos fundamentales, como son la ***difusión*** y la ***confusión***.

El propósito de la difusión de la información, es distribuir las propiedades estadísticas de los mensajes en claro, sobre todo el texto cifrado. Esto se puede conseguir de varias formas, por ejemplo:

- Haciendo que se altere la posición de los caracteres mediante cifrados por transposición.
- Haciendo que cada carácter del texto cifrado dependa de tantos caracteres del mensaje como sea posible.

El propósito de la confusión es establecer una relación lo más compleja posible entre la clave y el texto cifrado. De este modo, un criptoanalista no podrá deducir información acerca de la clave mediante un estudio del texto cifrado. Esta propiedad puede conseguirse por ejemplo mediante la aplicación de sustituciones.

Ambas técnicas, la difusión y la confusión, por separado, proporcionan fortaleza a los criptosistemas, sin embargo utilizadas conjuntamente pueden dar lugar a sistemas muy difíciles de atacar. El ejemplo más característico de combinación de estas técnicas es el DES (Data Encryption Standard); en éste, las permutaciones proporcionan difusión, mientras las sustituciones proveen la necesaria confusión.

Clasificación de los criptosistemas

⇒ **Restringidos.** Basan su técnica en mantener secreta la naturaleza del cifrado y del descifrado. Por ejemplo, un código.

⇒ **Clave privada**. Basan su técnica en un valor secreto, llamado clave. La cantidad de claves ha de ser grande para evitar su fragilidad por búsqueda exhaustiva.

⇒ **Clave pública.** Basan su técnica en que la clave para cifrar es pública, mientras que la de descifrar sólo es conocida por el usuario correspondiente, y además es computacionalmente difícil encontrar la clave de descifrado a partir del conocimiento de la clave de cifrado.

⇒ **Cuánticos.** Se basan en aspectos de la física cuántica.

⇒ **Probabilísticos.** Basan su técnica en que cifrar el mismo mensaje por la misma clave no siempre da el mismo mensaje cifrado. Para un criptoanalista es tan difícil conseguir cualquier información del mensaje original como reconstruirlo de nuevo.

Requisitos de un criptosistema

Todo criptosistema debe satisfacer los siguientes requisitos para ser utilizado en la práctica:

1. Las transformaciones de cifrado y descifrado deben ser computacionalmente eficientes (y no sólo eficaces) para todas las claves. Su aplicación no debe suponer un retraso excesivo en el funcionamiento del sistema, bien sea de almacenamiento o de transmisión de información; es decir, han de ser fácilmente calculables.
2. Los algoritmos de las transformaciones han de ser fácilmente implementables.
3. Principio de Kerckhoff. La seguridad del criptosistema debe depender exclusivamente del secreto de las claves, y no del secreto de las funciones de cifrado y descifrado.

Las funciones de cifrado y descifrado pueden conocerse de forma pública y deben ser tales que sin el conocimiento de las claves no pueda descifrarse un mensaje. De hecho el conocimiento público de las funciones es beneficioso para el sistema, pues las somete al escrutinio y comprobación por parte de la comunidad de criptoanalistas. Esto permite descubrir sus debilidades y su validez para la aplicación práctica.

Fuerza de un criptosistema

La seguridad de un sistema criptográfico depende de un parámetro denominado fuerza. Este parámetro define el grado de dificultad que supone romper el sistema, es decir, poder descifrar los mensajes sin conocer la clave.

Romper un criptosistema significa que un criptoanalista puede (en un porcentaje mayor del puramente aleatorio) reconstruir el texto en claro a partir de el texto cifrado, o puede hacer que el receptor acepte mensajes no generados por un emisor autorizado. En el primer caso, se habrá roto el secreto del sistema y en el segundo su autenticidad.

Los algoritmos o transformaciones de cifrado y descifrado deben buscarse para que el sistema sea lo más fuerte posible y cumpla los dos requisitos anteriores: secreto y autenticidad. De todos modos, con los medios adecuados, prácticamente todo sistema puede romperse si se dispone de mucho tiempo. Se debe pretender, no que un sistema sea totalmente inatacable, sino que sea computacionalmente imposible romperlo; es decir, implique demasiado costo determinar la clave.

Métodos de ataque de un criptosistema

Existen tres técnicas fundamentales utilizadas por los criptoanalistas para atacar un criptosistema, aunque casi siempre se utilizan combinaciones de ellas. En general las modernas técnicas de criptoanálisis suponen conocimientos matemáticos avanzados y utilizan mecanismos estadísticos, software y hardware muy sofisticados y en ocasiones muy caros.

1. Ataque a partir sólo del texto cifrado. El criptoanalista tan solo dispone de textos cifrados para obtener la clave. Todo sistema debe poder resistir este tipo de ataque, aún cuando el criptoanalista conozca la función de cifrado y el lenguaje del mensaje.

   En este método se utilizan estudios estadísticos de las características del texto cifrado, tales como distribución de caracteres, etc.

2. Ataque a partir de algún mensaje conocido. El criptoanalista puede interceptar un texto cifrado y conocer la posición de determinadas palabras o grupos de palabras en el mismo. Se ataca el sistema mediante parejas dadas de *mensaje - cifrado*, se trata de deducir la función de cifrado.

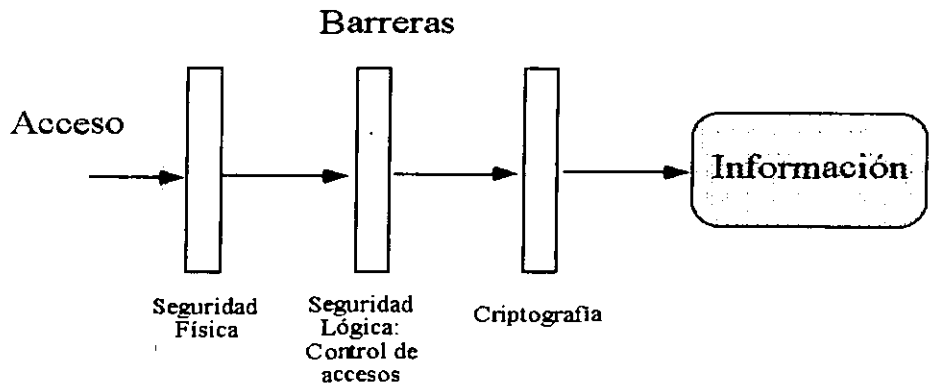
3. Ataque por elección de mensaje. Este tipo de ataque se produce cuando el criptoanalista puede introducir mensajes en el criptosistema y ver el resultado del cifrado.

   Un ejemplo de este tipo de ataque, es aquel que se realiza mediante diccionario a las contraseñas cifradas de un sistema UNIX. El criptoanalista dispone de los textos cifrados, y cifra toda una serie de textos en claro hasta encontrar uno que coincida con alguno de los cifrados.

3.3 CRIPTOGRAFÍA EN LA SEGURIDAD INFORMÁTICA

La criptografía puede aplicarse en dos ámbitos de la seguridad informática: en el almacenamiento de información y en la transmisión de la misma.

La criptografía es fundamental para la seguridad. Aunque se superen las barreras de seguridad física establecidas, e incluso las barreras de seguridad lógica para el control de accesos en el sistema operativo, la criptografía permite mantener algunas de las características de la seguridad informática, como se puede observar en la siguiente figura:



Aunque no salvaguarda la integridad de los datos ante un posible borrado total o parcial de los mismos, sí asegura su integridad en el sentido de que facilita la detección de cualquier tipo de modificación, incluido el añadido o borrado de información.

Obviamente y en primera instancia protege el secreto/confidencialidad de la información.

Cabe señalar que la criptografía no puede utilizarse para garantizar la disponibilidad de la información. Esta característica debe ser preservada mediante el uso de otro tipo de mecanismo.

Secreto o confidencialidad

Está claro que el cifrado de la información es un excelente método para proteger su confidencialidad. Aunque se acceda a la información, o se intercepte mientras se transfiere, si está cifrada sigue siendo inútil a menos que pueda descifrarse.

Integridad y precisión

Algunos sistemas criptográficos incorporan medios para prevenir que se dañe la integridad de la información, esto es, que ésta sea modificada voluntaria o involuntariamente. El sistema permite detectar cualquier pequeño cambio que se haya producido en el mensaje original.

En el ámbito militar o diplomático la principal preocupación se centra en mantener la confidencialidad de la información. Sin embargo, en la mayoría de los entornos comerciales y financieros, la principal preocupación es la integridad. Un buen sistema criptográfico debe garantizar que no se ha modificado inadvertida o maliciosamente la información enviada. Debe garantizar que no se ha deslizado ningún punto decimal o se ha producido algún tipo de redondeo no deseado en ciertas transacciones. Además debe garantizarse que no se ha añadido ningún mensaje nuevo y que no ha sido borrado alguno.

Autenticación

La criptografía también puede usarse para asegurar la autenticidad de los mensajes. Esto es, asegurar que el mensaje ha sido enviado por quién se identifica como su emisor. Se trata pues de identificar sin posible error el origen de los mensajes.

En relación con la autenticación suelen utilizarse las denominadas firmas digitales. Se trata de añadir algún tipo de información en el mensaje o de utilizar de algún modo las claves para validar al destino el origen del mensaje.

En el ámbito de la transferencia de mensajes cifrados la autenticación está muy relacionada con la integridad. Así, la autenticación de mensajes influiría tres aspectos:

1. Asegurar que el mensaje no ha sido alterado, ni maliciosa ni descuidadamente, durante su transmisión. El mensaje llegó tal y como se envío (integridad).
2. Asegurar que el mensaje no es el reenvío de uno previamente emitido e interceptado (no reenvío).
3. Asegurar que el emisor es quién dice que es (autenticidad).

No repudio

Es una característica que se relaciona con la transmisión de mensajes cifrados. Se trata de prevenir que la persona que envió el mensaje (el emisor) pueda alegar con posterioridad que él no envió ese mensaje (repudiarlo). El receptor debe disponer de mecanismos que demuestren ante terceros que sólo el emisor pudo enviar el mensaje.

3.4 SISTEMAS DE CIFRADO CLÁSICOS

Se consideran criptosistemas clásicos aquellos que son anteriores al uso sistemático de las computadoras en el campo de la criptografía. Sus características fundamentales son su simplicidad y la facilidad para recordar los algoritmos y la clave.

Dado que se aplicaban en el ámbito militar los mensajes tenían que poder cifrarse y descifrarse de modo rápido y sencillo, y el método utilizado debía ser fácil de recordar.

Estas características convertían a los sistemas en muy débiles y fáciles de atacar mediante métodos muy sencillos.

Fundamentalmente, se pueden distinguir dos tipos de cifrado clásicos:

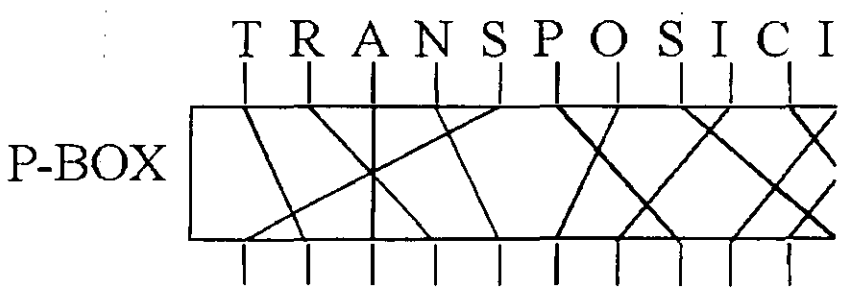
- Por transposición y
- Por sustitución.

Cifrados por transposición (o permutación)

Se reordenan los bits, caracteres o bloques de caracteres del texto en claro para obtener el texto cifrado.

El ejemplo más sencillo de este tipo de sistema es el método de transposición simple, el cual consiste en una reordenación de los símbolos del mensaje original, de modo que éste resulte ilegible. Simplemente desordenando las unidades que forman el texto "original" según la clave, dividiéndose el mensaje original en bloques de longitud *n* y aplicándose a cada bloque la transposición determinada por la clave elegida.

En la siguiente figura, se esquematiza un ejemplo de transposición de una porción de mensaje, la líneas centrales, sugieren el nuevo orden que podría tomar cada carácter dentro del mensaje así cifrado.



Cuando este sistema se aplica en computadoras, el dispositivo encargado de permutar cada bloque de texto suele denominarse *P-box (Permutation box)*.

Otro ejemplo de este sistema es el denominado de transposición por columnas. En éste, se dispone el texto por filas de una determinada longitud, rellenándose el final de la última fila con un carácter cualquiera. El texto cifrado se obtiene leyendo la matriz resultante por columnas. La clave de descifrado es simplemente el número de columnas utilizado.

Por ejemplo, se tiene el siguiente texto, y se dividirá en tres columnas para transponerlo:

EN UN LUGAR DE LA MANCHA

E	N	U
N	L	U
G	A	R
D	E	L
A	M	A
N	C	H
A	X	X

El texto cifrado, sería:

ENGDANANLAEMCXUURLAHX

Cifrados por sustitución.

Se reemplazan bits, caracteres o bloques de caracteres del texto en claro por otros en el texto cifrado.

La versión más sencilla de este tipo de método es el denominado cifrado por sustitución simple o monoalfabeto. En este sistema cada carácter del texto en claro es siempre sustituido por un mismo carácter en el texto cifrado.

Un caso de sustitución simple es el cifrado César, en el que, como ya se vio, cada carácter es sustituido por el situado tres posiciones delante en el alfabeto. Así, con el ejemplo anterior usando el cifrado por sustitución de César, el mensaje sería:

EN UN LUGAR DE LA MANCHA

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

HP XP ÑXJDU GH ÑD ODPFKD

Otra modalidad del sistema por sustitución es el cifrado por sustitución polialfabeto. En este, cada carácter del texto en claro es sustituido por un carácter distinto en el texto cifrado cada vez que aparece. En la práctica se utiliza un número limitado de alfabetos de modo que cada vez que aparece el carácter en el texto en claro se usa cíclicamente uno de los alfabetos. La máquina Enigma utilizaba un sistema de sustitución polialfabeto para cifrar los textos.

Un ejemplo de sistema de cifrado polialfabeto es el Método de Vigenere. En este sistema se utiliza como clave una palabra cuyas letras definen el desplazamiento de los distintos alfabetos a usar.

Supongamos que se utiliza como palabra clave *SOL*, así se tendría lo siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

Alfabeto 1

S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R

Alfabeto 2

O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ

Alfabeto 3

L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Cifrado

Mensaje	P	L	A	N	T	A	A	T	O	M	I	C	A
Clave	S	O	L	S	O	L	S	O	L	S	O	L	S
Cifrado	I	Z	L	F	I	L	S	I	Z	E	W	N	S

Sustitución y transposición no resultan muy efectivos usados individualmente, sin embargo constituyen la base de sistemas mucho más difíciles de criptoanalizar. Algunos de estos esquemas fueron usados en los años veinte para el diseño de las máquinas de rotor (implementaciones de cifrados de Vigenere con claves largas). Entre ellas, las dos más conocidas fueron Hagelin y la Enigma, que se usaron durante la Segunda Guerra Mundial y que ya han sido criptoanalizadas.

3.5 SISTEMAS DE CIFRADO MODERNOS

Los sistemas criptográficos modernos se desarrollan con la aparición de las computadoras, y basan su funcionamiento en la utilización de potentes y complejas herramientas hardware y software. Se utilizan claves secretas de gran longitud para controlar una compleja secuencia de operaciones con la información, que pueden incluir tanto transposiciones como sustituciones. Su posibilidad de uso se basa en la potencia y en la capacidad de las máquinas, que permiten aplicar algoritmos de gran complejidad y costos en tiempos admisibles.

Los criptosistemas modernos pueden dividirse en dos grandes categorías en función del tipo y número de claves que utilizan:

- ⇒ *Criptosistemas simétricos*, también llamados de clave única o de clave privada.
- ⇒ *Criptosistemas asimétricos*, también llamados de clave pública o de dos claves.

Ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr ciertos objetivos de seguridad.

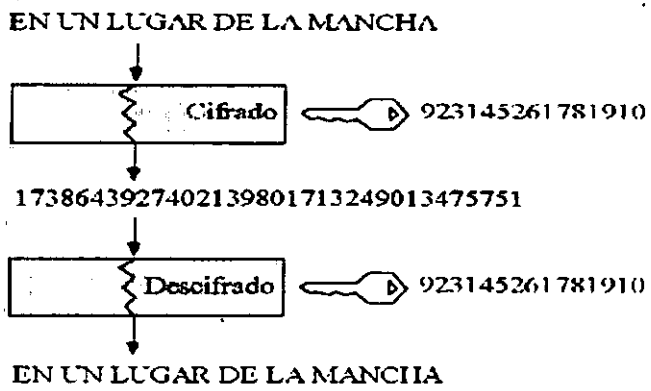
Criptosistemas de clave privada

En estos sistemas se utiliza la misma clave para el cifrado y para el descifrado. Esta clave se denomina clave privada (secreta o única) debido a que tan solo es conocida por el emisor y por el receptor del mensaje. Para que este tipo de sistema sea efectivo la clave debe ser mantenida en secreto por ambos componentes de la comunicación.

La seguridad de este tipo de sistemas depende totalmente del nivel de protección de la clave. Cuando se descifra un mensaje usando la clave privada, el hecho de que ésta sea tan solo conocida por el emisor y el receptor garantiza dos propiedades:

1. Que el mensaje no es inteligible por nadie más, es decir, que es confidencial.
2. Que si el texto descifrado es inteligible, sólo hay un emisor posible, aquel que conoce la clave privada. Esto garantiza la autenticidad del mensaje.

Por lo tanto, en este tipo de sistemas, el secreto (confidencialidad) y la autenticidad se obtienen al mismo tiempo. En la siguiente figura, se esquematiza el cifrado de un mensaje, usando un criptosistema de clave privada:



Las claves privadas deben intercambiarse de modo totalmente seguro, pues sobre ellas descansan todas las características de seguridad del sistema. Si existen *n* usuarios, cada usuario necesita *n-1* claves distintas para comunicarse con el resto. Todos estos procesos constituyen la denominada gestión de claves.

Criptosistemas de clave pública.

En este tipo de sistemas se utilizan dos claves: una clave pública y una clave privada. En un grupo de usuarios, cada uno de ellos posee dos claves distintas:

- La clave pública, *K'*, como su propio nombre indica, puede ser conocida por todos los usuarios del sistema.
- La clave privada, *K*, tan solo es conocida por su propietario.

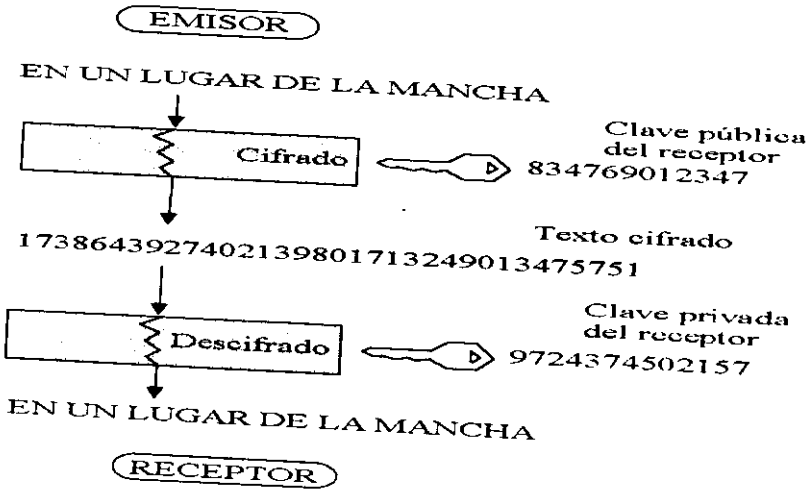
Aunque estas claves están relacionadas matemáticamente, la fortaleza del sistema depende de la imposibilidad computacional de obtener una a partir de la otra.

Este tipo de sistemas se denominan *asimétricos* porque no es posible usar una misma clave para cifrar y descifrar un mensaje. Ambas claves deben usarse en el proceso. Si se cifra un mensaje con una de ellas, se debe descifrar con la otra.

Si un usuario (emisor) quiere enviar un mensaje secreto a otro (receptor), debe cifrarlo utilizando la clave pública del receptor.

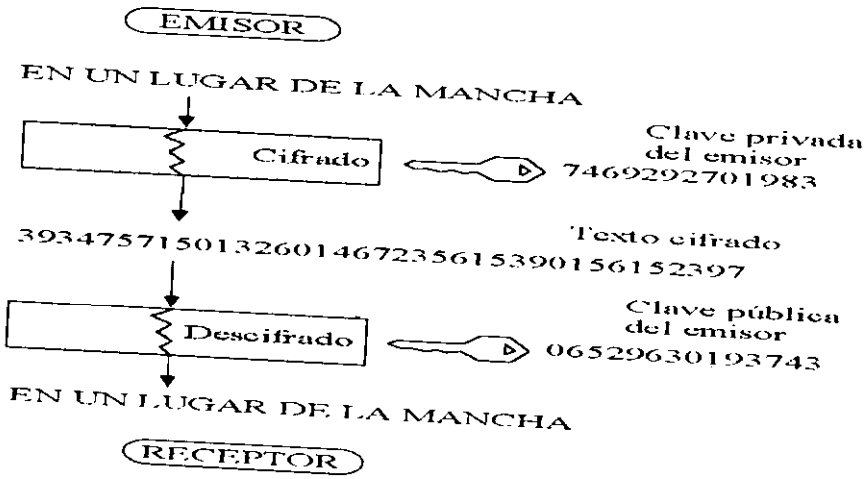
El mensaje tan solo puede descifrarse utilizando la clave privada del receptor, con lo que se garantiza la confidencialidad del mismo. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan solo el receptor (que es el único que conoce su propia clave privada), puede descifrarlo.

El funcionamiento de un sistema de clave pública, se observa en la siguiente figura:



Por otra parte, el mensaje NO es auténtico. Dado que cualquier usuario puede conocer la clave pública del receptor, cualquier usuario puede ser el emisor del mensaje. La recepción de un mensaje cifrado con la clave pública del receptor no identifica unívocamente al emisor, y por tanto no lo autentifica.

Si el emisor quiere garantizar la autenticidad de un mensaje, debe cifrarlo con su clave privada, como se esquematiza en la siguiente figura:



El receptor podrá descifrarlo usando la clave pública del emisor. Dado que todo el mundo puede conocer la clave pública del emisor, no se garantiza la confidencialidad del mensaje. Cualquiera puede descifrarlo. Sin embargo, dado que tan solo el emisor conoce su propia clave privada, tan solo él puede ser el origen del mensaje, con lo que se garantiza la autenticidad del mismo.

En este tipo de sistemas, el secreto y la autenticidad del mensaje se obtienen por separado. Para lograr las dos características de seguridad es necesario combinar ambas claves y realizar un doble proceso de cifrado y descifrado.

Criptosistemas híbridos

Tanto la criptografía de clave pública como la de clave privada tienen sus ventajas y sus inconvenientes. Debido a ello se suelen utilizar para distintos fines, y por tanto los criptosistemas de clave pública no son un sustituto de los de clave privada.

Existen dos razones que hacen que la criptografía de clave pública sea poco adecuada para la transferencia de información cifrada:

1. Los algoritmos de clave pública son lentos. Normalmente son unas 1000 veces más lentos que los de clave privada.
2. Los algoritmos de clave pública son vulnerables a ataques mediante elección de mensaje. Dado que la clave pública es de dominio público, cualquiera puede tratar de cifrar todos los mensajes posibles y comparar los resultados con los textos cifrados. Esto es especialmente posible cuando la cantidad de mensajes posibles es limitada o se tiene alguna información adicional sobre su estructura o contenido.

Debido a las razones anteriores, la transferencia de información cifrada se suele realizar mediante criptosistemas de clave privada, mientras los de clave pública se reservan para funciones tales como la transferencia de claves. Lo ideal es combinar ambos tipos de criptosistemas para lograr una transmisión segura.

Claves de un solo uso

Los criptosistemas de clave de un solo uso (*one-time pad*) pueden considerarse algunos de los más difíciles de romper. Su gran fortaleza recae en la enorme longitud de la clave y en que ésta tan solo se utiliza una vez.

La idea de estos sistemas es la siguiente. Para cifrar un mensaje dado, se genera aleatoriamente una clave de igual o mayor longitud que el mismo. La seguridad del sistema recae en la aleatoriedad de la clave, por lo que suelen utilizarse procesos de generación de números aleatorios basados en alguna fuente aleatoria natural, tal como el proceso de radiación de ciertos materiales. El ruido blanco (movimiento de electrones dentro de una resistencia) produce unas diferencias de potencial muy pequeñas y rápidamente variables, en resistencias dejadas al aire; suele ser un fenómeno físico bastante utilizado para la generación de claves aleatorias.

El emisor y receptor del mensaje comparten una única copia de la clave, y en este punto recae el problema del sistema, en la distribución segura de la misma.

La propiedad en la que se basa este criptosistema es bastante simple: la doble aplicación de la función XOR que lleva al dato original:

$$(A \text{ XOR } B) \text{ XOR } B = A$$

Si se intenta atacar este sistema mediante fuerza bruta, esto es, probando todas las claves posibles, se llegará a una situación bastante curiosa. Aunque la enorme longitud de la clave impide la implementación material de este sistema, ocurre además que dada una clave adecuada, a partir del mismo texto cifrado es posible llegar a cualquier mensaje descifrado que se quiera. De este modo cualquier mensaje descifrado es igualmente posible, con lo que un ataque por fuerza bruta es complemente inútil.

3.6 EL SISTEMA *DES* Y SUS MODOS

Origen del DES

El DES (Data Encryption Standard) es uno de los sistemas de cifrado de uso más extendido, dado que se ha convertido en un estándar reconocido por las agencias americanas y que se trata de un sistema de gran fortaleza.

El origen del DES se debe a una petición realizada en 1973 por el NBS (National Bureau of Standards) a distintos fabricantes para someter criptosistemas que pudieran servir como base a un estándar de cifrado de textos reservados no clasificados.

IBM disponía de un sistema altamente seguro denominado LUCIFER basado en una clave de 128 bits. Este sistema fue sometido al examen de la NBS y, tras ser analizado por expertos de la NSA (National Security Agency), y ser reducido a 56 bits, fue aceptado y denominado **DES**.

Funcionamiento del DES

El DES se basa en la permutación de combinaciones y sustituciones realizadas sobre bloques de 64 bits de datos usando una clave de 56 bits.

La información a cifrar se divide en bloques de 64 bits, y sobre cada uno de ellos se repite el mismo proceso. Inicialmente se divide cada bloque en dos de 32 bits, *L0* y *R0*, y se permutan estos. Posteriormente se aplican 16 etapas en las que se combina cada bloque *Li* (aplicando la función XOR), producido en la etapa anterior, con el resultado de aplicar una función al bloque *Ri* en base a 48 bits de la clave inicial, *Ki+1*, dando lugar al bloque *Ri+1*.

En una última etapa, se deshace la permutación inicial reuniendo los dos bloques resultantes para dar lugar a la salida cifrada.

Por lo tanto, el DES es reversible, es decir, puede aplicarse el mismo proceso para el cifrado como para el descifrado. Además puede utilizarse la misma clave para realizar ambos procesos, lo que lo convierte en un proceso simétrico. La clave *k* da lugar a 16 claves de 48 bits que se utilizan en cada una de las 16 etapas del método. Si para el proceso de cifrado estas claves se utilizan en un orden, para el descifrado deben utilizarse en el orden contrario.

Con el fin de reforzar la seguridad de este sistema se han propuesto diversas modificaciones del mismo, entre las que se puede destacar su aplicación reiterada (triple-DES), o la ampliación de la longitud de sus claves.

Modos del DES

El criptosistema DES puede utilizarse en cuatro modos distintos en función de que se quieran obtener ciertas características, tales como poder transmitir a través de canales con ruido, autentificar el mensaje resultante, poder descifrar sólo una parte del mismo, etc.

Los cuatro modos de operación del DES son:

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- CFB (Cipher Feedback)
- OFB (Output Feedback)

Modo ECB (Electronic Code Book)

En modo ECB el texto en claro es dividido en bloques de 64 bits que se cifran uno a uno y por separado usando el DES. La concatenación de los bloques cifrado da lugar al texto cifrado.

Este modo tiene el inconveniente de que es susceptible a ataques estadísticos y/o ataques sobre la clave, con un texto original conocido, sobre todo cuando las cabeceras de los textos tienen un formato estándar. Además, se presenta el problema de que pueden eliminarse porciones de texto cifrado sin que se note, esto es, puede ocurrir que si se conocen las características y posición de cierta información en el texto en claro, ésta puede eliminarse del texto cifrado sin impedir un correcto descifrado del mismo.

Por otro lado, este modo de funcionamiento tiene la ventaja de que trabaja bien en canales con ruido. Un fallo en la transmisión tan solo afecta a un bloque de 64 bits, no al mensaje completo.

Este modo suele utilizarse para el cifrado de claves.

Modo CBC (Cipher Block Chaining)

En este modo, antes de cifrar cada bloque de 64 bits, se le aplica una XOR sobre el bloque cifrado anterior. El primer bloque se combina con un valor conocido. De este modo, se produce un encadenamiento (chaining) entre los distintos bloques, y el resultado de cifrar cada uno de ellos depende de todos los anteriores.

Debido a esta última característica, el último bloque del texto cifrado puede actuar como firma digital o checksum del resto, permitiendo certificar que no ha sido alterado.

En este modo de funcionamiento, un error en el texto cifrado tan solo afecta al descifrado de dos bloques; es decir, tiene la ventaja de que impide la supresión y/o inserción de bloques de texto cifrado, puesto que en cualquier caso, el receptor sería incapaz de descifrar el criptograma recibido y, por lo tanto, quedaría alertado de las posibles intrusiones. Los ataques estadísticos, también se complican, debido a la interdependencia del texto cifrado a lo largo de todo el proceso.

Este modo suele utilizarse para cifrar y autentificar documentos.

Modo CFB (Cipher Feedback)

En este modo se mantiene una cola de caracteres. Se cifran bloques sucesivos de 64 bits de la cola. El byte más significativo del resultado se combina (XOR) con el siguiente byte en claro para dar lugar al byte cifrado a transmitir. Además este último byte se reintroduce en la cola provocando un desplazamiento de su contenido.

Este modo se utiliza para la seguridad de mensajes muy repetitivos y para cifrar/descifrar archivos, donde no es conveniente el almacén de información inútil.

Este método permite descifrar cualquier parte del texto cifrado sin conocer el resto. Además, tanto este modo como el siguiente realizan el cifrado a nivel de carácter, de tal manera que el texto cifrado va surgiendo de forma continua (stream mode) y no por bloques.

Modo OFB (Output Feedback)

Funciona de modo análogo al CFB, pero el byte realimentado en la cola es directamente el más significativo del cifrado de la misma.

Dado que un error en un bit del texto cifrado tan solo afecta a un bit en el texto descifrado, este modo suele utilizarse para comunicaciones vía satélite.

El sistema RSA

El algoritmo de cifrado **RSA**, es el criptosistema de clave pública más extendido. Su nombre proviene de sus creadores **R**ivest, **S**hamir y **A**dleman, quienes lo desarrollaron en 1978.

Este sistema usa dos claves y cualquiera de las dos puede ser pública o privada. Las dos claves se generan matemáticamente basándose en parte en la combinación de grandes números con factores primos.

Desde su aparición, el sistema de llave pública RSA ha ganado gran popularidad, por una parte, por la gran seguridad que ofrece al basar ésta en un problema matemático difícil de resolver que había dejado interés en la comunidad mundial, como lo es el Problema de la **F**actorización **E**ntera (**PFE**), y a causa del sistema RSA, se ha retomado e incrementado su investigación. La seguridad del sistema depende de que las claves sean de enorme longitud y de que una no pueda deducirse de la otra en un tiempo admisible.

Dado que las claves se generan a partir del producto de dos números primos, la única forma de atacarla sería factorizándolas en dichos números. Lo cual es demasiado costoso y complicado, ya que los números producto de dos primos, son de los más difíciles de factorizar.

El sistema RSA, ha sido uno de los más estudiados hasta el momento y por lo tanto se considera que es uno de los más seguros, ya que ha podido superar algunas controversias; así, actualmente es uno de los sistemas criptográficos de llave pública más usados en la industria, en el comercio, en los gobiernos, en la milicia y en general en toda actividad que requiera que la información tenga un alto grado de seguridad criptográfica. Es importante mencionar que hasta ahora se han desarrollado una gran cantidad de sistemas de llave pública con el fin de sustituir, generalizar o simplemente competir con RSA, sólo que no han tenido éxito, ya que en principio deben de pasar un riguroso criptoanálisis por parte de la comunidad criptográfica y después se someten a la competencia comercial, la prueba es en general proporcionar al menos la misma seguridad de los sistemas existentes con al menos la misma facilidad de implementación y después que basen su seguridad en problemas muy duros. Hasta ahora, solo los sistemas basados en el Problema del Logaritmo Discreto Elíptico (PLDE) [14] han podido competir exitosamente con el sistema RSA, incluso son más prometedores que RSA, ya que con sólo llaves de 160 bits proporcionan la misma seguridad. Existe otro tipo de sistemas que basan su seguridad en el PFE, sin embargo, se ha demostrado que son equivalentes a RSA, por lo que se desechan, ya que necesitan la misma o mayor longitud de las llaves.

[14] Criptosistemas públicos de curvas elípticas. Se consideran seguros, pero no han sufrido aun la misma aceptación que RSA.

3.7 PROTOCOLOS CRIPTOGRÁFICOS

La existencia de numerosos criptosistemas con determinadas características de fortaleza, seguridad, etc., no es suficiente para hacer uso de la criptografía. Es necesario aplicar una serie de técnicas denominadas protocolos para que la criptografía ofrezca ciertas propiedades de seguridad (secreto, integridad, autenticidad, etc).

Para utilizar un criptosistema en la transmisión de información es necesario establecer una serie de convenciones entre las dos partes. Estas convenciones se denominan protocolos.

Un protocolo es una secuencia ordenada de pasos tomados por dos o más partes para llevar a cabo una determinada tarea.

El uso de protocolos permite la interacción de varias partes sin la necesidad de un contacto directo, cuando se habla de realizar interacciones a distancia mediante el uso de computadoras y redes informáticas, si se habla de dinero digital por ejemplo, de compra electrónica o de transacciones monetarias entre entidades bancarias, es necesario establecer una serie de medidas que garanticen ciertas características de seguridad.

Los protocolos criptográficos son fundamentales en el actual mundo de Internet. Pueden utilizarse para transferir millones de pesos, para realizar compras, para firmar un contrato a distancia y hasta para participar en juegos sin poder hacer trampas.

Todo protocolo, debe poseer una serie de características:

- ⇒ Establecido previamente: El protocolo debe estar completamente diseñado antes de ser utilizado.
- ⇒ No ambiguo: Todas las partes deben entender perfectamente todos los pasos a llevar a cabo.
- ⇒ Completo: Para cada posible situación, el protocolo debe definir una acción a llevar a cabo.

Existen distintos tipos de protocolos:

Protocolos arbitrados

Las distintas partes que lo van a ocupar utilizan un árbitro. Se trata de una parte adicional en la transacción, desinteresado y de confianza, que garantiza que la transacción se completa correctamente.

Por ejemplo, en la compra/venta de un coche usado, un depositario del cheque y de la escritura de propiedad del coche, actuaría como árbitro del proceso. En el ámbito de los protocolos criptográficos, el árbitro puede ser tanto una persona como una máquina o un programa informático.

Protocolos adjudicados

Se utiliza un adjudicador para llevar a cabo la transacción. Se trata de una tercera parte que puede juzgar si la transacción se ha llevado a cabo justamente, por ejemplo, un notario público. Su función es atestiguar la autenticidad de ambas partes y la validez de la transacción. Mientras el árbitro participa en la transacción, el adjudicador tan solo juzga su validez. Así pues, el adjudicador tan solo es necesario en caso de disputas entre las partes.

Protocolos autoreforzados

Son aquellos en los que no es necesaria la participación de una tercera parte para garantizar la correcta ejecución de la transacción. Si cualquiera de las partes intenta "hacer trampa", este hecho se hace evidente inmediatamente y se puede demostrar ante terceras partes.

Firma digital

Una firma digital es un protocolo que produce el mismo efecto que una firma real. Se trata de una "marca" que sólo el emisor puede producir, y que otras personas pueden reconocer fácilmente como perteneciente al mismo.

El objetivo básico de las firmas digitales es que el emisor confirme su acuerdo con el mensaje y que el receptor confirme su origen y su autenticidad.

Las condiciones básicas que deben cumplir las firmas, son:

- ⇒ No falsificables: Si una persona forma un mensaje con cierta firma, es imposible que otra persona produzca el par *mensaje – firma* del remitente.
- ⇒ Auténtica: Si una persona recibe el par *mensaje – firma*, dando a entender que proviene de determinada persona, el receptor puede comprobar que la firma es realmente de quien dice ser, pues sólo esa persona puede reproducir esa firma y la firma está totalmente asociada al mensaje.

El que un mensaje no sea falsificable protege al emisor , puesto que evita que nadie pueda hacerse pasar por él en una transacción. El que sea auténtico protege al receptor, pues le permite verificar la identidad del emisor.

Además de las condiciones anteriores, las firmas digitales pueden proporcionar otras características deseables:

- ⇒ No alterables: Después de ser transmitido, el mensaje no puede cambiarse por parte del emisor, el receptor o alguien que lo intercepte.
- ⇒ No reutilizables: Un mensaje usado previamente debe ser detectable por parte del receptor.

Existen distintos tipos de firmas digitales:

- Implícitas. Las firmas implícitas se encuentran contenidas en el modo en que se ha escrito o cifrado el mensaje.
- Explícitas. Las firmas explícitas son una marca añadida pero inseparable del mensaje.
- Privadas. Las firmas privadas identifican al emisor tan solo ante alguna persona que conozca su clave privada.
- Públicas. Las firmas públicas identifican al emisor ante todo aquel que conozca su clave pública.
- Revocables. En las firmas revocables, el emisor puede negar a posteriori que él haya firmado el mensaje si se cumplen ciertas condiciones.
- Irrevocables. En las firmas irrevocables, el receptor puede probar ante terceros que el emisor es la única persona que pudo haber firmado el mensaje.

Firma digital convencional. Criptosistemas de clave privada

En un criptosistema con clave privada, la clave actúa como firma digital. El hecho de que la clave sea privada, y por tanto secreta, garantiza la confidencialidad del mensaje, es decir, nadie que no la conozca puede descifrarlo, y garantiza también su autenticidad: el receptor confirma quién es el emisor, pues sólo él pudo cifrar el mensaje con esa clave.

El problema de este sistema se encuentra en la posibilidad de falsificación. El receptor puede producir mensajes falsos y adjudicárselos al emisor. El emisor no puede repudiarlos ante terceros. La única solución a este problema es utilizar un protocolo arbitrado, en el que un árbitro garantice la corrección de la comunicación.

Supóngase que el emisor *S* tiene una clave privada *Ks*, el receptor *R* tiene una clave privada *Kr* y árbitro *A* conoce las claves de ambos.

Protocolo:

1. El emisor *S* envía el mensaje *M* cifrado al árbitro.
2. El árbitro descifra el mensaje y verifica su autenticidad: proviene de *S*.
3. El árbitro envía al receptor la identidad de *S*, su clave (*Ks*), el mensaje y la clave del propio receptor (*Kr*).
4. El receptor descifra el mensaje con *Kr* y obtiene:
   - El mensaje en claro,
   - La identidad del emisor dada por el árbitro y,
   - El mensaje original cifrado por *S*.

Condiciones cumplidas y características conseguidas:

⇒ Se cumple la autenticidad, dado que el receptor confía en el árbitro cuando afirma que el emisor es *S*.

⇒ Se cumple la no falsificación. Si *S* reclama que *R* ha falsificado el mensaje, entonces *R* puede presentar el mensaje original y su cifrado demostrando ante el árbitro que sólo *S* pudo producirlo.

Así pues, *S* no puede repudiar el mensaje, y *R* no puede falsificarlo.

Firma digital mediante criptosistemas asimétricos

Los sistemas asimétricos son ideales para aplicar firmas digitales. Utilizando la siguiente notación: *E(M,K')* supone el cifrado de un mensaje mediante una clave pública, mientras que *D(M,K)*, supone el cifrado del mensaje con una clave privada.

Para demostrar la autenticidad utilizando un criptosistema asimétrico, basta con cifrar el mensaje con la clave privada del emisor. La propia clave constituye la firma implícita del mensaje, y su descifrado permitirá verificar la validez de la misma.

Si *S* desea enviar un mensaje auténtico *M* a un receptor *R*:

1. *S* utiliza la transformación de autenticación y la envía a *R*.
2. *R* decodifica el mensaje con la clave pública de *S*.

Si el mensaje descifrado tiene sentido, queda autentificado, pues sólo *S* pudo reproducirlo con su clave privada.

Si *S* alega que el mensaje no es suyo, *R* puede mostrar el mensaje original y el cifrado. Puesto que sólo *S* pudo producir ese cifrado a partir del mensaje en claro, esto demuestra que el origen del mismo es *S*. Por lo tanto, el mensaje no es repudiable.

Supóngase que *S* desea enviar un mensaje *M*, tanto auténtico como secreto a *R*. Utilizando un criptosistema asimétrico, donde ambas características se obtienen por separado, será necesario un doble proceso de cifrado y descifrado.

1. *S* cifra el mensaje con su clave privada para autentificarlo.
2. *S* firma el resultado con la clave pública de *R* para mantener el secreto. El resultado se envía a *R*.
3. *R* descifra el mensaje con su clave privada y obtiene el mensaje cifrado y autentificado con la clave privada de *S*. Como sólo él puede llevar a cabo este paso, se mantiene el secreto del mensaje.
4. *R* descifra el resultado con la clave pública de *S* y obtiene *M*.

Si *M* tiene sentido se certifica la autenticidad del mensaje (se verifica la firma). Además, *S* no puede repudiar el mensaje, pues sólo él pudo producir el mensaje cifrado.

Es posible comprobar que los protocolos anteriores consiguen muchas características de seguridad sin la necesidad de intervención de una tercera parte. Se trata de *protocolos autoreforzados*.

Firma digital mediante funciones de resumen

Una función de resumen o sellado (sealing function o cryptographic hash function) es una función matemática que se une permanentemente a un mensaje con el fin de probar su autenticidad.

Una función de resumen produce un resumen/sello (message digest)de tamaño reducido a partir de un mensaje de gran tamaño. Debe poseer las siguientes características:

- Cualquier cambio en el mensaje, por mínimo que sea, produce un sello distinto.
- Muchos mensajes pueden dar lugar al mismo sello.
- La función no debe poder invertirse. Debe ser una función unidireccional que impida obtener el mensaje a partir del sello.
- Debe ser fácil y rápida de calcular.

En las funciones de sellado también es posible conseguir ciertas características de seguridad en las comunicaciones:

Uso arbitrado

S tiene una función personal *Fs* y *R* otra distinta *Fr*. Ambas son conocidas por el árbitro *A*.

1. *S* envía *M* y *Fs*(*M*) a *A*.
2. *A* calcula *Fs*(*M*) y lo compara con el recibido para autentificar el mensaje.
3. *A* envía el mensaje en claro, la identidad de *S*, *Fs*(*M*) y *Fr*(*M,S*) a *R*.
4. *R* recibe el mensaje,
    - Conoce *M*.
    - Pude verificar que proviene de *A* recalculando *Fr*(*M,S*) y comparándolo con el valor recibido.
    - Tras la comparación, y dado que confía en *A*, conoce la autenticidad del mensaje (proviene seguro de *S*).
    - *S* no puede repudiar el mensaje, pues *R* puede demostrar que lo produjo, presentando ante terceros *M* y *Fs*(*M*).

De esta manera se previene la revocación y mantiene la autenticidad del mensaje mediante funciones de sellado. Para evitar la reutilización, puede añadirse fecha y hora o un número de serie único a la firma digital. Es posible evitar también la reutilización de partes del mensaje, esta técnica puede usarse con distintos bloques del mensaje.

Los sistemas asimétricos son muy complejos y suponen mucho tiempo de cifrado y descifrado. Para evitar este problema pueden combinarse con el uso de funciones de resumen. Este es el mecanismo utilizado por el PGP (Pretty Good Privacy), para firmar mensajes de correo electrónico.

Supóngase que *S* quiere enviar un mensaje *M* a *R* y demostrar su autenticidad.

1. *S* aplica una función de resumen al mensaje, *Fs*(*M*).
2. *S* cifra el resumen obtenido con su clave privada *D*(*Fs*(*M*),*Ks*).
3. *S* envía a *R* el mensaje en claro y el resumen firmado.
4. *R* recibe el mensaje,
    - Conoce el mensaje en claro *M*.
    - Descifra el resumen con la clave pública del emisor y obtiene *Fs*(*M*).
    - Recalcula el resumen y lo compara con el recibido. Si ambos coinciden, el mensaje es auténtico.

Aplicación: Programa PGP

En 1992 apareció en la red un programa gratuito llamado Pretty Good Privacy (Muy Buena Privacidad). Mejor conocido por sus siglas en inglés, PGP por Philip Zimmermann y muchos otros, y que codifica archivos usando el algoritmo de encriptación RSA, lo cual permite garantizar la privacidad del mensaje, y además asegurar que un mensaje sólo pueda ser leído por la persona a la que está destinado.

PGP ofrece tres servicios:

⇒ Confidencialidad. Permite a un usuario, mediante encriptación, garantizar que solamente el destinatario podrá leer el mensaje.
⇒ Autentificación. Le da la posibilidad a un usuario de firmar el documento antes de enviarlo, lo cual permite:
    - Tener certeza de que el documento no ha sido modificado, puesto que ha sido firmado.
    - Verificar que el mensaje ha sido firmado por una determinada persona.
⇒ Integridad. La firma antes mencionada, tiene la particularidad de que depende no sólo de la identidad del remitente, sino también del contenido del mensaje, por lo que si éste es alterado, la firma ya no es válida.

En resumen, PGP permite que dos o más personas se comuniquen de manera cifrada sin que tengan que pasarse claves por vías seguras, también permite firmar digitalmente.

Modo de funcionamiento

PGP elige la clave aleatoriamente en cada mensaje, esta mide 128 bits, pero tiene el problema de cómo hacer saber al receptor cuál es la clave. Aquí es donde entra RSA, este algoritmo usará dos claves, una para cifrar y otra para descifrar, y lo que una cifra SOLO la otra lo puede deshacer.

Si alguna persona desea enviar un archivo encriptado, necesitará la llave pública del destinatario y su propia llave secreta. Cualquier archivo encriptado usando su llave pública, sólo podrá ser leído por el destinatario, lo cual es una garantía de seguridad.

Ahora, una vez concluidos los temas que componen el tercer capítulo de este trabajo, el lector tiene ya un panorama más fortalecido de lo qué es la criptografía, ya que se ha hecho un recorrido desde sus antecedentes, hasta los protocolos criptográficos usados actualmente.

Según lo aprendido a lo largo de este tema, es posible resumir que el principio básico de la criptografía es mantener la privacidad de la comunicación entre dos o más personas, alterando el mensaje original de tal forma que sea incomprensible a toda persona distinta al destinatario o destinatarios. Y que es precisamente en el hecho de mantener la privacidad en el almacenamiento y transmisión de la información, donde radica la importancia que tiene la criptografía dentro del tema de la seguridad informática; ya que incluso, permite la detección de alguna modificación o eliminación de información, asegurando de esta manera la integridad de la misma. Además, la criptografía permite asegurar la autenticidad de los mensajes, por medio del uso de las firmas digitales, por ejemplo.

Se ha visto también, con lo descrito aquí, que los sistemas de cifrado clásicos muestran mayores debilidades que los sistemas de cifrado modernos; en virtud de que estos últimos hacen uso de los potentes sistemas de cómputo actuales, por lo que no se usan en aplicaciones que necesiten una mínima seguridad, sistemas de cifrado como los usados por algunos procesadores para cifrar textos que han sido rápidamente criptoanalizados.

Se concluye de igual forma que el hecho de que los sistemas de clave pública sean más modernos y ofrezcan más posibilidades que los de clave privada, no supone que vayan a desplazarlos, ya que cada uno es adecuado para cada caso particular. Los de clave privada se usan cuando se requiere cifrar información que no se va a transmitir a una gran cantidad de usuarios; mientras que los de clave pública, son los más adecuados para el intercambio de información; además, éstos deben ser necesariamente empleados en los casos donde los de clave privada no son válidos, como para la creación de firmas digitales, el intercambio de claves o la autenticación de usuarios.

Finalmente, se vio que como en todo método de protección, también la criptografía requiere de cierta organización y características mínimas de funcionamiento, para lograr los mejores resultados posibles; para ello, existen los protocolos criptográficos, los cuales dan las propiedades de seguridad a un criptosistema en la transmisión de la información; ya que son la secuencia ordenada de los pasos a seguir por dos o más partes involucradas, con el fin de lograr la comunicación con las características deseadas.

Después de haber adquirido conocimientos en lo referente a precauciones mínimas necesarias en la transmisión y almacenamiento de información, con el tema aquí revisado: *criptografía*. Se hace ahora necesario ampliar un poco más el panorama, con respecto a los diferentes ataques a la información, que se pueden presentar cuando ésta se comparte a nivel de red; para ello, se revisarán temas a fin en el siguiente capítulo: *Seguridad en redes*.

4. SEGURIDAD EN REDES

En el capítulo anterior, se inició al lector en el problema de la seguridad en redes, con el tema de la criptología, la cual se encarga, principalmente del estudio y práctica de los sistemas de cifrado, que tienen la finalidad de ocultar el contenido de mensajes para cualquier interventor ajeno a ellos.

Se explicaron conceptos básicos como criptografía, que es la parte de la criptología que se encarga del estudio de cómo cifrar efectivamente los mensajes; y el criptoanálisis, que forma parte también de la criptología, y que busca esclarecer el significado de la escritura oculta sin conocer la clave correspondiente.

Se explicó también la clasificación de los algoritmos de cifrado, la cual es principalmente según la naturaleza del algoritmo y según la clave, como se puede observar en el siguiente recuadro:

Según la naturaleza	*Según la clave*
Sustitución: Sustituye unos símbolos por otros, ejemplo método César.	**Simétricos (clave privada)**: La clave de cifrado o descifrado es la misma, lo que implica que obteniendo una, se tiene la otra, siendo los únicos conocidos hasta el año 1976.
Permutación (Transposición): No sustituye los símbolos, exclusivamente cambia el orden de los mismos.	**Asimétricos (clave pública)**: Claves de cifrado y descifrado diferentes y el conocimiento de una no implica el conocimiento de la otra, por medios computacionales.
Producto (Supercifrado o recifrados): Son los cifrados obtenidos aplicando dos o más veces los métodos anteriores, cuantos más métodos se apliquen, más seguridad se tiene; siendo este método el más aplicado en la actualidad.	**Irreversibles**: Cifran un texto no permitiendo su descifrado, una de sus utilizaciones es la del cifrado de contraseñas, otra aplicación es la de las claves desechables o dinámicas que se utilizan en ciertos teléfonos móviles.

A lo largo del desarrollo de este capítulo, se complementará el tema de la seguridad en las redes de información, para ello, se expondrán algunos de los principales problemas que se presentan al respecto, y se describirán algunos mecanismos que se pueden utilizar para evitarlos; tales como los cortafuegos y la propia criptografía aplicada a las redes.

4.1 INTRODUCCIÓN

Desde el punto de vista de la seguridad informática, una red puede entenderse como un entorno de cómputo con más de una máquina independiente. No obstante, la introducción de las redes informáticas, implica también la introducción de toda una nueva serie de vulnerabilidades y amenazas, por lo tanto se hace necesario el uso de técnicas y herramientas para poder protegerse de ellas.

La "explosión" de Internet en los últimos años es el cambio más significativo en el mundo de la informática desde la aparición de las computadoras, e incluso, se podría decir que es la revolución más importante en el mundo de la información desde la aparición de la imprenta. En este momento nos encontramos en los inicios de la explotación de Internet, y falta todavía un asentamiento de la misma para conocer en qué se va a convertir a medio y largo plazo.

Iniciaré por citar algunas de las principales ventajas introducidas con el uso de redes informáticas:

⇒ En primer lugar y fundamentalmente, la introducción de las redes informáticas supone el hecho de compartir una enorme cantidad de recursos, tanto hardware, como software e información. Con la conexión a Internet, el usuario puede acceder a nuevas máquinas situadas en cualquier parte del mundo para desarrollar y ejecutar sus programas, puede acceder a toda una serie de aplicaciones que tal vez no podría utilizar en su máquina, y sobretodo tiene acceso a una cantidad inimaginable de información abarcando todo tipo de temas en continua actualización.

⇒ A la hora de acceder a los recursos, el uso de una red informática incrementa la fiabilidad de los mismos, puesto que su replicación permite seguir disponiendo de recursos alternativos en caso de fallo.

⇒ En aplicaciones que exijan una gran cantidad de recursos es posible repartir el trabajo entre varias máquinas distribuidas en red.

⇒ Internet es claramente expandible de modo totalmente transparente al usuario, lo que en la actualidad está permitiendo un continuo incremento en los recursos accesibles.

Como contrapartida a todas las ventajas anteriores, la conexión a la red y la expansión de Internet, ha incrementado muy sustancialmente los problemas de seguridad a los que se deben enfrentar. Desde un punto de vista general algunos de los principales inconvenientes, serían:

⇒ El hecho de compartir los recursos a través de la red incrementa el número de usuarios involucrados y por lo tanto el número de atacantes potenciales.

⇒ La complejidad del sistema. La combinación de distintos tipos de nodos con distintos sistemas operativos a través de redes que pueden ser heterogéneas, incrementa la complejidad del sistema. Los controles de seguridad se hacen entonces más difíciles de implementar.

⇒ Perímetro desconocido. La continua expansión de la red convierte en incierta la identidad de los integrantes de la misma. No se conoce qué nodos pueden conectarse ni qué nuevos problemas suponen.

⇒ Múltiples puntos de ataque. La información a proteger ya no se encuentra restringida a la memoria o los dispositivos de almacenamiento de un nodo. La introducción de la red y la transmisión de la información hace que sea necesario establecer mecanismos de protección, tanto en los nodos origen y destino, como en los dispositivos de encaminamiento y transmisión, y en todos los puntos intermedios por los que circula la información.

También es posible relacionar los nuevos problemas introducidos por las redes informáticas con cada uno de los principales aspectos de la seguridad informática:

- En cuanto a la privacidad de la información, se hace más difícil mantenerla en cada nodo debido al aumento de posibles usuarios que pueden penetrar en el mismo. Por otro lado al transferirse la información, en muchos casos sin ningún tipo de protección, aumenta el número de puntos en los que puede ser interceptada.

- En cuanto a la integridad, la transmisión de la información es un claro peligro para su mantenimiento. Los mensajes pueden ser interceptados, modificados, borrados, e incluso pueden insertarse mensajes falsos.

- En cuanto a la autenticidad, al utilizar redes informáticas no tan solo es necesario autentificar a los usuarios, sino también a los nodos.

- En cuanto a la disponibilidad, son muchos los ataques que pueden lanzarse contra una máquina con el fin de saturar sus recursos o de aislarla de la red.

4.2 REDES TCP/IP

Para poder entender algunos aspectos de la seguridad en redes informáticas es necesario recordar, aunque sea brevemente, la estructura y funcionamiento general de las mismas. Me centraré en las redes TCP/IP, dado que son éstas las que se utilizan fundamentalmente en Internet.

El modelo TCP/IP está formado por un conjunto de protocolos de comunicación, entre los que destacan los dos que le dan su nombre:

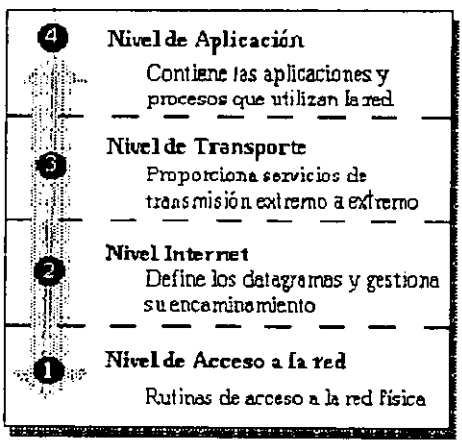
- TCP: Transmission Control Protocol.
- IP: Internet Protocol.

Todos los protocolos utilizados son estándares internacionalmente admitidos y, salvo los de más bajo nivel, son independientes del hardware y del sistema operativo utilizado.

Los distintos protocolos se integran en cuatro capas o niveles fundamentales. Cada nivel tiene sus funciones y ofrece servicios específicos. En una transmisión entre dos extremos, los mismos niveles en el emisor y el receptor manejan la misma información.

En las redes TCP/IP los cuatro niveles utilizados son :

- El nivel 4 o nivel de aplicación, donde se encuentran las distintas aplicaciones y procesos que utilizan la red, tales como el telnet, ftp o el correo electrónico (SMTP).

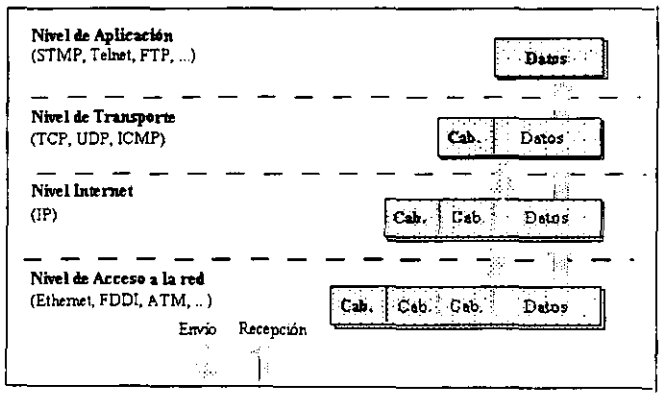


- El nivel 3 o nivel de transporte, que proporciona los servicios de transmisión extremo a extremo garantizando una serie de características en la transmisión. En este nivel se utilizan fundamentalmente los protocolos TCP (fiable, orientado a conexión y por flujo de datos) y UDP (no fiable y orientado a no conexión).

- El nivel 2 o nivel Internet, define los paquetes básicos de transmisión o datagrama y se encarga entre otros aspectos del encaminamiento de los mismos. En este nivel suele usarse el protocolo IP.

- El nivel 1 o nivel de acceso a la red, define cómo transmitir los datagramas IP sobre un soporte físico (ethernet, FDDI, X.25, etc.)

La información se encapsula en paquetes que en el emisor se transfieren desde las capas superiores a las inferiores, posteriormente circulan a través de la red física, y en el receptor se transfieren de niveles inferiores a superiores. Al transferirse entre los distintos niveles en el emisor, cada capa puede segmentar los paquetes generados por la anterior y añade su propia cabecera a cada uno de ellos, como se puede observar en la siguiente figura:



4.3 CRIPTOGRAFÍA EN REDES

Probablemente el mecanismo para proporcionar seguridad en redes más utilizado es la criptografía. Este mecanismo permite crear conexiones seguras sobre canales inseguros. El uso de la criptografía puede proporcionar propiedades tales como la privacidad, la autenticidad, la integridad y el acceso limitado a los datos, entre otras.

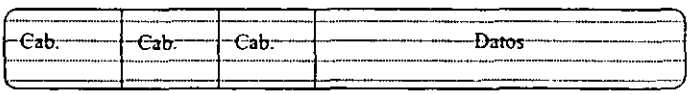
Existen dos métodos básicos de cifrado en redes:

- Cifrado de enlace.
- Cifrado extremo a extremo.

Cifrado de enlace

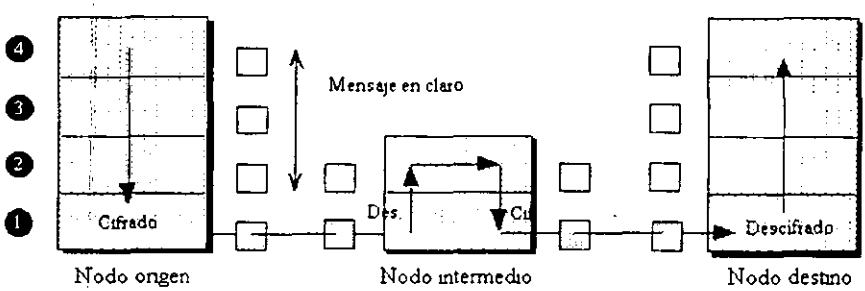
En este sistema el cifrado se realiza en la capa de acceso a red. Se cifra tanto la información del mensaje incluida en cada paquete, como las cabeceras añadidas por todos los niveles superiores.

El sistema se denomina de enlace o enlace por enlace debido a que se establece entre dos nodos consecutivos, conectados directamente mediante un enlace físico. Para ello se sitúa algún dispositivo hardware entre el nodo y el enlace que se encarga de cifrar toda la información enviada y de descifrar toda la información recibida. En la siguiente figura se observa un paquete de información:



Al transferir los mensajes, la información se encuentra protegida en cada enlace entre cada par de nodos consecutivos. Sin embargo es necesario descifrarla, aunque sea una mínima parte en cada uno de los nodos, para poder realizar procesos tales como el encaminamiento, el control de errores, etc.

En la siguiente figura se esquematiza el orden de cifrado de la información, desde un nodo origen; así como el procesamiento de descifrado en el nodo destino. Cabe señalar que al pasar por el nodo intermedio, se lleva a cabo un pequeño descifrado para lograr el encadenamiento final de la información, como se señaló en el párrafo anterior.



Así pues, el mensaje está cifrado y por tanto protegido en los enlaces, pero queda desprotegido en los nodos intermedios al tener que descifrarse.

Las principales ventajas de este sistema son las siguientes:

- El cifrado se realiza de modo totalmente transparente al usuario y a bajo nivel. Se trata de un servicio de la red, tal como el encaminamiento o la detección de errores.
- Existen dispositivos, tales como módems o encaminadores (routers), que realizan el cifrado de forma rápida y fiable por hardware. En estos casos el cifrado es invisible tanto para el sistema operativo como para el operador.
- Cada par de nodos directamente comunicados deben compartir una clave para realizar el cifrado y descifrado de la información. Si se compromete uno de los nodos, tan solo quedan comprometidas las claves que lo relacionan con los adyacentes, y no toda la red.
- Se protege toda la información, esto es, el mensaje y las distintas cabeceras. Cualquiera que intercepte un mensaje, no podrá conocer información de las cabeceras, tales como el origen o el destino del mensaje o los protocolos utilizados, que pudiera serle útil para plantear algún tipo de ataque.

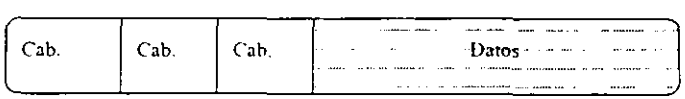
Los principales inconvenientes del cifrado de enlace son:

- La información se encuentra desprotegida en los nodos intermedios, lo que incrementa el número de puntos de ataque posibles.
- Para que el sistema sea efectivo, la información debe estar cifrada en todos los enlaces por los que transita, lo que obliga a que todos los nodos o encaminadores intermedios tengan capacidad de cifrado.

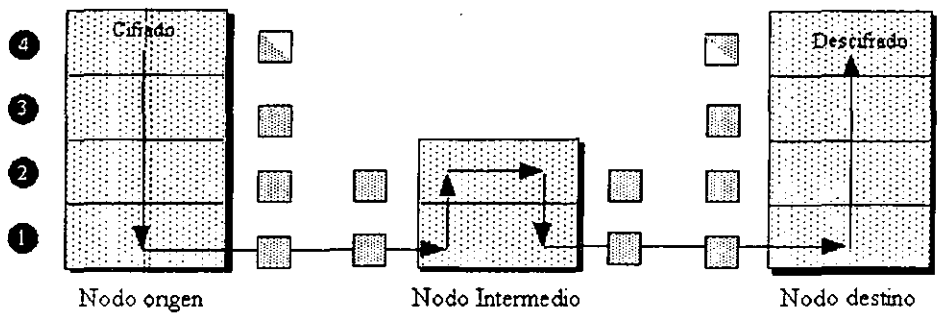
En general el cifrado de enlace es especialmente adecuado cuando la línea de transmisión es vulnerable. Si todos los nodos de la red son razonablemente seguros, pero el medio de comunicación es accesible a muchos usuarios o no es seguro, el cifrado de enlace es más conveniente.

Cifrado extremo a extremo

El cifrado extremo a extremo se realiza en el nivel de aplicación. Con este sistema tan solo se cifran los datos, y las cabeceras se añaden y transmiten sin cifrar; como se observa en la siguiente figura:



Tal y como indica su nombre, el cifrado de los datos se mantiene entre ambos extremos de la transmisión, esto es, entre el emisor y el receptor. La información no se descifra en cada uno de los nodos intermedios. En la siguiente figura, se ejemplifica el funcionamiento del cifrado extremo a extremo:



Las principales ventajas de este sistema son las siguientes:

- Es más flexible que el cifrado de enlace. El usuario puede cifrar sólo parte de la información que transmite, y puede hacerlo usando un criptosistema y una clave distinta en cada caso.
- Se protegen los datos desde el origen al destino de la transmisión. Los datos no se encuentran en claro en ningún punto intermedio, lo que hace que los únicos puntos de ataque a su confidencialidad sean los nodos emisor y receptor.
- La red no necesita disponer de ninguna facilidad específica de cifrado.

Los principales inconvenientes de este sistema son los siguientes:

- Se transmite parte de la información en claro. Cualquiera que intercepte los paquetes puede analizar las cabeceras y utilizar la información obtenida para plantear algún tipo de ataque.
- El emisor y el receptor deben ponerse de acuerdo para realizar el mismo tipo de cifrado e intercambiar la clave o claves correspondientes.

Comparación de sistemas

La siguiente tabla contiene una comparación de los aspectos fundamentales de los dos sistemas de cifrado en redes:

Cifrado de enlace	Cifrado de extremo a extremo
Seguridad en los nodos	
El mensaje queda expuesto en el nodo emisor.	El mensaje está cifrado en el nodo emisor.
El mensaje queda expuesto en los nodos intermedios.	El mensaje está cifrado en los nodos intermedios.
Papel del usuario	
El cifrado se aplica en el nodo emisor y en todos los nodos intermedios.	El cifrado es aplicado por el proceso emisor.
El cifrado es transparente al usuario.	El usuario aplica el cifrado.
El nodo se encarga del cifrado.	El usuario debe encontrar la aplicación y usarla.
Una sola facilidad para todos los usuarios.	Cada usuario selecciona su criptosistema.
Suele realizarse por hardware.	Suele realizarse por software.
Se cifran todos los mensajes o ninguno.	El usuario elige qué mensajes quiere cifrar.
Aspectos de implementación	
Se necesita una clave para cada par de nodos.	Si se usa cifrado simétrico se necesita una clave para cada par de usuarios.
Proporciona autentificación de nodos.	Proporciona autentificación de usuarios.

En resumen, el cifrado de enlace es más rápido y más fácil para el usuario. El cifrado extremo a extremo es más flexible, puede usarse selectivamente, involucra al usuario y puede personalizarse su aplicación.

Ambos sistemas pueden combinarse para conjuntar parte de sus ventajas.

4.4 VULNERABILIDADES, ATAQUES Y CONTRAMEDIDAS

Los protocolos TCP/IP no fueron pensados originalmente para proporcionar características de seguridad tales como la confidencialidad o la autenticidad, sino para transmitir información de forma eficiente. La preocupación básica en cuanto a seguridad de la versión actual del protocolo IP es el mantenimiento de la integridad de la información. Su objetivo es que todos los paquetes lleguen a su destino sin modificaciones y en el mismo orden en que fueron enviados.

Los nuevos mecanismos de seguridad en el protocolo IP se basan en la extensión de las cabeceras de los paquetes para incorporar características de autenticidad y confidencialidad, así como en la aplicación de la criptografía.

De modo general, se pueden distinguir dos grandes tipos de ataques a la seguridad en redes informáticas:

- Los ataques activos son aquellos que suponen la manipulación de los datos que circulan por la red. Pueden ser borrados, modificarse su contenido, cambiar el orden de los paquetes, e incluso añadir paquetes inútiles.

- Los ataques pasivos son aquellos basados en supervisar el tráfico en la red con el fin de obtener cierta información o para analizar sus características.

Es importante recordar que Internet se configura con base a una serie de servidores y clientes. Los servidores ofrecen servicios tales como la conexión Telnet, el correo electrónico, la transferencia de ficheros, las páginas web, etc. Los clientes acceden a los servicios conectándose a los sockets en los que se encuentran esperando los servidores.

Cada servicio en Internet tiene sus propias características y riesgos asociados. Por consiguiente es necesario estudiarlos en profundidad y por separado para establecer la combinación adecuada de medidas para hacerlos seguros. De modo general, algunas de las medidas que se pueden tomar son las siguientes:

- Configurar adecuadamente el sistema operativo, normalmente UNIX.

- Configurar los servicios atendiendo a la seguridad. Establecer los parámetros adecuados en los archivos de configuración y protegerlos adecuadamente dentro del sistema de archivos.

- Aplicar algún mecanismo de envoltura (wrapping) para hacer más seguros los servicios.

- Usar la criptografía para cifrar la información transferida.

- Utilizar algún mecanismo de filtrado o de delegación en base a un cortafuegos.

- Eliminar el servicio si se considera demasiado arriesgado.

A continuación se describen brevemente algunos de los tipos de ataques más comunes que se presentan en las redes.

Sniffing

El sniffing o fisgoneo se basa en supervisar los paquetes que circulan por la red con el fin de averiguar las contraseñas de los usuarios, o cualquier otra información transferida.

En la mayoría de las redes más extendidas, tales como ethernet, la información circula sin ningún tipo de cifrado. De este modo cualquier persona que sea capaz de "fisgonear" el tráfico, puede capturar cualquier tipo de información transmitida, incluyendo los nombres de usuario y sus contraseñas sin cifrar.

En Internet pueden encontrarse diversos programas freeware[15] que permiten vigilar el tráfico circulando por ethernet. Para utilizarlos basta con disponer de una máquina conectada a la red y, en algunos casos, de los permisos del superusuario en dicha máquina. Este sistema puede ser utilizado por cualquier usuario que disponga de una computadora en red, o bien que pueda acceder a ella y conectar su máquina con el programa fisgón.

Aunque por defecto la tarjetas de red y sus controladores están programados para vigilar tan solo paquetes dirigidos a ellas, es posible configurarlos para escuchar todo el tráfico de la misma. De este modo estos programas pueden revisar todos los paquetes, filtrar aquellos que puedan contener alguna contraseña (por ejemplo los dirigidos al puerto 23, que es el que atiende el servicio de telnet) y recortar por ejemplo los 100 primeros bytes, donde se encontrarán el nombre de usuario y su contraseña asociada.

Una variante del fisgoneo es la basada en software de dominio publico (Xwatchwin). Este programa tiene como objeto capturar sesiones Xwindows de un nodo concreto y observar las acciones realizadas. Estas herramientas se pensaron con fines docentes y para ser utilizadas por los administradores para auditar las acciones de presuntos crackers. Sin embargo en manos de usuarios malintencionados pueden ser herramientas muy dañinas, dado que permiten violar la intimidad de las personas observadas sin que éstas lo noten.

Existen diversos mecanismos para protegerse de los fisgones:

El mecanismo más seguro para protegerse del fisgoneo es la criptografía. Basta con cifrar la información que circula por la red, para evitar que, aunque ésta sea interceptada, pueda conocerse su contenido.

En segundo lugar es posible impedir que cualquier usuario no autorizado conecte un nuevo nodo a la red. Esto puede lograrse por ejemplo, controlando la identificación física de todas las tarjetas desde las que se intenta acceder a la red. El administrador del sistema mantiene una base de datos que asocia las direcciones IP de las distintas máquinas con el código de la tarjeta ethernet instalada en ellas. En el momento en que alguien intenta conectarse, se comprueba si está usando una IP válida, y si está asociada a la máquina adecuada.

Spoofing

El spoofing, que se traduce como burla o suplantación, consiste en hacerse pasar por otro para acceder a sus privilegios. Existen distintas variantes de esta técnica, según afecten a usuarios, direcciones IP o incluso servidores de nombres.

[15] Programas localizables en la red y que son de libre distribución.

La técnica más usual de suplantación consiste en obtener la contraseña de algún usuario autorizado y hacerse pasar por él para entrar en alguna máquina. El método más extendido para obtener las contraseñas se basa en el uso de programas "crackers" que efectúan un ataque mediante diccionario sobre los archivos que contienen las contraseñas de usuario cifradas.

Otro tipo de suplantación muy extendida es el de IP. En este caso se hace creer al nodo que se están conectando desde una máquina con una IP perteneciente a otra. En muchas redes locales UNIX existen distintos mecanismos para establecer un alto grado de confianza entre las máquinas que las integran. De este modo, una vez conectado a una de las máquinas de la red local es posible conectarse a cualquier otra sin necesidad de repetir el proceso de identificación y autenticación. Así, es posible suplantar la IP de alguna de las máquinas de la red local, y de esta manera, acceder directo a todas aquellas que confíen en la misma.

Otro tipo de suplantación bastante extendido se basa en el uso del protocolo STMP utilizado para la transferencia de correo electrónico. En muchos casos es posible conectarse directamente al programa servidor de este protocolo que se encuentra escuchando en el puerto 25 de alguna máquina remota. Es relativamente sencillo utilizar las ordenes admitidas por el servidor para enviar un correo en nombre de otro usuario. Mucho más peligrosas son las versiones antiguas del servidor sendmail que permiten la modificación de archivos en el nodo remoto, incluyendo el /etc/passwd. Afortunadamente las nuevas versiones del programa sendmail evitan este tipo de problemas.

La solución a todos estos tipos de ataques mediante suplantación se basa en usar técnicas de autenticación adecuadas. Se trata de validar no tan solo a los usuarios que intentan conectarse a una máquina dada, sino también al nodo desde el que intentan conectarse. Una posible técnica consiste precisamente en verificar cada IP en base al identificador físico de la tarjeta de red asociada.

Otro método de autenticación utilizado en el caso de conexiones mediante modem es la remarcación automática. En este caso la máquina destino de las conexiones, dispone de una tabla altamente protegida que asocia los identificadores de usuario con los números de modem de los mismos. Los pasos necesarios para establecer y verificar las conexiones usando este mecanismo son los siguientes:

1. El usuario llama a la máquina usando el modem.
2. El usuario se identifica.
3. La máquina corta la conexión.
4. La máquina consulta la tabla de números de modem e intenta establecer la conexión con el modem asociado al usuario.

Utilizando la remarcación automática, se impide que algún usuario se haga pasar por otro; o al menos se asegura que la llamada se origina en el modem asociado al usuario autorizado.

Hijacking

El hijacking o secuestro consiste en tomar el control de una conexión ya establecida de forma que el secuestrador suplanta la identidad del usuario autorizado, mientras este parece quedar "colgado".

Denegación de servicio

Otro tipo de ataque extendido en redes se basa en la denegación de servicio. En este sentido, se puede aplicar la denegación de servicio sobre los nodos o sobre la red. En el primer caso se saturan los recursos de la máquina o se bloquea de algún modo y se impide su uso normal. En el caso de la denegación de servicio de la red, se impide su normal funcionamiento, o se aísla completamente un grupo de máquinas de la misma evitando que se conecten.

Un método de denegación de servicio denominado flooding consiste en inundar la red con una enorme cantidad de mensajes inútiles. Otra forma más sutil de denegación se basa en interceptar ciertos paquetes selectivamente o en redireccionarlos a otros destinos. Para lograr esto último sería necesario acceder a las tablas de encaminamiento de los servidores de red y modificar su contenido.

Wrapping

El wrapping o envoltura es un mecanismo de protección software aplicable fundamentalmente a servidores UNIX. Se trata de modificar el servidor original de UNIX envolviéndolo o rodeándolo con un código adicional que lo haga más seguro. El código que se añade al servidor estándar tiene dos objetivos fundamentales:

- Restringir la conectividad. Para ello se controlan los parámetros que se le pasan al servidor en los intentos de conexión. En base a unas reglas de seguridad de la organización, se restringe el paso de ciertas peticiones. Por ejemplo, se impide el paso de conexiones desde determinadas redes o nodos, conexiones requiriendo determinados servicios, o con ciertas opciones en las cabeceras.

- Monitorización y almacenamiento de los servicios solicitados.

El aspecto general de un servidor con envoltura sería el siguiente:

```
servidor ()
{
        Control de parámetros de conexión
        Posible almacenamiento de la información
        Si petición permitida
                Llamar al servidor estándar UNIX
        finsi
}
```

Existen distintas herramientas de libre distribución que permiten envolver los servidores estándar UNIX; entre ellas cabe destacar el programa tcpwrapper, cuya característica obedece precisamente al procedimiento general arriba señalado, ya que se encarga de envolver los servicios de red que ofrece una máquina UNIX, con el fin de que en esta primera etapa sea analizada la petición de servicio, realizando las operaciones necesarias, por ejemplo, la redirección de puertos de servicio, comprueba los archivos de permisos existentes, como el hosts.allow[16] y el hosts.deny[17]. Si el software de envoltura o protección califica la petición como confiable, entonces hasta ese momento se llama al servicio propio de la máquina para que atienda la solicitud. En resumen, un programa wrapper, es aquel que sirve como intermediario entre el servidor y los servicios de éste, para incrementar la seguridad, a él llegan las peticiones de servicios, las verifica, y decide si finalmente se ejecuta o no el servicio que se ha solicitado.

4.5 CORTAFUEGOS

Además de la criptografía, el mecanismo más utilizado para proporcionar seguridad en redes son los cortafuegos (firewalls).

Cabe señalar que los cortafuegos no proporcionan seguridad absoluta, sino que son un mecanismo más, y deben combinarse con otras medidas de seguridad como las descritas en este trabajo (criptografía, autentificación de usuarios y máquinas, etc.); tanto en redes como en sistemas operativos, para hacer el sistema lo más seguro posible.

4.5.1 DEFINICIÓN Y FUNCIONES

Existen múltiples concepciones posibles para un cortafuegos, las cuales pueden ser abarcadas por la siguiente definición:

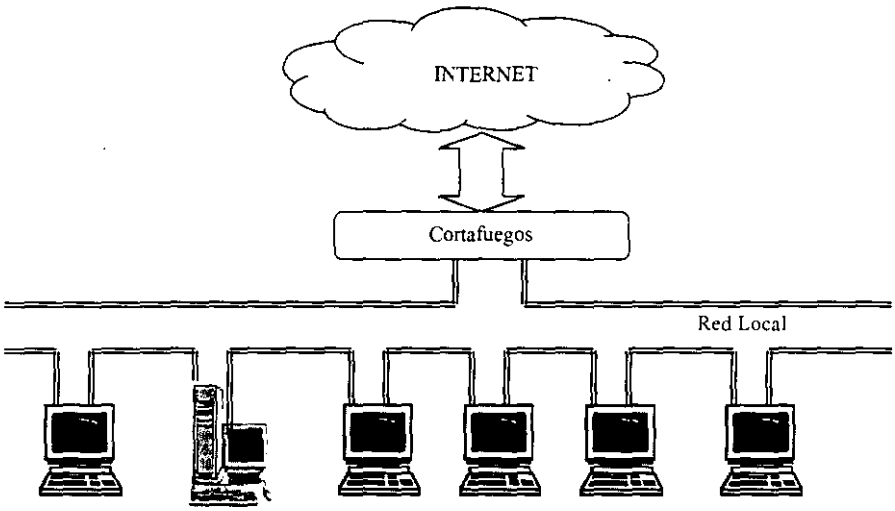
Un cortafuegos es un mecanismo que combina hardware y software para aislar una red local de Internet, ya que es el que decide qué servicios pueden ser accedidos desde el exterior de una red privada, por quiénes pueden ser ejecutados estos servicios y también qué servicios pueden ejecutar los usuarios de la red interna hacia el exterior. Para realizar esta tarea, todo el tráfico entre las dos redes tiene que pasar a través de él.

Se trata de colocar algún dispositivo o conjunto de dispositivos y programas entre la red local y la red exterior (Internet), con el fin de proteger a la primera de los posibles peligros involucrados por la segunda.

[16] Archivo de configuración en UNIX, que contiene la lista de las máquinas a las que se les permite establecer comunicación con el servidor.
[17] Archivo de configuración en UNIX, que contiene la lista de las máquinas a las que no se les permite establecer comunicación con el servidor.

Es importante no confundir un firewall con un enrutador, ya que el primero no direcciona información, función que si realiza el enrutador, además de que el firewall solamente filtra información.

En la siguiente figura se esquematiza el funcionamiento de un cortafuegos:



Así pues, el objetivo fundamental de un cortafuegos es restringir el flujo de información entre las dos redes, la local e Internet. Se trata de prevenir que cualquier ataque desde el exterior afecte a la red local. Por lo tanto, un cortafuegos no previene los ataques desde el interior, o aquellos que se llevan a cabo mediante la colaboración de usuarios interiores y exteriores.

Todo el tráfico hacia el interior y desde el interior pasa a través del cortafuegos, lo que permite establecer un punto de control donde se implementen toda una serie de medidas de seguridad. Es en el cortafuegos, donde se concreta la política de seguridad relativa al tráfico de la institución propietaria de la red local.

Existen dos políticas generales para el uso de los cortafuegos que coinciden con las establecidas en el control de accesos a sistemas operativos:

⇒ Permitir por defecto.
Siguiendo esta política todos los paquetes cuya circulación no se prohíbe explícitamente pueden circular a través del cortafuegos. Cuando el administrador considera que los paquetes de algún origen o relacionados con algún servicio son peligrosos, bloquea su paso.

Este tipo de política es más sencillo de aplicar, pero puede ser más peligroso. En este caso si algún servicio desconocido o no controlado es peligroso puede causar problemas en la red local.

⇒ Denegar por defecto.
Siguiendo esta política los paquetes cuya circulación no esté explícitamente permitida quedan bloqueados en el cortafuegos. En este caso el administrador del cortafuegos debe estudiar qué paquetes quiere dejar pasar y cuales son sus implicaciones de seguridad. Esto hace que sea una política más costosa de implementar, pero mucho más segura.

Las principales funciones de los cortafuegos son las siguientes:

- Bloquear el acceso a determinados lugares en Internet (redes, subredes, nodos específicos), o prevenir que ciertos usuarios o máquinas puedan acceder a ciertos servidores o servicios.
- Filtrar los paquetes que circulan entre la red local e Internet, de modo que sólo aquellos correspondientes a servicios permitidos puedan pasar (Telnet, e-mail, ftp, www...).
- Monitorear el tráfico. Supervisar el destino, origen y cantidad de información enviados o recibidos.
- Almacenar total o selectivamente los paquetes que circulan en el cortafuegos con el fin de analizarlos en caso de problemas.
- Establecer un punto de cifrado de la información si se pretenden comunicar dos redes locales a través de Internet.

4.5.2 COMPONENTES

Los cortafuegos se construyen a partir de dos componentes fundamentales: Filtros y nodos bastión.

Los filtros (routers o chokes) son dispositivos que permiten bloquear selectivamente determinados tipos de paquetes. Normalmente se utilizan para este propósito encaminadores (routers) o máquinas con esta función específica.

Los nodos bastión (bastion host o gate) son computadoras altamente seguras que sirven como punto de contacto principal entre Internet y la red local. Se trata de máquinas muy vulnerables al encontrarse expuestas directamente a Internet.

Los nodos bastión suelen ser máquinas UNIX en las que se han extremado las medidas de seguridad. Para ello el sistema debe reducirse al máximo y tan solo deben instalarse los servicios que sean absolutamente imprescindibles. Algunas de las medidas de seguridad a tomar en estos nodos son las siguientes:

- Intensificar la monitorización y auditación de acciones.
- No permitir las cuentas de usuario normales.
- Borrar:
  - Todos los comandos innecesarios para su funcionamiento, tales como: cc, awk, sed, perl, etc.
  - Todos los compiladores y las librerías innecesarias.
  - Todos los intérpretes de órdenes (/bin/sh, /bin/bash, etc.).
- Extremar la rigurosidad en los permisos sobre archivos y directorios.
- Eliminar todos los servicios de red innecesarios.
- Sustituir las versiones estándar de los servidores de red por otras versiones más seguras.

Los distintos tipos de cortafuegos existentes, se basan en la combinación adecuada de uno o varios de los siguientes componentes:

- Un enrutador que sirva única y exclusivamente de filtro de paquetes.
- Un servidor proxy o gateway a nivel de aplicación.
- El gateway a nivel de circuito.

4.5.3 TÉCNICAS DE USO

El funcionamiento de los cortafuegos se basa en el uso de dos tipos de técnicas básicas sobre los filtros y nodos bastión:

- El filtrado de paquetes y
- La delegación (proxying).

Filtrado de paquetes

El filtrado de paquetes consiste en controlar selectivamente qué paquetes circulan entre la red local e Internet. Para llevar a cabo este control se definen una serie de reglas que especifican qué tipos de paquetes pueden circular en cada sentido y cuáles deben bloquearse. El filtrado de paquetes se desarrolla en un filtro, que como se comentó anteriormente, puede ser un encaminador (router) o una máquina a la que se le ha asignado esta función.

Las reglas para definir los paquetes permitidos y bloqueados se basan en las cabeceras de los paquetes, y fundamentalmente en los siguientes datos incluidos en las mismas:

- Dirección IP de la fuente.
- Dirección IP del destino.
- Tipo de protocolo (TCP, UDP, ICMP, etc.).
- Puerto TCP o UDP de la fuente.
- Puerto TCP o UDP del destino.
- Alguna de las banderas (flags) u opciones de las cabeceras.

El hecho de que los programas servidores para determinados servicios Internet, tales como el ftp, Telnet, correo electrónico, etc., residan en ciertos puertos, permite al filtro aceptarlos o bloquearlos, simplemente especificando el puerto correspondiente. Así, sería posible bloquear las conexiones Telnet desde el exterior sin más que impedir el paso de todos los paquetes cuyo puerto destino sea el puerto TCP 23.

Algunos ejemplos de uso del filtrado de paquetes podían ser los siguientes:

⇒ Bloquear todas las conexiones desde el exterior excepto aquellas correspondientes a paquetes SMTP, es decir aquellas que van destinadas al puerto 25 y que permiten la recepción de correo electrónico.
⇒ Bloquear todas las conexiones desde o hacia ciertos sistemas (redes, subredes o nodos) en los que no confiamos.
⇒ Permitir ciertos servicios básicos como correo electrónico o FTP, pero bloquear otros "peligrosos", tales como RPC, rlogin, rsh, etc, porque permiten acceder al servidor en cuestión remotamente y sin identificación continua del usuario.

Mediante el uso del filtrado de paquetes, es posible discriminar entre determinados tipos de paquetes, permitir o denegar determinados servicios, pero no es posible protegerse de operaciones elementales dentro de los servicios que pueden resultar inseguras, es decir, no se puede personalizar el funcionamiento de los mismos. Con el fin de lograr este último tipo de control se suele utilizar la delegación (proxying).

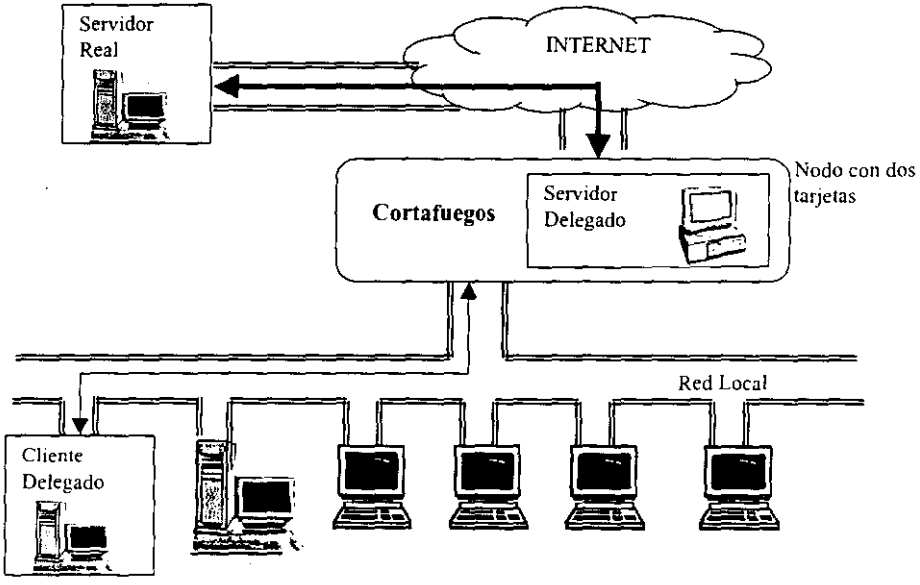
Servicios delegados (Proxy services)

Los servicios delegados son aplicaciones especializadas que funcionan en un cortafuegos (normalmente en el nodo bastión) y que sirven de intermediarios entre los servidores y clientes reales. Estas aplicaciones reciben las peticiones de servicios por parte de los usuarios, los analizan y en su caso modifican, y los transmiten a los servidores reales.

En un servicio delegado, se distinguen tres componentes:
⇒ El servidor real.
⇒ El servidor delegado (proxy server), y
⇒ El cliente delegado (proxy client).

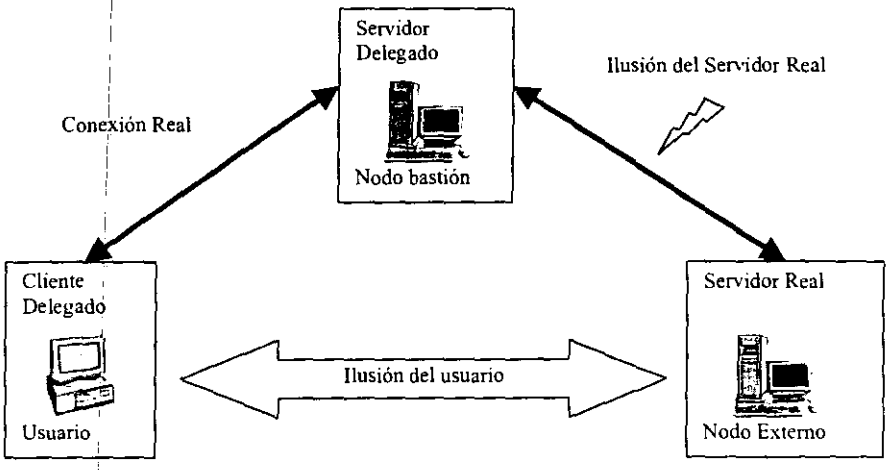
El servidor real funciona en un nodo externo en Internet y proporciona algún servicio, tal como conexión telnet, correo electrónico, conexión HTTP, etc. Se trata de alguno de los programas servidores propios del sistema operativo, tales como el telnetd, ftpd, sendmail, entre otros, que se encuentran activos en los puertos del nodo servidor remoto.

El cliente delegado (proxy client) es una versión especial del programa cliente estándar del sistema operativo (telnet, ftp, netscape, etc.). Este programa funciona en los nodos de la red local y es utilizado por los usuarios para acceder al servicio. El programa se ha preparado para que cuando el usuario solicite algún servicio se conecte al servidor delegado, y no al servidor real en Internet. Como se ejemplifica en la siguiente figura:



El servidor delegado (proxy server) es un programa especial que funciona sobre el cortafuegos (normalmente sobre el nodo bastión). Este programa actúa como intermediario entre el cliente delegado y el servidor real. Su funcionamiento es totalmente transparente a ambas partes, es decir, al servidor real y al usuario que utiliza el programa cliente. Cuando el usuario intenta obtener un servicio lo hace a través del servidor delegado, pero cree estar contactando directamente con el servidor real en Internet. En cuanto al servidor externo, cuando recibe o envía paquetes al servidor delegado, cree estar conectado directamente con el nodo local en el que se origina la petición, y no con el programa cliente funcionando sobre el nodo bastión.

Las conexiones se efectúan como esquematiza la siguiente figura:



La función del servidor delegado es analizar los paquetes que circulan a través de él, estudiar su contenido y, en función de la política de seguridad de la organización, permitir o denegar su acceso o modificar su contenido o cabeceras. También pueden usarse estos programas para monitorear el tráfico y almacenar datos sobre el mismo, tales como los destinos u orígenes más comunes, los servicios más solicitados, etc.

Algunos ejemplos de uso de los servicios delegados son los siguientes:

- Cifrado de la información enviada y descifrado de la recibida. Especialmente útil cuando se requiere conectar dos redes locales a través de Internet.
- Modificación de las cabeceras de los correos electrónicos con el fin de ocultar información sobre la red local.
- Autentificación mediante un sistema más potente que el de contraseña simple. Por ejemplo puede utilizarse un mecanismo de contraseñas de un solo uso para acceder a la red local desde Internet, mientras que las máquinas locales tan solo utilizan un mecanismo de contraseña simple.

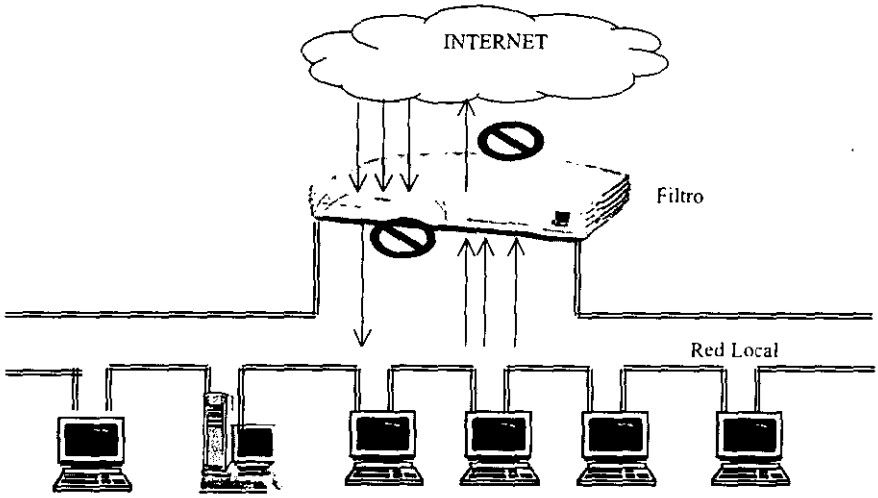
4.5.4 TIPOS DE CORTAFUEGOS

La combinación de las dos componentes básicas de los cortafuegos (filtros y nodos bastión), y la utilización de las dos principales funciones (filtrado y delegación) sobre ellas, permite definir múltiples tipos de arquitecturas para los cortafuegos. Las cuatro más comunes de menor a mayor grado de sofisticación y seguridad proporcionada, son:

1. Filtro de paquetes (Screening Router)

Esta arquitectura se basa en el uso de un simple filtro de paquetes que se encuentra entre Internet y la red local. Este filtro de paquetes suele ser un encaminador (router) que implementa las reglas de filtrado de la red local.

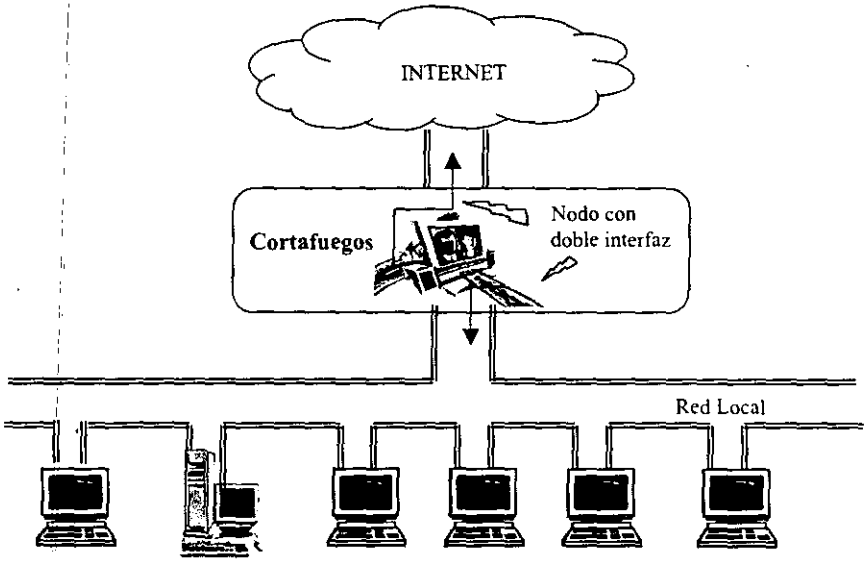
En la siguiente figura se puede observar cómo se seleccionan los paquetes en ambos sentidos de la comunicación, por medio del filtro existente:



El problema de este tipo de cortafuegos es que toda la seguridad del sistema con respecto a Internet se concentra en el encaminador. Adicionalmente el simple filtrado de paquetes no permite una gran flexibilidad a la hora de controlar la seguridad de los diferentes servicios que incluyen.

2. Nodo con doble interfaz

El nodo con doble interfaz (dual-homed host architecture) se construye sobre una máquina que actúa como nodo bastión y que incorpora dos tarjetas o interfaces de red. Una tarjeta tan solo permite la comunicación con el exterior (Internet), mientras la otra tan solo permite la comunicación con la red local. Cualquier tipo de comunicación entre las dos tarjetas se encuentra bloqueada. Su funcionamiento, se esquematiza en la siguiente figura:



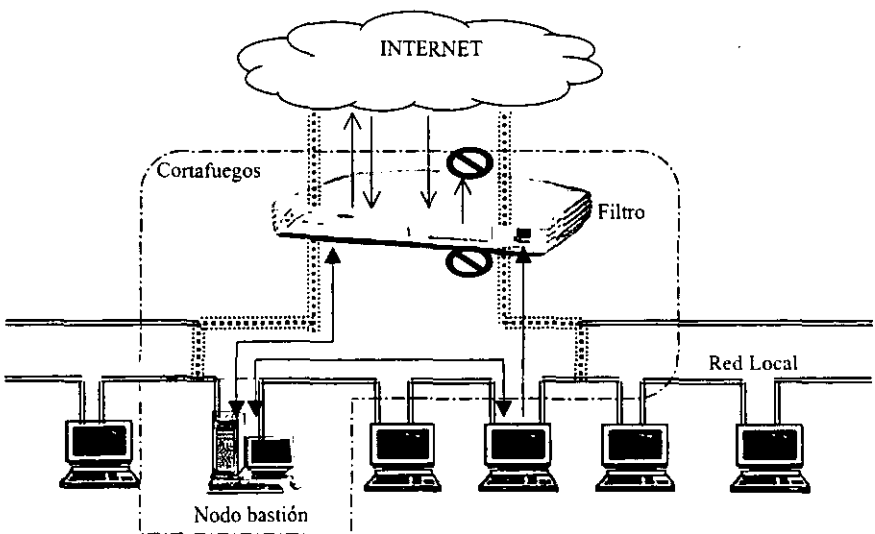
Usando este tipo de cortafuegos la comunicación directa entre la red local e Internet está prohibida. Cualquier servicio que se quiera proporcionar a los nodos locales debe implementarse mediante un servidor delegado ejecutado sobre el nodo con doble bastión.

Otra solución consiste en permitir a los usuarios conectarse al nodo bastión para que éstos accedan a los servicios de Internet. Sin embargo esta opción es bastante peligrosa puesto que puede dejar desprotegido el nodo bastión.

3. Nodo pantalla

En esta arquitectura, el cortafuegos se construye combinando un filtro y un nodo bastión; el primer nivel de seguridad descansa sobre el filtro y sobre el modo en que éste realice la función de filtrado de paquetes. El nodo bastión se sitúa en la red local y se encarga de ejecutar los distintos servidores que conectan a la red local con Internet.

El funcionamiento de esta arquitectura, se muestra en la siguiente figura:



El filtrado de paquetes se diseña de modo que no se permite el tráfico directo entre los nodos locales e Internet. Todo el tráfico, tanto de salida como de entrada, debe circular a través del nodo bastión y del filtro. Cuando el filtro recibe paquetes desde el interior, sólo debe dejar pasar aquellos que provengan del nodo bastión. Asimismo, cuando el filtro recibe paquetes desde el exterior, tan solo debe dejar pasar aquellos que vayan dirigidos al nodo bastión.

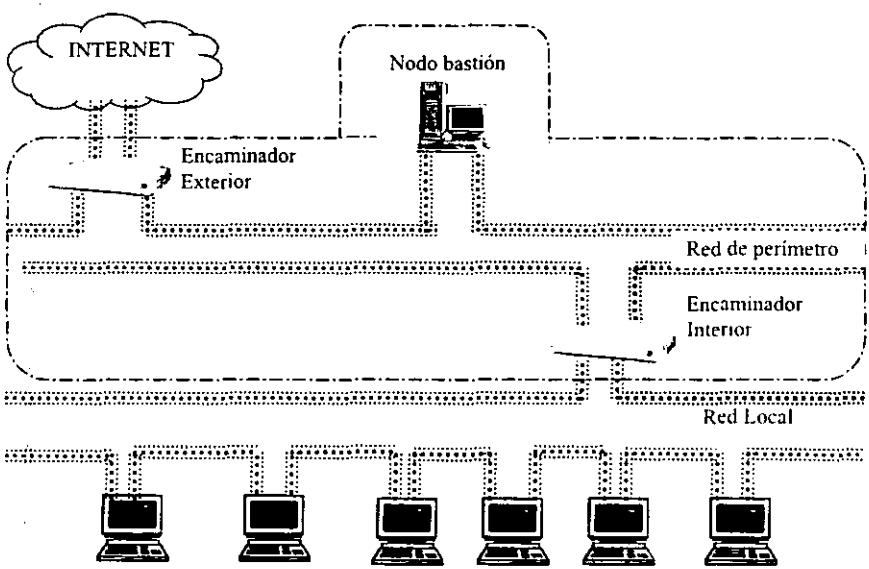
De este modo, el único nodo que realmente puede recibir y enviar correo, abrir conexiones Telnet, enviar o recibir ficheros por FTP, etc., es el nodo bastión. La seguridad en los distintos tipos de servicios puede conseguirse directamente a través del filtrado de paquetes, o bien combinando este con el uso de un servidor delegado. En el segundo caso, cuando un usuario quiere acceder a alguno de estos servicios, si están permitidos, utiliza el cliente delegado en su nodo local, este programa contacta con el servidor delegado en ejecución en el nodo bastión, y es el servidor delegado el que realmente interactúa con los servidores de Internet pasando a través del filtro.

Dado que el nodo bastión es la única máquina de la red local expuesta a Internet (siempre a través del filtro), se deben tomar especiales medidas de protección sobre el mismo.

El principal problema de este tipo de arquitecturas se produce cuando se compromete el nodo bastión. En este caso toda la red local queda expuesta a cualquier tipo de ataque desde el exterior.

4. Red pantalla

Se trata de una arquitectura más sofisticada, y al mismo tiempo más segura que las anteriores, lo que está haciendo que cada vez se utilice más. Tal y como refleja la siguiente figura, este tipo de cortafuegos consta de dos filtros y de un nodo bastión.



Los dos filtros, uno interior y uno exterior, definen entre ellos una red de perímetro (que actúa como red pantalla). En esta red de perímetro se encuentra situado el nodo bastión. Con este tipo de configuración, si el nodo bastión es comprometido, el atacante tan solo tendrá acceso a la red de perímetro, y no podrá acceder directamente a los nodos de la red local.

La red perímetro actúa como un nivel más de seguridad del sistema. Todo el tráfico confidencial entre los nodos locales, incluyendo las contraseñas de usuario, circula tan solo a través de la red local. El único tráfico permitido en la red de perímetro debe ser el destinado o proveniente de Internet.

Las técnicas de protección utilizadas con este tipo de arquitectura son similares a las de la arquitectura de nodo pantalla. Los servicios pueden controlarse directamente mediante los dos filtros, o bien pueden implementarse mediante un servidor delegado en ejecución en el nodo bastión.

En ocasiones la red de perímetro contiene más de un nodo bastión. Cada nodo en esta red puede encargarse de algunos de los servicios. Por ejemplo, uno podría encargarse del FTP y WWW, mientras otro podría encargarse del correo electrónico (SMTP) y el servicio de nombres (DNS).

4.5.5 BENEFICIOS Y LIMITACIONES DE UN CORTAFUEGOS

Beneficios

Los cortafuegos manejan el acceso entre dos redes, si no existiera, todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El cortafuegos es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red tendrá el poder de decidir si revisar estas alarmas o no, la decisión tomada por éste, no cambiará la manera de operar del cortafuegos.

Otra causa que ha hecho que el uso de los cortafuegos se halla convertido en casi imperativo, es el hecho de que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet por medio de un NAT (Network Address Traslator), y efectivamente el lugar ideal y seguro para alojar el NAT, ha sido el cortafuegos.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda usado por el tráfico de la red, y qué procesos han influido más en ese tráfico, de esta manera el administrador de la red, puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda.

Finalmente, los cortafuegos también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

Limitaciones

La limitación más grande que tiene un cortafuegos, es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los firewalls no son sistemas inteligentes, actúan de acuerdo a parámetros introducidos por el diseñador, por lo tanto, si un paquete de información no se encuentra dentro de esos parámetros como una amenaza de peligro, simplemente lo dejará pasar. Pero esto no es lo más peligroso, sino cuando el intruso deja puertas traseras, es decir, abre un hueco diferente y borra las pruebas o indicios del ataque original.

Otra limitación es que el cortafuegos "no es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o se entera de los huecos del cortafuegos y difunde la información, éste no se será capaz de detectarlo.

4.6 POLÍTICAS DE SEGURIDAD EN REDES

Antes de construir una barrera de protección, como preparación para conectar una red con el resto de Internet, es importante que se entienda con exactitud qué recursos de la red y servicios se desean proteger. Una política de red es un documento que describe los asuntos de seguridad de red de una organización. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

Una organización puede tener muchos sitios y cada uno contar con sus propias redes. Si los sitios están conectados por una red interna, la política de red deberá agrupar las metas de todos los sitios que estén interconectados.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos relacionados con la red; por ejemplo,

- Estaciones de trabajo.
- Computadotas anfitrión y servidores.
- Dispositivos de interconexión (enrutadores, puentes, repetidoras, etc).
- Software para red y aplicaciones.
- Cables de red.
- Información en archivos y bases de datos.

La política de seguridad del sitio debe tomar en cuenta la protección de estos recursos.

Al crear una política de seguridad, se debe saber cuáles recursos de la red vale la pena proteger, y entender que algunos son más importantes que otros. Para ello, es importante tener muy claros los siguientes puntos:

- ¿Qué se necesita proteger?
- ¿De quién debe ser protegido?
- ¿Cómo protegerlo?

Se debe evitar llegar a una situación donde se gaste más para proteger aquello que es menos valioso.

Otro de los puntos importantes que debe ser considerando dentro de una politica de seguridad de red, es el acceso no autorizado; y se refiere a que sólo se permita el acceso a los recursos a usuarios autorizados. Para ello, puede hacerse una lista de los usuarios que requieren ingresar a los recursos de la red; los cuales, normalmente se organizan en grupos, para identificar qué recursos requieren usar de acuerdo a las funciones que desempeñan dentro de la organización.

El siguiente paso será proveer guías para el uso aceptable del recurso, éstas dependerán de la clase de usuario y por lo tanto de sus normas. La política debe establecer qué tipos de uso de red es aceptable e inaceptable, y qué tipo de uso será restringido. Si el acceso a un recurso se restringe, se deberá considerar el nivel de acceso que tendrán las diferentes clases de usuarios.

Finalmente, es importante también aqui cuidar el aspecto de las contraseñas seguras; ya que si éstas no son seguras, la cuenta y el sistema son vulnerables. Por tal motivo, se deberá tener una política para inhabilitar total o parcialmente las cuentas que nunca se han usado durante cierto tiempo. Si el sistema lo permite, se deberá forzar a los usuarios a cambiar las contraseñas en el primer registro. Muchos sistemas tienen la política de caducidad de contraseña, lo cual puede ser útil para protegerlas.

Cuando ocurren las amenazas a la seguridad de la red, el administrador del sistema podrá examinar los directorios y archivos privados del usuario para el diagnóstico del problema hasta cierto límite estipulado por la política del sistema o red.

Al término de este capítulo, el lector tiene un panorama más completo de lo que implica el problema de la seguridad en las redes de comunicación; así como de los factores implicados en el tema. Se ha explicado que a una red la forma todo un entorno de elementos de cómputo, los cuales a su vez pueden presentar diferentes tipos de amenazas. Se explicó también el modo en que trabaja el protocolo TCP/IP, ya que es por medio de éste, que está organizada la comunicación entre redes a nivel Internet.

Además del planteamiento de los riesgos que pueden existir en una red de comunicación, también fueron revisadas sus posibles soluciones o métodos para tratar dichas amenazas; tener siempre localizados la mayoría de los posibles problemas, es algo que debe tratar de implementarse; así como tener la posibilidad de verificar cualquier uso de la red.

Se concluyen entonces a continuación algunas reglas para evitar intromisiones:

- Mínimos espacios por donde salir o entrar.
- Mínimos recursos accesibles desde fuera.
- Mínima importación de datos con posibilidad de robo, sin encriptar.
- Máximos controles posibles entre la red interna y el exterior.

Finalmente, se planteó la importancia de las políticas de seguridad en redes, para lo cual se enfatizó en la identificación plena de los elementos a proteger; así como la revisión constante de la política de seguridad, para evitar que ésta sea violada y pudiera llevar incluso a la negación del servicio en un caso grave de intromisión.

La política de seguridad, debe estar diseñada de tal manera que sea posible corregirla para adecuarla en el momento que sea necesario; ya que si es demasiado restrictiva o no está bien explicada, es muy posible que sea violada.

CONCLUSIONES

Como se ha podido apreciar a lo largo de este trabajo, el tema de la seguridad de la información, cobra valor en diferentes situaciones, en virtud de que es innegable la importancia general y creciente del tratamiento de la información para el funcionamiento e incluso para la supervivencia de cualquier organización, sea pública o privada. Como la información es inmaterial, necesita de soporte que adoptan muchas formas:

- Puede almacenarse en sistemas informáticos.
- Puede transmitirse a través de redes.
- Puede registrarse en papel, discos u otros medios de almacenamiento transportables.
- Puede transmitirse o registrarse en conversaciones habladas.

Independientemente del medio por el que sea transmitida o almacenada la información, lo que se pretende es combatir las amenazas a su seguridad o limitar su impacto sobre los activos de la organización, al tiempo que se permite la necesaria agilidad en la compartición de datos y recursos.

Las funciones, servicios y mecanismos de seguridad, requieren en general, el concurso de una serie de medidas, las cuales se pueden clasificar como:

- Medidas administrativas/organizativas de los sistemas. Publicación de normas de uso adecuado, u otros medios apropiados. Deben definirse claramente las áreas de responsabilidad de usuarios, administradores y directivos.
- Medidas Legislativas. Deben preverse sanciones para aquellos en que la prevención no sea técnicamente posible o conveniente.
- Medidas técnicas. Se refieren esencialmente a la criptografía.

Está claro que las precauciones con la información, deben ser tomadas desde los niveles más bajos de una organización; y que sea cual sea el nivel de almacenamiento, deben realizarse copias de seguridad, como una de las principales medidas, y que preferentemente, los respaldos deben estar organizados en un procedimiento operativo de seguridad, que defina puntos clave, tales como:

- Niveles de periodicidad.
- Procedimiento de recuperación de información.
- Control de almacén de respaldos.
- Máquinas de respaldo, etc.

Se hizo notable también el papel que juega la seguridad dentro del sistema operativo que se usa, porque éste es el encargado de administrar los recursos del equipo y sus procesos internos. Con la revisión de este tema, poco a poco se van complementando los primeros conceptos vistos, ya que en este punto se está tratando la seguridad tanto física como lógica de la información.

Con respecto a los servicios de Internet; está visto que el enviar datos por la red, se convierte en una amenaza a la seguridad de la información. Esta amenaza se convierte en ataque, pudiendo atender a las siguientes categorías:

- Análisis de tráfico: Consiste en la captura de todo tráfico que pasa por la red.
- Interrupción: Cuando un recurso del sistema es destruido o se vuelve no disponible.
- Intercepción: Una entidad no autorizada consigue tener acceso a la información.
- Modificación: Una entidad no autorizada consigue tener acceso a la información, y la manipula.
- Fabricación: Una entidad no autorizada inserta información, modificando así la original.

Para evitar este tipo de intromisiones, se dieron algunas medidas, tales como el uso de la criptografía y la implementación de cortafuegos, cuya misión principal es mantener protegida y distanciada la red interna, del exterior.

Cabe señalar la importancia que tiene identificar incluso los recursos de red que deben ser considerados al estimar las amenazas a la seguridad general:

- Hardware: Procesadores, tarjetas, terminales, líneas de comunicación, enrutadores, etc.
- Software: Programas fuente, programas objeto, utilerías, programas de comunicación, sistemas operativos, etc.
- Datos: Durante la ejecución, almacenados en línea, bitácoras de auditoria, bases de datos, en tránsito sobre medios de comunicación, etc.
- Gente: Usuarios, personas para operar sistemas.
- Documentación: Sobre programas, hardware, sistemas, procedimientos administrativos locales.
- Accesorios: Papel, formas, cintas, información almacenada.

Con la finalidad de lograr mejores resultados en el uso de medidas de seguridad, es importante el manejo de políticas de seguridad. Cabe señalar que tanto las políticas de seguridad en el acceso, como los sistemas de encriptamiento, dependen en gran medida de la habilidad que se tenga para implementarlos, este hecho es incluso más relevante que el costo de los equipos que se utilicen para desarrollar el sistema de seguridad. Una prueba notable al respecto es que el auge del comercio electrónico ha obligado a las empresas que dependen sustancialmente de esta clase de negocios, a replantear las políticas de conexiones seguras y de métodos de autenticación, cada vez más complejos y confiables.

Debido también a la globalización que ha tenido Internet , los ataques a redes privadas se han incrementado a tal punto que en el momento se puede decir que es casi de uso obligatorio la implementación de cortafuegos y/o servicio de proxy entre la Intranet e Internet.

Con base a lo visto aquí, se puede deducir que no se debe dar más importancia a la seguridad externa que a la interna; ya que la divulgación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza; de nada servirá tener un cortafuegos perfectamente configurado, si los usuarios hacen lo que quieren entre ellos.

Finalmente, en conclusión, el objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas, o de la información contenida en ellos; así como tratando de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública.

Con todo lo aprendido a lo largo de este trabajo, es posible ahora percibir la gran relevancia del tema de la seguridad informática, y que es propia responsabilidad aplicar los conceptos; así como investigar cuáles son los últimos problemas de seguridad reportados.

BIBLIOGRAFÍA

- Administración UNIX,
  Jean-Luc Montagnier,
  Ed. Ediones Gestión 2000, S. A.

- Building Internet Firewalls,
  B. Chapman and E. Zwicky,
  O'Reilly and Associates, 1995.

- Computer Security,
  J. Carroll, 2nd Edition,
  Butterworth Publishers, 1987.

- Data Encryption Standard,
  Federal Information Processing Standard (FIPS) publication 46,
  National Bureau of Standards, U.S. Department of Commerce, Washington, DC
  (January 77).

- Differencial Cryptoanalysis of the Dta Encryption Standard,
  Biham, E. y Shamir, A. ,
  Ed. Springer-Verlag, 1993.

- Improving the Security of Your UNIX System,
  D. Curry, SRI International Report
  April 1990.

- Introducción a los sistemas operativos,
  Hrvey M. Deitel,
  Addison Wesley Iberoamericana, Segunda Edición.

- Introducción a la seguridad,
  D. Andina, Madrid, España,
  Febrero 1998, pp. 217-231.

- Network Security PRIVATE Communication in a PUBLIC World,
  C. Kaufman, R. Perlman, and M. Spencier,
  Prentice Hall, 1995.

- Operating Systems Concepts,
  Silberschatz, A., y Galvin, P.
  Addison-Wesley, 1998.

- Operating Systems: Design and Implementation,
  Tanenbaum, A. S., y Woodhull, A. S.
  Prentice Hall, 1997.

- PGP: Pretty Good Privacy,
  S. Garfinkel
  O'Reilly and Associates, 1996.

- Practical Unix Security,
  Simson Garfinkel, and Gene Spafford,
  O'Reilly and Associates, 1991.

- Sistemas Operativos,
  Deitel, Harvey
  Addison-Wesley Publishing, Cap. 7, 1998.

- Sistemas Operativos,
  Rueda Francisco,
  Mc Graw Hill.

- Sistemas Operativos Conceptos Fundamentales,
  Abraham Silberschatz, James L. Peterson, Peter B. Galvin,
  Addison-Wesley Iberoamericana.

- Sistemas Operativos Conceptos y Diseño,
  Milenkovic Milan,
  Mc Graw Hill.

- Sistemas Operativos Diseño e Implementación,
  Andrew S. Tanenbaum,
  Prentice Hall, 1991.

- Sistemas Operativos Modernos
  Andrew S. Tanenbaum,
  Prentice Hall, 1991.

- Seguridad en UNIX,
  Manuel Mediavilla Mauriz.
  Ed. Ra-Ma.

- Seguridad en UNIX: Internet y Sistemas Abiertos,
  Ribagorda, Calvo Gallardo
  Paraninfo 1996.

- Seguridad y protección de la información,
  J. Luis Morant Ramon,
  Ed. Centro de Estudios Ramón Areces.

- Unix Security: A Practical Tutorial,
  Arnold
  Mc Graw Hill, 1993.

- Unix System Security,
  Rick Farrow,
  Addison-Wesley.

- Unix System Security: A Guide for Users and Systems Administrators,
  D. Curry
  Addison-Wesley, 1992.

REFERENCIAS DE INTERNET

- http://andercheran.aiind.upv.es/toni/unix/index.html#docs
- http://kriptopolis.com/
- http://penta.ufrgs.br/gereseg/node7.htm
- http://segurinet.com/gsal/default.htm
- http://www.comnet.mex/segtecno.htm
- http://www.gratisweb.com/ivanherrera/redes.htm
- http://www.iec.csic.es/criptonomicon/info.html
- http://www.iec.csic.es/criptonomicon/mecanism.html
- http://www.linux-es.com/que_es.html
- http://www.nalejandria.com/axioma/logaritmos/historia.htm
- http://www.ugr.es/~aquiran/cripto/pgp02.htm