UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DE SEGURIDAD EN LAS REDES DE DATOS DEL NEGOCIO BANCARIO Y ENTIDADES FINANCIERAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO ELECTRÓNICO

PRESENTADO POR:

MANUEL ANTONIO DIAZ RICALDE

PROMOCIÓN
1989 – II

LIMA – PERÚ
2002

Al Señor del Santuario de Santa Catalina. Por alumbrarme día a día, a mi Madre Margarita por su Amor y Comprensión; a mi hermana Luisa y a mis sobrinos: Jonathan, Angelo y Elizabeth por el Aliento Constante.

Manuel.

SISTEMA DE SEGURIDAD EN LAS REDES DE DATOS DEL NEGOCIO BANCARIO Y ENTIDADES FINANCIERAS

SUMARIO

El presente Informe de suficiencia da a conocer las amenazas a la seguridad en redes de transmisión de datos de las entidades financieras y bancarias, así como los servicios de seguridad requeridos y los mecanismos necesarios para proveer estos servicios. También se introducen algunos de los algoritmos y aplicaciones criptográficas más extendidos en la actualidad y de mayor utilización en los próximos años.

La Criptología es el mecanismo más usado en los procesos de protección de datos, como las transacciones bancarias por Internet, el correo electrónico cifrado, etc., en su camino entre el emisor y el receptor.

ÍNDICE

CAPÍTULO IV

SOLUCIÓN DEL PROBLEMA PLANTEADO 17

PRÓLOGO

Como inicio del presente informe "SISTEMA DE SEGURIDAD EN LAS REDES DE DATOS DEL NEGOCIO BANCARIO Y ENTIDADES FINANCIERAS" , pretendo hacer comprender el problema de la seguridad en las redes de transmisión de datos como por ejemplo Internet. En el desarrollo del informe nos centraremos en la seguridad en la comunicación a través de redes de área local, área extendida o redes metropolitanas, redes virtuales privadas y redes de área extendida especialmente Internet, que consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de datos, más que en la seguridad en los computadores, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, más que físicos.

En el capítulo I pretendo hacer comprender las causas de la inseguridad en las redes de datos, como así también los beneficios de un sistema de seguridad y en el capítulo II los

objetivos y alcance del informe, la descripción socio-económico en el Perú del uso del comercio electrónico y acceso a internet.

En el Capítulo III tratamos del planeamiento de ingeniería del proyecto donde se describe lo que vamos ha proteger y contra quién se debe proteger. En el capítulo IV se describe los conceptos generales de la comunicación segura en las redes de datos de las entidades financieras y bancarias, se analizan los diferentes tipos de dispositivos de interconexión de redes que se dividen genéricamente en cuatro categorías: repetidores, puentes, enrutador y pasarela. Cada uno esta asociado a uno o varios de los niveles OSI. También el objetivo del desarrollo de una política de seguridad que es prevenir incidentes de seguridad y en el análisis de riesgos involucramos la determinación de qué se necesita proteger, qué se necesita para protegerlo y cómo. En el capítulo V nos introducimos en la ciencia de la criptografía, que estudia la ocultación, disimulación o cifrado de la información, utilizada en las entidades financieras y bancarias, una de las herramientas más utilizadas para proteger la información es la tecnología criptográfica en la cual desarrollamos en el capítulo VI, permite cifrar los mensajes mediante una o varias llaves para que estos no puedan ser interpretados, a menos que se realice un proceso inverso o

descifrado, que requiere volver a utilizar las llaves. En el capítulo VII se hace una descripción de los protocolos que existen actualmente para ofrecer distintos niveles de seguridad. Además, se resalta especial hincapié en el modelo de seguridad basado en redes privadas virtuales, que es actualmente uno de los mecanismos más avanzados de seguridad corporativa en las entidades financieras y bancarias. También realizamos una explicación sencilla de las diferencias entre los cortafuegos y los proxys, que son bastante confundidos por los usuarios en general.

Me queda agradecer a todos los que facilitaron la tarea de esclarecer las dudas y ofrecieron su valioso tiempo, para explicar aquellos aspectos confusos que tenía.

En primer lugar para el Profesor Ingeniero ALFREDO RODRÍGUEZ GUTIERREZ, que me sugirió el tema y orientó en el desarrollo del Informe de Suficiencia.

A Todos los Profesores Ingenieros del segundo programa de Titulación Profesional por Actualización de Conocimientos, que alentaron a transformar apuntes de clases, para aplicar en la actividad laboral actual en que desarrollo y facilitar, bibliografías importantísimas para el desarrollo del Informe de Suficiencia.

Al Decano de nuestra facultad de Ingeniería Eléctrica y Electrónica, Ingeniero CARLOS MEDINA RAMOS, un profundo agradecimiento por liderar esta forma de graduarse.

CAPÍTULO I

INTRODUCCIÓN

1.1 Generalidades

Todos somos conscientes que los nuevos avances tecnológicos aplicados en los sistemas de Información y telecomunicaciones, constituyen uno de los acontecimientos más importantes del presente siglo como por ejemplo el desarrollo de la red de redes llamado Internet. En los años 70s y 80s, las redes consideradas como importantes y grandes eran las redes privadas de negocios como las de los bancos, cadenas de supermercados, empresas de tecnología como la red mundial de IBM, y la gran mayoría usaba protocolos propietarios principalmente como el SNA (System Network Arquitecture) de IBM, y la arquitectura de redes Burroughs (Burroughs Networks Architecture BNA) de Unisys entre otros.

A comienzos de los años 80s, un intento de estandarización llevó a que se diseñe la arquitectura y los protocolos OSI (Open System Interconnection), pero nunca fue exitoso. Ha sido realmente el mercado y las necesidades de negocio, que exigían compartir e intercambiar información

entre todas las entidades financieras, bancos, proveedores, vendedores y consumidores, los que escogieron desde los años 90s a la red de Internet; y por ende su protocolo TCP/IP, debido a que las redes de comunicación actuales permiten la conectividad de un gran número de usuarios que pueden estar situados en cualquier parte del mundo, tanto para transmisión de voz (red telefónica), imágenes (redes de distribución de televisión, TV vía satélite) como para la trasmisión de datos entre computadoras (redes locales, metropolitanas, así como redes a nivel mundial, como por ejemplo Internet). La explosión de servicios ofrecidos por estas redes, especialmente las de datos (en realizar transferencia de nuestras cuentas de bancos y programas de servicio o nos conectamos a un portal y realizamos compras con toda seguridad, facilidad, fiabilidad y transparencia), ha incrementado la dependencia de individuos y organizaciones de la trasmisión de datos por estas redes. Hoy en día el negocio de las entidades financieras, depende en gran medida de la seguridad de sus sistemas, hasta tal punto de que si los sistemas se detienen, se detiene el negocio, y eso es algo que ninguna entidad financiera puede permitir, por lo que es un costo demasiado alto.

1.2 Antecedentes

La seguridad tiene su nacimiento con la aparición de ataques a los datos por parte de intrusos. El flujo oportuno y exacto de los datos es fundamental en las entidades financieras y bancarias para realizar sus negocios diarios. Necesitan saber que los datos son auténticos, que tienen su origen y son recibidos por partes válidas y que no están disponibles para observadores no autorizados. La seguridad de la red de datos pueden entenderse como la capacidad de una red o un sistema de información para resolver, con un determinado nivel de confianza, los efectos de accidentes o actos malintencionados.

1.2.1 Causas de la Inseguridad en las redes de datos

Pensar en que a mayor complejidad del sistema de seguridad, obtenemos mayor seguridad, tener la idea de que se está totalmente protegidos con la asignación de contraseñas a todos los recursos, usuarios funcionales y aplicaciones, o comprar un equipo seguro (firewall), suponer que los usuarios funcionales o posibles atacantes tienen bajo conocimiento. El crecimiento acelerado de las redes empresariales y particularmente el crecimiento de Internet, aunado a que el diseño de las redes se asumía en ambientes

seguros controlados a través de usuarios autorizados y sin vulnerar la futura conexión a redes externas.

1.2.2 Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que la las entidades financieras trabajan sobre una plataforma confiable, que se refleja en:

a. Aumento de la productividad.
b. Aumento de la motivación del personal.
c. Compromiso con la misión de la organización.
d. Mejora de las relaciones Laborales.
e. Ayuda a formar equipos competentes.
f. Imagen.

CAPÍTULO II

OBJETO Y ALCANCE DEL ESTUDIO

2.1 Objetivos

Los objetivos que persigue este proyecto son:

a. Asegurar resultados eficaces en la toma de decisiones para la implementación de sistemas de seguridad o la revisión de los existentes frente a las amenazas contra la privacidad e integridad de los sistemas de comunicaciones y los datos.

b. Contribuir al conocimiento y desarrollo de la cultura informática y en salvaguarda de los sistemas y datos activos importante para las entidades financieras.

c. Examinar los nuevos medios de comunicación, sistemas y tecnologías para la prevención de todo tipo de ataque, al mismo tiempo, generar un verdadero cambio de actitud y aptitud en la Alta Dirección y en el nivel Gerencial de las entidades financieras hacia el resguardo de personas y bienes.

2.2 Alcance del Proyecto

El desarrollo del Informe alcanza a Directores, Gerentes de sistemas y telecomunicaciones, administradores de redes, áreas de soporte técnico y desarrollo, consultores, profesionales técnicos y profesionales en redes y telecomunicaciones. Con la finalidad de brindarles ciertos conocimientos en la aplicación de políticas y herramientas de seguridad en las redes de datos de las entidades financieras y bancarias.

2.3 Descripción socio económico

La siguiente información se ha obtenido del diario el Comercio del viernes 20 de septiembre del 2002. La Cámara de Comercio de Lima estima que durante el próximo año el comercio electrónico en el Perú movilizará alrededor de 160 millones de dólares, cifra muy superior a los 50 millones que se transaban por Internet entre los años 1999 y 2000. Asimismo, se prevé que existen alrededor de 13 mil personas que utilizan Internet como un medio para hacer transacciones comerciales, nivel que representa el 1% del total Latinoamericano. Estas cifras se corroboran con el hecho de que el mercado peruano cuenta con una base de computadoras del orden de los 893 mil equipos y alrededor de 1.4 millones de ínter nautas, se estima que con la introducción de la firma y

los certificados digitales, cuyo fin principal es el de dotar de seguridad a los intercambios comerciales y societarios en el ciberespacio, la cifra de penetración del Internet y del e-comercie, antes descritas, se multipliquen en un breve plazo.

También la siguiente información se ha obtenido de la revista PC World del 18 de septiembre del 2002. En sus estudios, la empresa Dominio Consultores estima que existirían, hasta agosto de este año, 2,3000,000 usuarios de Internet en el Perú. En el caso de Lima Metropolitana, Apoyo Opinión y Mercado calcula que 1,740,000 de personas acceden a la Red, en un rango de 12 a 50 años de edad. De acuerdo con su estudio "Usos y Actividades hacia Internet" aplicado a una muestra de 600 ínter nautas, el 7% efectuó alguna vez una compra en línea. El 64% lo hizo desde una página local y utilizando una tarjeta de crédito 43%. Entre las principales razones para no comprar electrónicamente se citaron la falta de interés un 29%, la desconfianza en el medio 18% y no tener una tarjeta de crédito 13%.

CAPÍTULO III

PLANEAMIENTO DE INGENIERÍA DEL PROBLEMA

La intimidad es un derecho constitucional del individuo, que con los medios de comunicación tradicionales, como el correo postal, correo certificado, los apartados de correo, etc., están más que garantizados. En cambio, con el uso generalizado de los sistemas de comunicación electrónicos, la intimidad y el anonimato de las personas resultan crecientemente amenazadas, de hecho no hay seguridad alguna en caso de no utilizar algún tipo de medio para preservar esta intimidad de agentes externos.

3.1 ¿Qué queremos proteger?

Los tres elementos principales a proteger en cualquier sistema de redes son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de la red como equipos de conectividad, comunicaciones, procesamiento, almacenamiento, cableado. El software es el conjunto de programas lógicos que hace funcional al hardware, tanto sistemas operativos como

aplicaciones, y por datos el conjunto de información lógica que maneja el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas a una base de datos. Habitualmente los datos constituyen el principal elemento de los tres a proteger ya que es el más amenazado y seguramente el más difícil de recuperar. Las amenazas a la seguridad en redes de trasmisión de datos en las entidades financieras pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como puede ser un usuario, o fichero, a un destino, que pudiera ser otro usuario o fichero.

3.2 Tipos de ataques

Podríamos definir como ataques todas aquellas acciones que supongan una violación de la confidencialidad, integridad o disponibilidad de nuestro sistema de comunicaciones y dichas acciones las podemos clasificar de modo genérico según los efectos causados:

a. Interrupción:

Un recurso del sistema es destruido o se vuelve no disponible. Éste es un ataque contra la disponibilidad. Ejemplos de este ataque son los Nukes, que causan que los equipos queden fuera de servicio. También la destrucción o sabotaje de un elemento hardware, y la línea de comunicación.

b. Intercepción:

Un usuario no autorizado consigue acceso a un recurso. Éste es un ataque contra la confidencialidad. Ejemplos de este ataque son la obtención de datos mediante el empleo de programas troyanos o la copia ilícita de archivos o programas, o bien la lectura de las cabeceras de paquetes de datos para conocer la identidad de uno o más de los usuarios mediante el Spoofing o engaño implicados en la comunicación intervenida.

c. Modificación:

Un usuario no autorizado no sólo consigue acceder a un recurso, si no que es capaz de manipularlo, este es un ataque contra la integridad. Ejemplos, son la modificación de cualquier tipo en fichero de datos, alterar un programa para que funcione de forma distinta y modificar el contenido de información que esté siendo transferida por la red.

d. Fabricación:

Un usuario no autorizado inserta objetos falsificados en el sistema, es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir datos a un fichero. Asimismo estos ataques se pueden clasificar en términos de ataques pasivos y ataques activos.

d.1 Ataques activos:

Estos ataques implican algún tipo de modificación de los datos o la creación de falsos datos: Suplantación de identidad, Modificación de mensajes, Web Spoofing.

d.2 Ataques pasivos:

En los ataques pasivos el atacante no altera la comunicación, si no que únicamente la escucha o monitoriza, para obtener de esta manera la información que está siendo transmitida. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos.

e. Autenticación:

Consisten, en la suplantación de un usuario del sistema o de la red. Se realiza de dos formas: obteniendo el nombre y contraseña del atacado o suplantando al usuario una vez ésta ya ha iniciado una sesión en su sistema. Para realizar ataques de este tipo se utilizan varias técnicas, las cuales pasamos a describir a continuación.

e.1 Simulación de Identidad:

Es una técnica para hacerse con el nombre y contraseña de usuarios autorizados de un sistema. El atacante instala un programa que recrea la pantalla de entrada al sistema, cuando el usuario intenta entrar en él teclea su login y contraseña, el programa los captura y muestra una pantalla de “error en el

acceso" al usuario. El usuario vuelve a teclear su login y contraseña, entrando esta vez sin problemas. El usuario cree que en el primer intento se equivocó al teclear, sin embargo, su login y contraseña han sido capturada por el atacante.

e.2 Engaño:

Conocido también como spoofing, consiste en sustituir la fuente de origen de una serie de datos, por ejemplo un usuario adoptando una identidad falsa para engañar a un cortafuego o filtro de red. Los ataques Spoofing más conocidos son el IP Spoofing, el DNS Spoofing , el Web Spoofing y el fake-mail.

e.3 Bucle (Looping):

El intruso usualmente utiliza algún sistema para obtener información e ingresar en otro, que luego utiliza para entrar en otro, y así sucesivamente. Este proceso se llama looping y tiene como finalidad hacer imposible localizar la Identificación y la ubicación del atacante, de perderse por la red.

e.4 Diccionario:

Los Diccionarios son programas que en su base de datos contienen millones de palabras. Van probando con millones de combinaciones de letras y números cifrados, incluso con caracteres especiales hasta descubrir la combinación correcta de la contraseña del usuario o sistema.

CAPÍTULO IV

SOLUCIÓN DEL PROBLEMA PLANTEADO

4.1 Teoría de la comunicación en las redes de datos

4.1.1 Definición

Las redes de transmisión de datos son aquellas en las cuales los usuarios tienen un canal en el que están conectados, e intercambian información si y solo si son usuarios pertenecientes a la red. El objetivo de las redes en general es compartir recursos, y unos de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. El otro objetivo es el ahorro económico porque los pequeños computadores tienen mejor relación costo/rendimiento, comparadas con la ofrecida por los computadores grandes o mainframe.

4.1.2 Aplicaciones

Las redes de datos permitieron y permitirán una gama muy amplia de servicios y necesidades tanto persona a

persona como persona a entidades financieras o empresas y viceversa, aplicaciones que van desde acceso a información remota vía transferencia de archivos, correo electrónico, pagos en entidades bancarias de servicios varios (agua, luz, teléfono, etc.) hasta compras de inmuebles. Muchas de estas aplicaciones requieren de equipos y programas muy eficientes y de altas prestaciones sin mencionar la infraestructura física de transporte como redes de fibra óptica, microondas y cobre necesarias para la interconexión.

4.1.3 Elementos de comunicación

Los elementos que integran un sistema de Comunicación son cuatro.

a. Mensaje o Fuente:

Son los datos que transmitimos, puede ser analógica o digital. Lo importante es que llegue íntegro y con fidelidad.

b. Emisor:

Sujeto que envía el mensaje. Prepara los datos para enviar por el canal, tanto en calidad es decir adecuación a la naturaleza del canal como en cantidad amplificando la señal.

c. Canal o Medio:

Es el elemento a través del cual se envía los datos del emisor al receptor.

d. Receptor:

Tendrá que demodular la señal, limpiarla y recuperar de nuevo el dato original.

4.1.4 Dispositivos de interconexión

Los dispositivos de interconexión son:

a. Módem:

Un Módem es un dispositivo que convierte la señal digital en señal analógica y viceversa para posibilitar que el mensaje enviado por un equipo terminal de datos (DTE) pueda llegar a otro(s) DTE's a través de líneas análogas.

b. Concentradores:

Dispositivo que permite un almacenamiento temporal de datos procedentes de canales de baja velocidad y su retrasmisión por canales de alta velocidad, y viceversa, se dividen en:

b.1 Concentradores Analógicos:

Dispositivo que permite la comunicación entre un módem, conectado a un puerto de una computadora y varios módems conectados a DTE's en aplicaciones que usan protocolos de sondeo/selección. Con este tipo de concentrador, podemos bajar los costos de las líneas de comunicación. El concentrador análogo es el encargado de crear un equilibrio eléctrico entre los distintos enlaces.

b.2 Concentradores Digitales:

También llamados Port-Sharing Devices, permiten que varios DTE's compartan un módem o un puerto de computador en aplicaciones que usan protocolos de sondeo/selección. Con este tipo de concentrador podemos ahorrar, dependiendo de como lo conectemos, puertos de un procesador de comunicaciones, o modems requeridos para una conexión.

c. Multiplexores:

Dispositivos que permiten la combinación de varios canales de datos en un circuito físico, y se dividen en:

c.1 Multiplexor por División de Frecuencia:

Divide el ancho de banda de una línea entre varios canales, donde cada canal ocupa una parte del ancho de banda de frecuencia total.

c.2 Multiplexor por División de Tiempo:

Cada canal tiene asignado un periodo o ranura de tiempo en el canal principal y las distintas ranuras de tiempo están repartidas por igual en todos los canales. Tiene la desventaja de que en caso de que un canal no sea usado, esa ranura de tiempo no se aprovecha por los otros canales, enviándose en vez de datos bits de relleno.

c.3 Multiplexor por División de Tiempo Estadísticos:

No le ofrece anuras de tiempo a los canales inactivos y además podemos asignar prioridades a los canales.

d. Procesador de Comunicaciones:

Equipo cuya función principal consiste en reducir la carga de trabajo de comunicaciones del computador central. Regula la comunicación tanto local como remota desde y hacia el computador central. Los Procesadores de Comunicación cargan, su propio sistema operativo desde una unidad de almacenamiento secundaria instalada en su interior o en un computador central y es un nodo más en la red.

e. Hubs:

Dispositivos que unen grupos de computadores y permiten su comunicación.

f. Repetidores:

Dispositivos que generan la señal de un segmento de cable y pasan estas señales a otro segmento de cable sin variar el contenido de la señal. Son utilizados para incrementar la longitud entre conexiones en una LAN.

g. Puentes:

Consiste en un equipo que contiene dos puertos de comunicación, crea unas tablas en memoria que contienen todas las direcciones de MAC (direcciones de las tarjetas de comunicaciones), de ambos extremos, de tal manera que restringen el trafico de datos de un segmento a otro, no permitiendo el paso de tramas que tengan como destino una dirección del mismo segmento al que pertenece la estación de origen. Es conveniente el uso de los mismos cuando

requerimos la interconexión de dos redes locales o remotas, también se les conoce como bridges.

h. Enrutador:

Conocido como router, son dispositivos que nos permiten unir varias redes, tomando como referencia la dirección de red de cada segmento. Al igual que los bridges, los Routers restringen el trafico local de la red permitiendo el flujo de datos a través de ellos solamente cuando los datos son direccionados con esa intención. Muchos routers comerciales proporcionan la capacidad de seleccionar paquetes con base a criterios como el tipo de protocolo, los campos de dirección de origen y dirección de destino para un tipo particular de protocolo y los campos de control que son parte del protocolo. A estos routers se les llama routers de selección.

i. Conmutador:

Divide la red de área local en varios segmentos limitando él tráfico a uno o más segmentos en vez de permitir la difusión de los paquetes por todos los puertos. Dentro del conmutador, un circuito de alta velocidad se encarga del filtrado y de permitir él tránsito entre segmentos de aquellos segmentos que tengan la intención de hacerlo.

j. Compuerta:

También se conoce como pasarela de enlace o gateway. Una pasarela es un programa o dispositivo de comunicaciones

que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes. Permite la comunicación entre protocolos diferentes (por ejemplo, redes NetWare y no NetWare) utilizando protocolos estándares de la industria tales como TCP/IP, X.25 o SNA. Las pasarelas o gateway se colocan entre dos sistemas y convierten las solicitudes del emisor a un formato que puede ser entendido por el receptor.

4.1.5 Protocolos

Al intercambio de información entre computadores se le llama comunicación entre computadores. Al conjunto de computadores que se interconectan se le llama red de computadores. Para la comunicación entre dos entidades financieras situadas en sistemas diferentes, se necesita definir y utilizar un protocolo. Un protocolo es una serie de códigos y formatos que se utilizan para que los computadores se entiendan entre sí. Las tareas que definen un protocolo son: la sintaxis (formato de los datos y niveles de señal), Todas estas tareas se subdividen en niveles y a todo se le llama arquitectura del protocolo. Cada nivel está auto contenido, y sólo se ocupa de la interfaz con los niveles inmediatamente superior e inmediatamente inferior. Este diseño por niveles divide los protocolos de comunicación en zonas funcionales manejables que permiten que los vendedores de hardware y

software creen productos que puedan trabajar con los de otros vendedores a cualquier nivel deseado.

4.2 Arquitectura en niveles del modelo OSI

4.2.1 Definición

La organización internacional de normalización ISO (Internacional Organisation for Standarisation) ha generado un protocolo de siete niveles conocido como la norma ISO-7494 que define el modelo de interconexión de sistemas abiertos (OSI, Open System Interconnection). El proceso de intercomunicación entre dos computadores es complejo y difícil de entender en su totalidad, son muchos los elementos que intervienen en el esquema de intercambio de datos entre equipos diferentes. Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO divide el modelo de referencia OSI en niveles, entendiéndose por "nivel" una entidad que realiza de por sí una función especifica. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. Como podemos ver en la figura 4.1.

4.2.2 Arquitectura en niveles

El modelo consiste en siete niveles, cada una de las cuales especifica funciones particulares de la red, como por ejemplo direccionamiento, control de flujo, control de errores, encapsulación y transferencia confiable de mensajes. El nivel superior (nivel de aplicación) es la más próxima al usuario; el nivel inferior (nivel físico) es la más próxima a la tecnología de medios. El nivel siguiente al nivel inferior está implementado en hardware y en software mientras que los cinco niveles superiores están implementadas únicamente en software.

4.2.3 Niveles OSI

a. Nivel 1 — Físico:

Define los procedimientos para establecer, mantener, y liberar las conexiones entre los circuitos eléctricos que están conectados por el medio de comunicación. También lleva a cabo el intercambio de señales eléctricas que representan los datos y la información de control. Incluye la especificación de las características mecánicas y eléctricas de la conexión física. Como ejemplo los dispositivos: El cable, conectores, tarjetas, y repetidores (hub); Y como protocolos RS-232, X21.

b. Nivel 2 — Enlace de datos:

Define los protocolos para enviar y recibir datos entre equipos conectadas directamente entre sí. Proporciona a los datos la sincronización de necesaria para delimitar el flujo de

bits del nivel físico. Asimismo, garantiza la identidad de los bits, encargándose de que los datos lleguen sin errores al equipo receptor. Algunos ejemplos los dispositivos que trabaja en este nivel son los puentes (bridges) y los protocolos son: HDLC, CSMA/CD (Ethernet), Testigo en anillo (802.5) y Testigo en bus (802.4).

c. Nivel 3 — Red:

Se definen los protocolos sin conexión que encaminan de forma dinámica los datos del usuario entre los sistemas de la red. Entre sus funciones se incluye el encaminamiento de los bloques de datos, la segmentación y posterior recomposión de los bloques de datos cuando sea necesario, la supervisión de los bloques de datos para asegurar una transmisión rápida. El dispositivo que trabaja en este nivel es el encaminador (router) y los protocolos se incluyen el protocolo de internet(IP) y el intercambio de paquetes entre redes (IPX, Internetwork Packet Exchange) de Novell.

d. Nivel 4 — Transporte:

En este nivel toma los datos del nivel de sesión y los divide en partes del tamaño del campo de datos de un paquete. Después pasa los bloques de datos al nivel de red. Proporcionando un servicio de transmisión y recepción de datos fiable a nivel de sesión. El dispositivo que trabaja en este nivel es la pasarela (gateway) y los protocolos más

usados son: el protocolo de control de la trasmisión (TCP: Transmisión Control Protocol) de internet, el intercambio secuencial de paquetes (SPX: Sequenced Packet Exchange) de Novell y NetBIOS/NetBEUI de Microsoft.

e. Nivel 5 — Sesión:

Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona un servicio fiable al nivel de presentación y tiene la capacidad de reestablecer una conexión en caso de que falle uno de los niveles más bajos de la jerarquía. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez. El dispositivo que trabaja en este nivel es la pasarela (gateway) y los protocolos: X.215 (ISO 8326) Servicio de Sesión y X.225 (ISO 8327) Especificación del Protocolo de Sesión .

f. Nivel 6 — Presentación:

Se encarga del formato de los datos, pero no de su significado. Proporciona un conjunto de servicios que se pueden usar en el proceso de intercambio de datos a través de la conexión de la sesión. El dispositivo que trabaja en este nivel es la pasarela(gateway). Los servicios en este nivel son: comprensión, traducción y cifrado de datos.

g. Nivel 7 — Aplicación:

Este nivel proporciona unos servicios estandarizados para poder realizar funciones especificas en la red. Las

personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero).

4.2.4 Comunicación entre niveles

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada nivel del modelo OSI en el origen debe comunicarse con su nivel igual en el lugar destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Las reglas y convenciones que controlan esta conversación se denominan protocolo del nivel "n", y controlan el formato y significado de las unidades de datos intercambiadas. Durante este proceso, cada protocolo de nivel intercambia información, que se conoce como unidades de datos de protocolo (PDU), entre niveles iguales. Cada nivel de comunicación, en el computador origen, se comunica con un PDU específico de nivel y con su nivel igual en el computador destino. También cada nivel de un modelo o arquitectura de red recibe servicios al nivel que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario, como podemos ver en la figura 4.2. A continuación

describo los servicios orientados a la conexión, sin conexión y servicios confiables.

a. Servicios orientados a la conexión:

La conexión es como un tubo a través del cual se envía la información de forma continuada, por lo que los mensajes llegan en el orden que fueron enviados y sin errores. Los pares en el nivel de red establecen en este caso conexiones con características como la calidad, el costo y el ancho de banda. La comunicación en este caso es duplex, y el control de flujo automático. Una analogía es el sistema telefónico.

b. Servicios sin conexión:

En el que cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continuada y el ruteo de cada mensaje es independiente. El servicio no es entonces confiable, pues se limita solamente a portar bits. En este caso el nivel de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

c. Servicios confiables:

Son aquellos en los que la transmisión de datos está controlada en cada momento, pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos.

Para ello el receptor envía acuses de recibo de las tramas recibidas a la emisora.

4.3 Arquitectura del modelo TCP/IP

4.3.1 Definición

Se llama TCP/IP (TCP: Transmisión Control protocol, e IP: Internet Protocol), es un protocolo de transporte de comunicaciones; esto es, un conjunto de reglas, convenciones y comandos para que las computadoras y los programas, no personas, puedan comunicarse desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio. Se compone de dos protocolos interrelacionados:

a. El protocolo TCP:

Funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

b. El protocolo IP:

Funciona en el nivel de red del modelo OSI, que nos permite encaminar los datos hacia otros equipos.

4.3.2 Características de TCP/IP

Las características del protocolo son:

a. Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación.
b. La comunicación no esta orientada a la conexión de dos equipos, eso quiere decir que cada paquete de datos es independiente, y puede viajar por caminos diferentes entre dos equipos.
c. La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
d. El uso de la red no impone ninguna topología en especial.

4.3.3 Niveles del modelo TCP/IP

El modelo TCP/IP está basado en la de conmutación de paquetes (packet switched), y tiene cuatro niveles: el nivel de aplicación, el nivel de transporte, el nivel de Internet y el nivel de red. Es importante observar que algunas de los niveles del modelo TCP/IP poseen el mismo nombre que los niveles del modelo OSI, aunque no se corresponden exactamente unas con otras, por lo que no deben confundirse. Ver Fig.4.3.

a. Nivel de aplicación:

En este nivel maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una solo nivel y da por sentado que estos

datos están correctamente empaquetados para la siguiente capa. Se incluyen protocolos destinados a proporcionar servicios tales como correo electrónico (smtp), transferencia de ficheros (ftp), conexión remota (telnet) y otros como http.

b. Nivel de transporte:

Permite que niveles pares emisor y receptor puedan conversar. El nivel de transporte se refiere a la calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza los servicios del nivel de red para proveer un servicio eficiente y confiable a los procesos del nivel de aplicación. En este nivel se produce la segmentación de los datos producidos en el nivel de Aplicación en unidades de menor tamaño, denominadas paquetes o datagramas (un datagrama es un conjunto de datos que se envía como un mensaje independiente), El nivel de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. simplemente considera que la comunicación entre ambos extremos está ya establecida y la utiliza.

c. Nivel de Internet o de red:

El propósito del nivel de Internet es enviar paquetes origen desde cualquier red y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. En este nivel se produce la

determinación de la mejor ruta y la conmutación de paquetes, durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino. Para poder enrutar los datagramas de la capa de Transporte, éstos de encapsulan en unidades independientes, en las que se incorporan diferentes datos necesarios para el envío, como dirección de origen del datagrama, dirección de destino, longitud del mismo.

d. Nivel de acceso a la red:

Uno de los principales elementos que maneja este nivel es el de las direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red, y que son el medio principal de localización de un host (cualquier computadora conectado a Internet, capaz de compartir información con otra computadora) dentro de una red. Cada tarjeta tiene un número identificador, cuyos 3 primeros bytes son asignados por el fabricante de la misma, mientras que los otros 3 se asignan de forma especial. Cuando un host debe enviar un paquete a otro de su red busca a éste mediante su número de tarjeta de red (dirección física).

4.3.4 Comparación de modelos OSI y TCP/IP

Si comparamos el modelo TCP/IP y OSI. Ver Fig.4.4, observaremos que ambos presentan las siguientes Analogías y diferencias:

a. Analogía:

Se dividen en niveles, tienen niveles de aplicación (aunque incluyen servicios muy Distintos), La tecnología es de conmutación de paquetes (no de conmutación de circuitos).

b. Diferencias:

OSI distingue de forma clara los servicios (lo que un nivel hace), las interfaces (como se pueden acceder a los servicios) y los protocolos (implementación de los servicios). TCP/IP no lo hace así, no dejando de forma clara esta separación. OSI fué definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente. TCP/IP combina las funciones del nivel de presentación y de sesión en el nivel de aplicación. TCP/IP combina el nivel de enlace de datos y el físico del modelo OSI en una solo nivel.

4.4 Encapsulamiento

Si el emisor desea enviar datos al receptor, en primer término los datos que se deben enviar se deben colocar en paquetes que se puedan administrar y rastrear a través de un

proceso denominado encapsulamiento. Los tres niveles superiores (aplicación, presentación y sesión) preparan los datos para su transmisión definiendo un formato común para la transmisión. Una vez pasados a formato común, el encapsulamiento, rodea los datos con la información de protocolo necesaria antes de que se una al transito de la red. Los tres niveles inferiores (red, enlace de datos, física) del modelo OSI son los niveles principales de transporte de los datos a través de una red interna o de Internet. A medida que los datos se desplazan a través de los niveles del modelo OSI, reciben encabezados(agregar la información correspondiente a la dirección), información final y otros tipos de información. Una vez que se envían los datos desde el origen, viajan a través del nivel de aplicación directo hacia los otro niveles. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales. Como muestra la figura 4.5, las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

a. Definir los datos (nivel de Presentación):

Cuando un usuario (emisor) envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer el conjunto de redes interconectadas.

b. Empaquetar los datos para ser transportados de extremo a extremo (nivel de Transporte):

Se dividen los datos en unidades de un tamaño que se pueda administrar, llamados segmentos, y se les asignan números de secuencia para asegurarse que los computadores receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por el conjunto de redes interconectadas. Al utilizar segmentos, la función de transporte asegura que el emisor y receptor del sistema de correo electrónico se puedan comunicar de forma confiable.

c. Agregar la dirección de red al encabezado (nivel de Red):

El siguiente proceso se produce en el nivel de red, que encapsula el segmento creando un paquete o datagrama, agregándole una dirección de red destino y origen, por lo general IP. Con esto, los datos se colocan en un paquete que contiene el encabezado de red con las direcciones lógicas de origen y destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

d. Agregar la dirección local al encabezado de enlace de datos (nivel Enlace de datos):

En el nivel de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (control de acceso al

medio de la tarjeta de red, única para cada tarjeta) origen y destino. Luego, el nivel de enlace de datos transmite los bits binarios de la trama a través de los medios del nivel físico. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de la red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

e. Transmitir el tren de bits creado. (nivel Físico):

Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, fibra óptica, etc.), Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el conjunto de redes interconectadas.

4.5 Servicios de seguridad

Para hacer frente a las amenazas a la seguridad de los datos se definen los servicios para proteger los sistemas de proceso de datos y de transferencia de información de las entidades financieras y bancarias. Estos servicios hacen uso de varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

a. Autenticación:

Requiere de una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Por ejemplo

la autenticidad se consigue mediante el uso de los certificados y firmas digitales en las transacciones electrónicas.

b. Confidencialidad:

Requiere que la información sea accesible únicamente por las entidades autorizadas. Por ejemplo la confidencialidad se consigue en las transacciones electrónicas con el uso de la criptografía. Se distinguen dos tipos de confidencialidad:

b.1 Confidencialidad de datos:

El cual está relacionada con el almacenamiento de los datos.

b.2 Confidencialidad del flujo de tráfico:

Se encuentra relacionada con el proceso de transmisión de datos. Se dan tres casos diferentes de confidencialidad de flujo: confidencialidad de un servicio orientado a la conexión, confidencialidad de un servicio no orientado a la conexión y servicio de confidencialidad de campo selectivo.

c. Integridad de datos:

Asegura que los datos que enviamos lleguen íntegros, sin modificaciones, a su destino final. Por ejemplo la integridad de datos se consigue combinando criptografía, funciones hash y firmas digitales.

d. No repudio:

Debemos estar seguros de que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar el haberlos recibido. Por ejemplo en una compra on-line debe garantizarse que una vez finalizada la misma ninguna de las partes (emisor y receptor) que intervienen pueda negar haber participado en ella. El no repudio se consigue mediante los certificados y la firma digital.

4.6 Políticas de seguridad

4.6.1 Definición

Una política de seguridad es un conjunto de normas, procedimientos y prácticas que regulan como las entidades financieras manejan, protegen y distribuyen los datos.

4.6.2 Características de la Políticas de Seguridad

a. Debe ser simple y entendible.
b. Debe estar siempre disponible.
c. Debe ser practicable y desarrollable.
d. Se debe hacer cumplir.
e. Debe ser estructurada.
f. Se establece como una guía.
g. Debe ser cambiante con la evolución tecnológica.

h. Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas como una unidad corporativa.

4.6.3 Elaboración de la Política de seguridad

Para la elaboración de la política de seguridad en las entidades financieras, el primer procedimiento es hacer una relación de los aspectos sensibles dentro de la organización, tanto físicos (equipos computo, comunicaciones, etc.), Como no materiales (aplicaciones, software, bases de datos, etc.), una vez realizada esta lista de puntos sensibles a proteger, se pondera cada uno de ellos con un peso específico, y se calcula la posibilidad de que sea vulnerado, ya sea por ataques intencionados o por causas meramente accidentales. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios con accesos a los recursos de acuerdo a las funciones a realizar. Las tres preguntas fundamentales que debemos responder para desarrollar cualquier política de seguridad son:

a. ¿Qué queremos proteger?

b. ¿Contra quién?

c. ¿Cómo?

Respondiendo a estas preguntas tenemos: Se deberían proteger todos los elementos de la red interna, incluyendo hardware, software, datos, etc., de cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros. La respuesta a la tercera pregunta requiere unas soluciones más dinámicas y cambiantes en lo que se refiere **a** la vigencia de dicha política de seguridad, podemos aplicar el modelo de que: Todo lo que no se prohibe expresamente está permitido, todo lo que no se permite expresamente está prohibido y realizando un análisis de riesgo clasificando por el nivel de serevidad en la cual involucra hacer decisiones costo-beneficio.

4.6.4 Responsabilidades en torno a la política de seguridad

Un aspecto importante en torno a la política de seguridad es asegurar que todos las personas saben cuál es su responsabilidad para mantener la seguridad, por lo tanto la política debe poder garantizar que cada tipo de problema tiene alguien que puede manejarlo de manera responsable, así mismo pueden existir varios niveles de responsabilidades

asociados con una política de seguridad de la entidad financiera. Por ejemplo cada persona es responsable de su contraseña de acceso a la red o recurso del sistema. Una persona que pone en riesgo su cuenta de acceso a la red aumenta la probabilidad de comprometer otras cuentas y recursos.

4.7 Análisis de Riesgos

Consiste en listar todo tipo de riesgos a los cuales esta expuesta los datos y cuáles son las consecuencias, los posibles atacantes entre persona, entidades financieras, las posibles amenazas etc., enumerar todo tipo de posible pérdida, desde pérdidas directas como dinero, clientes, tiempo etc., así como indirectas, créditos no obtenidos, Pérdida de imagen, implicación en un litigio, pérdida de confianza etcétera. El riesgo sé calcular por la formula:

riesgo = probabilidad x pérdida

Por ejemplo el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la pérdida total en nuevos soles de no hacer el contrato. El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la pérdida en nuevos soles de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña el riesgo es menor,

pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la perdida total. Si por otro lado la pérdida es menor aunque la probabilidad de que ocurra el evento sea muy grande tenemos un riesgo menor.

Ejemplo: La pérdida de una transacción comercial de S/.10,000.00 nuevos soles con una probabilidad muy grande de que ocurra al usar una seguridad débil en la red de datos (ejemplo criptografía débil), el riesgo llega a ser menor por lo que depende de la política de seguridad para que este riesgo se asuma.

4.8 Mecanismos de seguridad

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

a. Una información secreta, como llaves y contraseñas, conocidas por las entidades autorizadas.
b. Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
c. Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

No existe un único mecanismo capaz de proveer todos los servicios de seguridad anteriormente citados, pero la

mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

a. Intercambio de autenticación:

Corrobora que un usuario, ya sea emisor o receptor de la información, es la deseado, por ejemplo, el usuario UNI1 envía un número aleatorio cifrado con la llave pública del usuario UNI2, UNI2 lo descifra con su llave privada y se lo reenvía a UNI1, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

b. Cifrado:

El cifrado de datos se puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar desde el emisor al receptor o individualmente a cada enlace del sistema de comunicaciones. Soporta el servicio de confidencialidad de datos al tiempo que actúa como complemento de otros mecanismos de seguridad.

c. Integridad de datos:

Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos. El receptor repite la compresión y el cifrado posterior de los

datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

d. Firma digital:

Este mecanismo implica el cifrado, por medio de la llave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos. Este mensaje se procesa en el receptor, para verificar su integridad, esta relacionado con el servicio de no repudio.

e. Control de acceso:

La función es de asegurar si el emisor está autorizado a usar los recursos del sistema o a la red comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar un registro y/o alarma.

f. Unicidad:

Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

g. Tráfico de relleno:

Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

Fig.4.1 Niveles del Módelo OSI

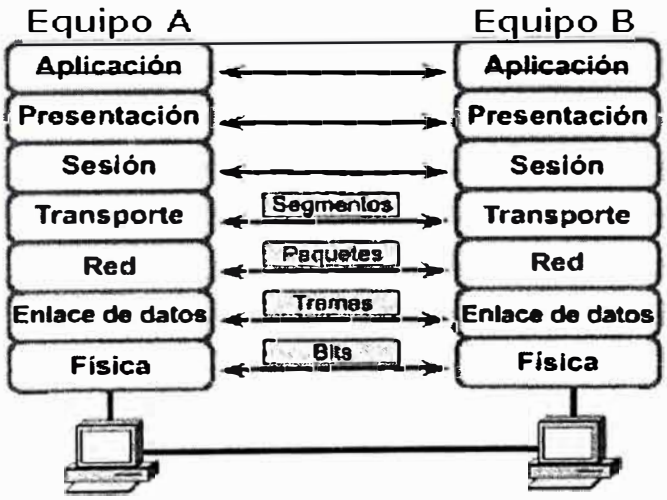

Fig.4.2 Comunicación entre niveles

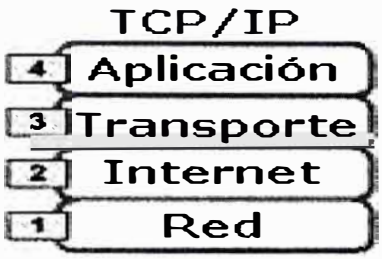

Fig 4.3 Niveles del modelo TCP/IP

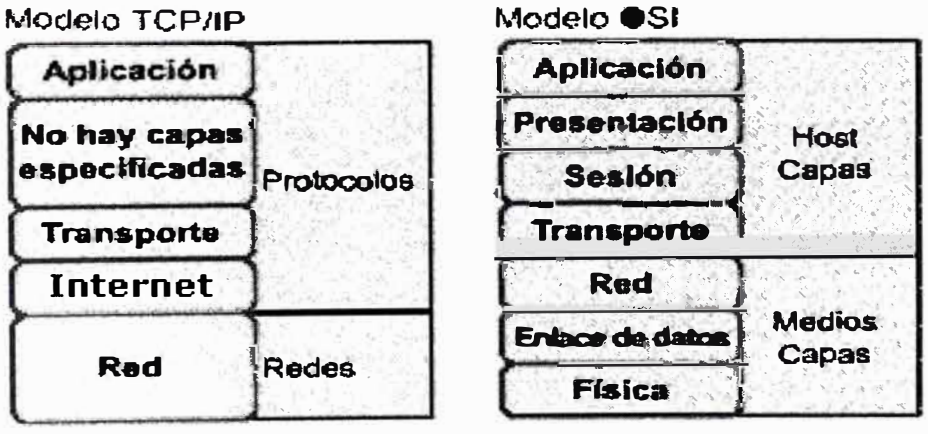

Fig.4.4 Comparación de Modelos TCP/IP - OSI

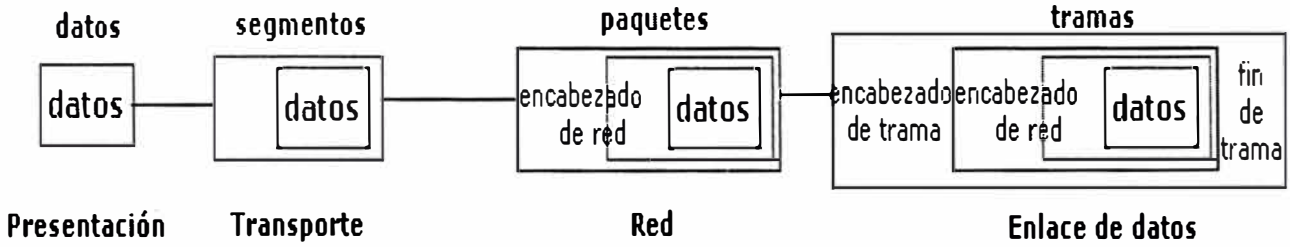

Fig.4.5 Encapsulamiento de datos

CAPÍTULO V
CRIPTOGRAFÍA

5.1 Definición

La tecnología utilizada para mantener confidencialidad de datos y comunicaciones se llama criptología (es una técnica heurística). La técnica heurística es el método de resolver operaciones matemáticas complejas, utilizando exploración y métodos de ensayo y error las cuales se aplican a los datos cuya confidencialidad se desea mantener. Las raices etimológicas de la palabra criptología son Kriptós, que significa oculto y logías, que se traduce como estudio, ciencia. Tiene dos componentes criptografía y criptoanálisis:

a. Criptografía:

Es la técnica de transformar los datos inteligible, denominado texto en claro (plaintext o cleartext), en otro que sólo puedan entender las personas autorizadas a ello, que llamarenos criptograma o texto cifrado. Las raices etimológicas de la palabra critografía son Kriptós, que significa oculto y Graphos, que se traduce como escribir.

b. Criptoanálisis:

Es la ciencia de determinar la llave (analizan los métodos de cifrado) o descifrar los datos sin conocer la llave con el objetivo de encontrar una debilidad, es decir, realizar una especie de criptografía inversa. Las raices etimológicas de la palabra critoanálisis son Kriptós, que significa oculto y Análisis, se traduce como descomposición.

La base de la Criptografía es la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose criptosistema o sistema de cifrado (encriptado) a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

5.2 Llaves criptográficas

Entre ellas tenemos a las llaves secreta, pública y privada.

a. La llave secreta:

Es el código básico de cifrado (encriptación), se utiliza para poner en claro un datagrama. Lo necesitan tanto el emisor como el receptor en los algoritmos simétricos.

b. La llave pública:

Es un tipo de llave que es propia de cada usuario y que es necesaria para enviarle un datagrama, deben de estar disponibles en un directorio público electrónico residente en un servidor.

c. La llave privada:

Solamente la conoce su dueño, es necesaria para descifrar (desencriptar) los mensajes que le envían cifrados con su llave pública.

5.3 Métodos Criptográficos Clásicos

Desde el inicio de la humanidad y antes de la aparición de los primeros computadores, los métodos de cifrados se basaban en la sustitución y transposición de caracteres. Presentaban una dificultad en cuanto a la relación longitud de la llave y el tiempo necesario para cifrar y descifrar el mensaje. Actualmente a estos métodos se les conoce como métodos de cifrado clásicos y se dividen en:

a. Sistema de Cifrado Monoalfabético Simple:

Llamado también César Extremadamente simple, se sustituye una letra por otra. Utilizado por los romanos para cifrar sus mensajes, por eso el nombre de César. Un ejemplo sería substituir:

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

por

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

Por lo tanto, el mensaje "INGENIERO UNI" quedaría cifrado de la siguiente manera: "LPJHPLHURQXPL".

b. Sistema de Cifrado por Sustitución polialfabética:

Emplea múltiples alfabetos de cifrado que se utilizan en rotación de acuerdo con un criterio o llave, cuyo objetivo es adecuar las frecuencias del texto cifrado, de forma que las letras con mayor frecuencia de aparición, no sobresalgan tan claramente. Un ejemplo sería substituir:

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

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

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

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

con una llave 3-1-2, el mensaje "INGENIERO UNI" quedaría: "LUJTUDTPRQ,ZL".

c. Sistema de Cifrado por Transposición de Filas:

Este método consiste en escribir el mensaje en columnas y luego utilizar una regla para reordenarlas. Esta regla es elegida al azar para cifrar el mensaje. El mensaje ha cifrar es "EL SEMINARIO ES EN LA UNI"

1	2	3	4	5	6	7
E	L		S	E	M	I
N	A	R	I	O		E
S		E	N		L	A
U	N	I				

Cifrando el mensaje con una llave 6-3-1-4-2-5-7 quedaría como: "M L REIENSUSIN LA NEO IEA "

5.4 Métodos criptográficos modernos

Los métodos criptográficos modernos, se basan en el uso de llaves, algoritmos y programas de computación para cifrar y descifrar mensajes. Estos métodos modernos empiezan a desarrollarse a partir de la segunda guerra mundial, cuando empiezan a aparecer los primeros computadores. Debido a que se abandona el papel para poder realizar estos complejos cálculos, y se requieren complejos algoritmos computacionales, se les cataloga como "sistemas criptográficos". Los sistemas criptográficos se clasifican en simétricos y asimétricos que a continuación describimos:

a. Sistemas Criptográficos Simétricos:

Son sistemas basados en llaves secretas. La simetría se refiere a que los usuarios involucradas en el proceso tienen la misma llave tanto para cifrar como para descifrar. Este sistema, consiste en aplicar un número finito de interacciones, dando como resultado el mensaje cifrado. La desventaja que presentan es que el usuario emisor como el receptor tiene que emplear la misma llave, para cifrar y descifrar el mensaje. Para ello, la llave debe ser enviada a través de un medio de transmisión: correo, teléfono, fax, mail, etc. y ésta pueden ser interceptada por un tercero que podrá luego utilizarla para leer todos los mensajes cifrados.

b. Sistemas criptográficos asimétricos:

La criptografía asimétrica, también denominada criptografía de llave pública, forma parte de los estándares internacionales: ISO 9796 (Organización de Estándares Internacionales), ANSI X9.31 (Instituto Americano de Estándares Nacionales), ITU-T X.509 (Unión Internacional de Telecomunicaciones), PKCS (Estándares de Criptografía de llave pública), SWIFT (Sociedad para las Telecomunicaciones Financieras Interbancarias mundiales), ETEBAC Nº 5 (Sistema Financiero Francés). Es el sistema que mayor seguridad que se brinda en la actualidad a las transacciones electrónicas e intercambio electrónicos de datos que pueden realizar las empresas, entidades financieras. Utilizan dos llaves diferentes por cada usuario: la llave pública y la llave privada. Ambas llaves, aún cuando son completamente diferentes, trabajan a dúo para cifrar y descifrar mensajes. Esto permite que se puedan compartir públicamente las llaves públicas de cada usuario, sin el temor de que éstas sean vistas por terceros.

5.5 Algoritmos criptográficos

El método o sistema empleado para cifrar el texto en claro se denomina algoritmo de cifrado o de encriptación se forma mediante una fórmula matemática compleja y una llave que pueda ser variada cada vez que nos convenga. Generalmente el algoritmo de cifrado es conocido, se divulga

públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la llave empleada, ya que una de las formas de criptoanálisis de cualquier tipo de sistema es la de prueba-ensayo, mediante la que se van probando diferentes llaves hasta encontrar la correcta. Los algoritmos se clasifican por el modo de operación, simétricos y asimétricos Los modernos algoritmos simétricos mezclan la trasposición y la permutación, mientras que los algoritmos asimétricos se basan más en complejas operaciones matemáticas. A continuación describimos los algoritmos mencionados:

5.5.1 Algoritmos criptográficos simétricos

Para que un algoritmo de este tipo sea considerado fiable debe cumplir los siguientes requisitos básicos: Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la llave. Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la llave que el valor posible de la información obtenida por terceros. Las limitaciones de la criptografía Simétrica es la autenticación (si se deduce la llave se podría descifrar los datos), el cambio de llave (origina distribuir esa nueva llave a todos los usuarios que deseemos comunicarnos por algún

medio electrónico ó físico para distribuir esa nueva llave) y la dificultad de almacenar y proteger muchas llaves diferentes.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son DES, TDES, IDEA SAFER, y BLOWFISH. Actualmente se está llevando a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llamará AES (Advanced Encryption Standart), que se quiere que sea el nuevo sistema que se adopte a nivel mundial, y el algoritmo que utilice se denominará AEA (Advanced Encryption Algorithm), ver figura 5.1.

a. Norma de cifrado de datos (DES):

Es el más estudiado y utilizado de los algoritmos de llave simétrica, fue diseñado por IBM y utilizado desde los años 70. Es un método de cifrado altamente resistente frente ataques criptoanalíticos diferenciales (utiliza los conceptos de transposición y sustitución), Su tamaño de llave (56 bits) la hace vulnerable a ataques de fuerza bruta. El algoritmo cifra bloques de información de 64 bits con una llave de 56 bits, realmente la llave inicial es de 64 bits, pero los bits menos significativos de cada byte se utilizan como bits de paridad, por ello se pueden eliminar al no aportar ninguna información adicional, por lo que nos queda la llave de 56 bits. Dependiendo de la naturaleza de la aplicación DES tiene 4

modos de operación para poder implementarse: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit ó byte por byte y el OFB (Output Feedback Mode) el mismo uso pero evitando propagación de error.

b. Triple Norma de cifrado de datos (TDES):

Una mejora del algoritmo DES, que siempre había sido muy criticado debido a la pequeña longitud de la llave, es Triple-DES. Con este procedimiento, el mensaje es cifrado tres veces. Existen varias implementaciones:

b.1 DES-EEE3:

Se cifra tres veces con una clave diferente cada vez.

b.2 DES-EDE3:

Primero se cifra, luego se descifra y por último se vuelve a cifrar, cada vez con una clave diferente.

b.3 DES-EEE2 y DES-EDE2:

Similares a los anteriores con la salvedad de que la llave usada en el primer y en el último paso coinciden.

Se estima que las dos primeras implementaciones, con llaves diferentes, son las más seguras, como podemos ver en la figura 5.2.

c. IDEA (International Data Encription Algorithm):

Ha sido desarrollado por Xuejia Lay y James Massey. Utiliza llave de 128 bits y es resistente al criptoanálisis. Se encuentra bajo patente de Ascom-Tech, Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones, por lo que se ha difundido ámpliamente, utilizándose en sistemas como UNÍX y en programas de cifrado de correo como PGP (programa Pret ty Good Privacy).

d. SAFER:

Es un algoritmo diseñado por Robert Massey. Tiene llaves de hasta 128 bits y, a pesar de algunas debilidades en la primera versión y de ciertos ataques, parece un algoritmo seguro. Este programa fue desarrollado para la empresa Cylink, que algunos relacionan con la Agencia de Seguridad Nacional Norteamericana (NSA).

e. Blowfish:

Fue creado por Bruce Schneier, utiliza llaves de hasta 448 bits y, hasta el momento, ha resistido con éxito todos los ataques. Por ello y por su estructura se le considera uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente.

Como futuro estándar del algoritmo simétrico se denominará Rijndael, creado por los belgas Vincent Rijmen y Joan Daemen. **Rijndael** es un cifrador de bloque que opera con bloques y llaves de longitudes variables, que pueden ser

especificadas independientemente a 128, 192 ó 256 bits. El resultado intermedio del cifrado se denomina Estado, que puede representarse como una matriz de bytes de cuatro filas.

5.5.2 Algoritmos Criptográficos Asimétricos

También se les llama algoritmo de llave pública. La criptografía asimétrica es por definición aquella que utiliza dos llaves diferentes para cada usuario, una para cifrar que se le llama llave pública y otra para descifrar que es la llave privada. La criptografía de llave pública es una importante tecnología para las aplicaciones de comercio electrónico, intranet, extranet y otras aplicaciones Web. Sin embargo, para poder beneficiarse de la tecnología de llave pública, es necesario una infraestructura de llave pública (PKI) que la soporte.

La ventaja de los algoritmos de llave pública es que eliminan la necesidad que tienen los algoritmos simétricos de tener un secreto compartido entre los usuarios que desean usar un sistema criptográfico. La principal desventaja es que son más costosos temporalmente. Mientras que en los algoritmos simétricos la generación de la llave puede ser aleatoria, en los asimétricos (llave pública) debe hacerse siguiendo un procedimiento determinado debido a la relación existente entre las dos llaves.

Las tres aplicaciones principales de los algoritmos de llave pública son el cifrado de mensajes, la firma digital y el intercambio de llaves, como podemos ver en la figura 5.3.

a. El cifrado de mensajes:

Se realiza cifrando el mensaje con la llave pública y descifrándolo con la llave privada correspondiente. Otra posible forma de cifrar un mensaje es combinar un algoritmo de llave privada con uno de llave pública. Se utiliza el algoritmo de llave secreta para cifrar el mensaje y el de llave pública para transmitir la llave secreta utilizada. Así se alivia parte del alto coste computacional provocado por el cifrado mediante llave pública.

b. La firma de mensajes:

Consiste en aplicar una función hash sobre el mensaje original, y cifrar el resultado mediante la llave privada. El resultado de esta operación es la firma. Para comprobarla lo que se hace es aplicar la misma función hash sobre el mensaje y compararla con el resultado de descifrar la firma usando la llave privada.

c. Intercambio de llaves:

Consiste en utilizar algún algoritmo de llave pública para negociar una llave privada entre dos partes.

Los tres algoritmos de llave pública más relevantes son:

a. Rivest Shamir y Adleman (RSA):

Es un Algoritmo que utiliza llaves de cualquier longitud, aunque actualmente de 1024 bits consideradas lo bastante largas como para resistir ataques de fuerza bruta. Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño. No fué sino hasta 1978 que Rivest, Shamir y Adleman patentan y publican el método más popular, el RSA.

b. Diffie-Hellman (DH):

Este algoritmo de cifrado de Whitfield Diffie y Martin Hellman es el punto de partida para los sistema asimétricos, basados en dos llaves diferentes, la pública y la privada. En la práctica sólo es válido para el intercambio de llaves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer) y VPN (Virtual Private Network).

c. Digital Signature Algorithm DSA:

Este algoritmo fue propuesto en 1,991 por el NIST (National Institute of Standards and Technology) para ser usado en su estándar para firma digital, el Digital Signature Standard DSS. Su uso está limitado a la firma digital de mensajes. Se basa en la dificultad computacional del problema del logaritmo discreto.

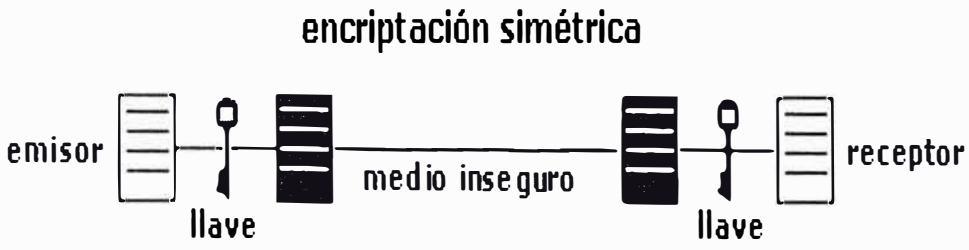

Fig.5.1 Encriptación simétrica.

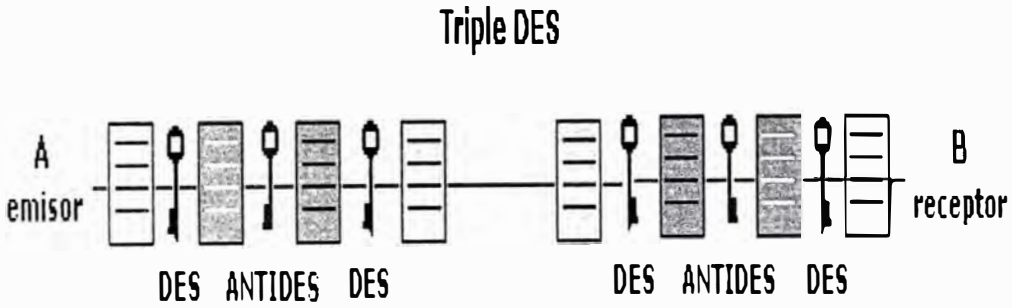

Fig.5.2 Triple DES.

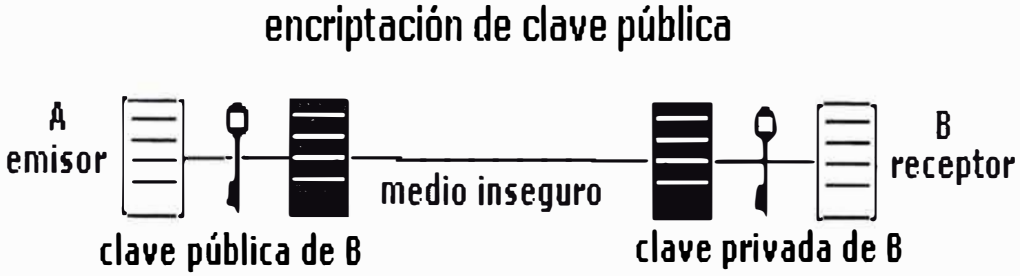

Fig.5.3 Encriptación de clave pública.

CAPÍTULO VI

APLICACIONES DE LAS TECNOLOGÍAS DE CRIPTOGRAFÍA

El avance de la Tecnología, fundamentalmente en lo que a Comunicaciones electrónicas e Información electrónica se refiere y a las nuevas tecnologías como firma digital, certificados digitales y la infraestructura de llave pública, se aplican cada día más en las empresas, entidades financieras que tienden fundamentalmente al incremento de la Eficiencia, la Eficacia, y al ahorro de Costos.

6.1 Firma Digital

6.1.1 Definición

La firma digital es un bloque de caracteres que acompaña a un mensaje o fichero acreditando quién es su emisor (autenticación) y que no ha existido ninguna modificación de los datos (integridad). Para firmar un documento digital, el emisor utiliza su propia llave privada (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación). De esta forma, el emisor queda vinculado al texto

de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier usuario que disponga de la llave pública del emisor. En la Figura 6.1, se encuentra el esquema básico de una firma digital, en la cual se realiza de la siguiente manera: el software del emisor (firmante) aplica un algoritmo hash sobre el texto del mensaje a firmar (algoritmo matemático unidireccional, es decir, lo cifrado no se puede descifrar), obteniendo un extracto de longitud fija (según el algoritmo utilizado oscila entre 128 y 160 bits), y absolutamente específico para ese texto. Se somete a continuación al cifrado mediante la llave privada del emisor. De esta forma obtenemos un extracto final cifrado con la llave privada del emisor el cual se añadirá al final del texto para que se pueda verificar la autoría e integridad del texto del mensaje por aquel usuario interesado que disponga de la llave pública del emisor.

Sin embargo, es necesario comprobar que la firma realizada es efectivamente válida. Para ello es necesario, la llave pública del emisor. El software del receptor, previa introducción en el mismo de la llave pública del emisor (obtenida a través de una autoridad de certificación), descifraría el extracto cifrado del emisor; a continuación calcularía el extracto hash que le correspondería al texto del mensaje, y si el resultado coincide con el extracto

anteriormente descifrado se consideraría válida, en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

6.1.2 Funciones Hash

Si imaginamos el envío de un texto extenso que queremos firmar digitalmente, nos daremos cuenta que cifrar el texto entero es una pérdida de tiempo, ya que los medios de cifrado de llave pública son lentos, porque precisan un gras proceso de cómputo. Para solventar éste aspecto aparecen las funciones hash, que son unas funciones matemáticas que realizan un resumen del texto a firmar. Su forma de operar es comprimir el texto en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash. Estas funciones son además de dominio público. A un texto del mensaje resumido mediante una función hash y cifrado con una llave privada es lo que en la vida real se denomina firma digital. Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales.

6.1.3 Algoritmos Hash

Los algoritmos hash más conocidas y usadas son:

a. Message Digest 5 (MD5):

Desarrollado por Ron Rivest, y ha sido ámpliamante usado como autenticador de mensajes en el protocolo secure sockets layer (SSL) y como firmador de texto de mensajes en el programa de correo Pretty Good Privacy (PGP).

b. Secure Hash Algorithm (SHA-1):

Desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Es muy utilizada en el algoritmo de firma, como en el programa PGP en sus nuevas llaves DH/DSS (Diffie-Hellman/Digital Signature Standar).

c. RIPEMD-160:

Desarrollada por un grupo de investigadores europeos, entre los que se encuentra Hans Dobbertin. Maneja llaves normalmente de 160 bits, aunque existen versiones de 128 y se están planteando nuevas de 256 y 320 bits. Es muy rápido, no está patentado y su código fuente es abierto, de libre acceso.

6.2 Certificado Digital

Debido al creciente auge en el uso de Internet para aplicaciones como el correo y el comercio electrónico, aparece la necesidad de ofrecer nuevos servicios a las empresas y entidades financieras (usuarios). Estos nuevos servicios deben proporcionar al usuario confianza al utilizar estas aplicaciones. Para ofrecer esta confianza aparecen los certificados digitales o electrónicos.

Los certificados digitales son elementos que permiten identificar las partes intervinientes en una transacción telemática. Así mismo y gracias a sus funcionalidades y características, permiten el proteger la información intercambiada mediante mecanismos de cifrado y ofrecen el soporte necesario para implementar firma electrónica, los certificados contienen además la siguiente información:

a. Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
b. Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
c. Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir

de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.

d. Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.

e. Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Para que las entidades financieras y bancos estén completamente seguros de cualquier transacción electrónica es necesario utilizar, al menos dos tipos de certificados, uno general para comunicaciones seguras (X.509) y otro especifico para transacciones económicas (SET). Además de servir como mecanismo confiable y seguro de identificación en la red, el certificado de identidad digital le permite enviar y recibir información confidencial, asegurándose que sólo el remitente pueda leer el mensaje enviado; puede acceder a sitios Web de manera segura con su identidad digital, sin tener que usar el peligroso mecanismo de contraseña; puede firmar digitalmente documentos, garantizando la integridad del contenido y autoría del documento; y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la

identidad de las partes y confidencialidad e integridad de la información intercambiada, comc comercio electrónico, declaración de impuestos, pagos provisionales, uso en la banca. Ver figura 6.2.

6.3 Infraestructura de llave pública PKI

6.3.1 Definición

La infraestructura de llave pública (Public Key Infrastructure PKI) es la infraestructura técnica, legal y comercial que permite el amplio despliegue de la tecnología de llaves públicas y se usa para crear firmas digitales y para gestionar llaves simétricas.

El objetivo de la infraestructura PKI es dotar de los mecanismos básicos de seguridad para mantener la integridad del negocio, la disponibilidad del s e rvicio y la confidencialidad del cliente para, en última instancia, generar confianza.

La autentificación de la clave pública es un requisito indispensable y, por este motivo, las llaves públicas se almacenan en certificados de llaves públicas. Un certificado contiene la llave pública y sus datos identificativos, y una Autoridad de Certificación (CA) que certifica que el propietario de una llave pública es quien realmente dice ser.

6.3.2 Componentes de una PKI

En una PKI encontramos dos tipos de componentes principales: las autoridades certificadoras (Certificate Authority CA) y las entidades finales. En algunos casos puede aparecer un tercer tipo de componentes, que son la autoridades de registro (RA). A continuación describiremos los componentes mencionados:

a. Autoridad de certificación (Certificate Authority CA): Las CA son entidades capaces de certificar la correspondencia entre una entidad y una llave pública. Para ello deben ofrecer un grado de seguridad que haga que el usuario pueda depositar su confianza en ellas. Cuando un usuario confía en una CA considera que todos los certificados emitidos por la misma son auténticos y correctos.
b. Usuario final: Representan al usuario del PKI, utilizan los servicios ofrecidos por las CA para poder obtener las posibilidades que ofrece la criptografía de llave pública. El Usuario no debe de realizar ninguna función de gestión de los certificados. Son simples usuarios, que obtienen los certificados desde una CA y los utilizan. Sí deben tener la posibilidad de almacenar los certificados, para no tener que obtenerlos cada vez que los necesiten. En cuanto a las llaves sí deben ofrecer varias posibilidades. Por una parte, en algunos casos es más interesante la generación de la

llave en la entidad final que en la CA. Por otra parte es necesario que las llaves se puedan almacenar de forma segura, para mantener la seguridad de la PKI.

c. Autoridad de registro (Registration Authority RA): Una RA es una entidad que se comunica tanto con las entidades finales como con la CA, y que realiza funciones de autentificación de usuarios y gestión de llaves. La RA aparece como un puente entre la entidad final y la CA. Para todos los procesos relacionados con autentificación de usuarios y gestión de llaves la entidad final interactuará con la RA, mientras que para los procedimientos relacionados con certificados interactuará directamente con la CA.

   La infraestructura PKI y los certificados digitales son una herramienta fundamental para la seguridad en las entidades financieras. Permiten autenticar las identidades online y cifrar los mensajes de correo electrónico y otra información comercial confidencial a las empresas y entidades financieras que utilizan la red para realizar negocios. De este modo, se ofrece la confianza necesaria para establecer comunicaciones y realizar negocios con total seguridad en un entorno basado en Internet.

d. Políticas de Certificación: Deben diseñarse una serie de políticas, o procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos

entre la Autoridad Certificadora y los Usuarios Finales. Estos documentos tendrán un carácter tanto técnico como legal. El Proceso de Construcción de una PKI deberá siempre partir de la definición de las Políticas Operativas y contemplar como requerimiento esencial el asegurar la calidad y seguridad de las operaciones que los usuarios finales realizan con sus llaves privadas (p.e. Firma Digital de Documentos).

e. Publicación de Certificados: El repositorio de certificados permite a los usuarios operar entre ellos (p.e. Para la validación de una Firma Digital), y es un requisito legal que cuente con una total disponibilidad de acceso.
f. Soporte de la llave Privada. La elección de un buen soporte para que los usuarios custodien su llave privada es un punto esencial y complejo en si mismo (p.e. si la llave está en una SmartCard, es necesario diseñar el Sistema de Gestión de SmartCards que permita la emisión y distribución de las tarjetas a los usuarios).
g. Aplicaciones "PKI-Enabled": Se denomina así a las aplicaciones software capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la PKI de cara al usuario.

6.3.3 Aplicaciones de un PKI

a. Servicios financieros on-line: autenticación y transacción con firma para aplicaciones y actividades de banca electrónica y de bolsa.
b. Acceso a Extranets/Intranets.
c. Servicios estatales on-line: información de ciudadanos, registro de vehículos, declaraciones de impuestos y sanidad.
d. Servicios de comercio electrónico B2B y B2C: autenticación y transacción con firma para aplicaciones de comercio electrónico.
e. Autenticación en Servidores de Acceso Remoto.
f. Conexión segura a la red: en comunicaciones por correo electrónico, cifrado y firma digital.

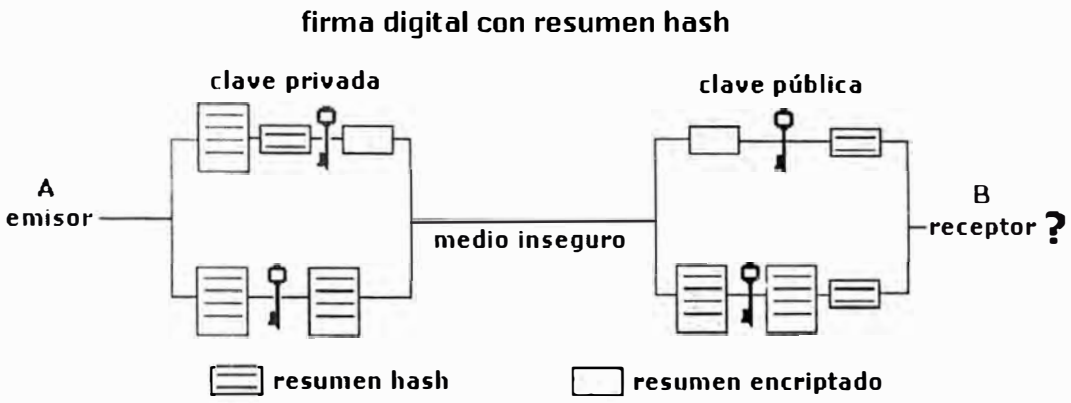

Fig.6.1 Firma digital.

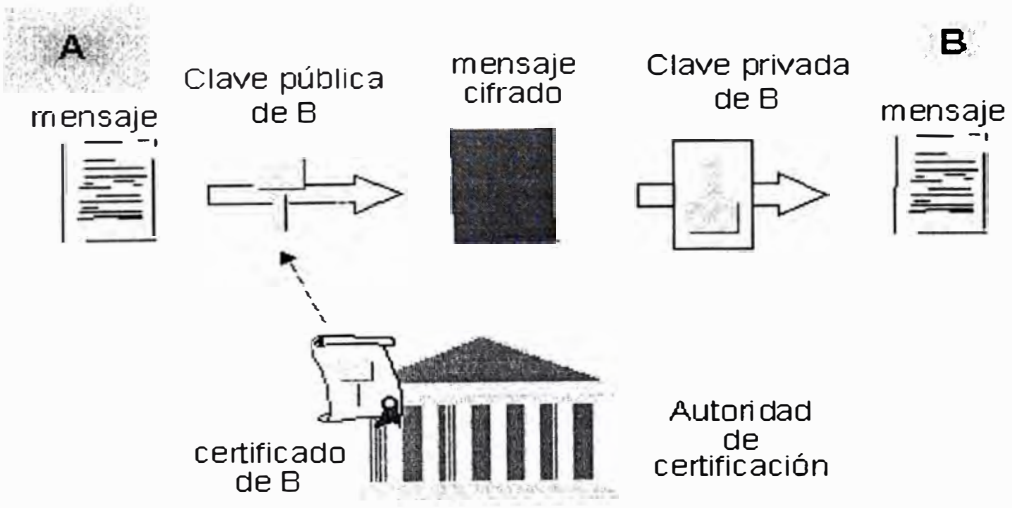

Fig.6.2 Certificado Digital.

CAPÍTULO VII

PROTOCOLOS DE SEGURIDAD EN EL MÓDELO TCP/IP

7.1 Definición

El protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo especifico y que usan esquemas de seguridad de cifrado (criptográfica), cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características. Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

7.2 Esquemas de seguridad en los niveles TCP/IP

A continuación describiremos los protocolos de seguridad en los niveles TCP/IC.

7.2.1 Extensiones Multipropósito para Correo en Internet (S- MIME)

El protocolo seguro MIME (Multi-purpose Internet Mail Extensions) se ha desarrollado para poder transmitir mensajes multimedia a través de las redes IP. Es pues una ampliación del correo electrónico (e-mail) para la transmisión de información multimedia, que convierte en texto cualquier clase de información y que la regenera al formato original en el destino. MIME es, actualmente, el protocolo más utilizado para enviar textos con formato no ASCII a través de Internet. Se conserva todo tipo de información y se muestra íntegramente el contenido al receptor. S-MIME que se utiliza para hacer seguro el envío de mensajes y las transacciones electrónicas incluye firma digital y cifrado basado en el algoritmo RSA de llave pública, es un competidor de otras técnicas como PGP (Pretty Good Privacy), y PEM (Privacy Enhanced Mail), también conocidos como PGP-MIME y PEM-MIME o MOSS/Mime Object Security Standard, respectivamente.

El estándar MIME fue creado en junio de 1992 por IETF (Internet Engineering Task Force). El objetivo de MIME es permitir a los clientes de correo electrónico enviar y recibir mensajes de texto plano y, también, textos con formatos y figuras, ficheros ejecutables, sonidos, imágenes, etc. El protocolo anterior a MIME, SMTP (Simple Mail Transfer

Protocol), estaba limitado al juego de caracteres ASCII americano, y causaba problemas a los usuarios de otros países que necesitaban caracteres con tilde y símbolos especiales. Sin embargo, con MIME los mensajes de correo electrónico pueden contener:

Múltiples objetos en un mensaje simple, texto de longitud ilimitada, conjuntos de caracteres permitiendo lenguajes diferentes al inglés (distintos de ASCII), mensajes con fuentes múltiples, archivos binarios o de aplicación específicos, mensajes con imágenes, audio, vídeo y multimedia y campos de encabezado.

MIME define los siguientes campos de encabezado, que son utilizados por los clientes de correo electrónico para enviar/recibir los mensajes: El campo de versión MIME, que especifica la versión del estándar MIME que se ha utilizado en el mensaje y El campo de Content type, que se utiliza para especificar el tipo y subtipo de los datos en el cuerpo del mensaje.

7.2.2 Protocolo de autenticación Kerberos

Kerberos es un servicio de autenticación desarrollado en MIT (Massachusetts Institute of Technology) y diseñado por Miller y Neuman en el contexto del Proyecto Athena en 1987.

Esta basado en el protocolo de distribución de llaves

presentado por Needham y Schroeder en 1978.MIT. Utiliza criptografía de llave en lugar de contraseñas en texto plano. Kerberos ofrece una capa de seguridad del sistema y dificulta que un usuario no autorizado logre interceptar las contraseñas de usuario. La seguridad de Kerberos descansa en la seguridad de varios servidores de autenticación.

a. Funcionamiento:

Cada usuario y cada servidor tendrán una llave, y Kerberos tiene una base de datos que las contendrá a todas. En el caso de ser de un usuario, su llave será derivada de su contraseña y estará cifrada, mientras que en el caso del servidor, la llave se generará aleatoriamente. Los servicios de red que requieren autenticación y los usuarios que requieran estos servicios, se deben registrar con Kerberos. Las llaves privadas se negocian cuando se registran. Como Kerberos sabe todas las llaves privadas, puede crear mensajes que convenzan a un servidor de que un usuario es realmente quien dice ser y viceversa. La otra función de Kerberos es generar las llamadas llaves de sesión, que serán compartidas entre un cliente y un servidor, y nadie más. La llave de sesión podrá ser usada para cifrar mensajes que serán intercambiados entre ambas partes. El almacenamiento de la base de datos y la generación de llaves, se lleva a cabo en un servidor que se

denomina Servidor de Autenticación (AS por las siglas en inglés de Authentication Server).

b. Niveles de protección:

Kerberos provee tres niveles distintos de protección. El programador de la aplicación determinará cual es apropiado, de acuerdo a los requerimientos de la aplicación.

b.1 Autenticación:

Prueba que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la conexión de red y luego se asuma que los siguientes mensajes de una dirección de red determinada se originan desde la parte autenticada.

b.2 Integridad de datos:

Asegura que los datos no se modifican en tránsito. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo. Éstos se denominan mensajes seguros.

b.3 Privacidad de datos:

Asegura que los datos no son leídos en tránsito. En este caso no sólo se autentica cada mensaje sino que también se cifra. Éstos son mensajes privados.

7.2.3 Protocolo de Transacción Electrónica Segura

Conocido como SET (Secure Electronic Transactions), protocolo creado para proporcionar mayor seguridad a los pagos on-line con tarjetas de crédito verificando la identidad

de los titulares de las tarjetas con "certificados digitales" y cifrando los números de las tarjetas durante todo el trayecto, desde el navegante, el vendedor y el centro de proceso de datos. Este estándar ha sido creado por VISA y Master Card y tiene un amplio apoyo de la comunidad bancaria mundial.

En el proyecto SET participan actualmente empresas como IBM, Microsoft, Netscape, RSA, Verisign y otras, y se esperan nuevas incorporaciones. SET busca un entorno seguro para el comercio en Internet, a base de autentificar a todas las partes implicadas en la compra mediante certificados digitales y autoridades certificadoras, emplea diversos algoritmos criptográficos para garantizar la seguridad de la transacción.

Los objetivos del SET son de, proporcionar la autentificación necesaria entre compradores, comerciantes e instituciones financieras. Garantizar la confidencialidad de la información sensible (número de tarjeta o cuenta, fecha de caducidad, etc.). Preservar la integridad de la información que contiene tanto la orden de pedido como las instrucciones de pago. Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

Para poder realizar pagos mediante el protocolo SET es necesario que el comprador disponga de una cartera electrónica (Wallet), que puede descargarse de forma On-Line, la cual deberá llenar con los certificados SET de las tarjetas

que vaya a utilizar para realizar los pagos. Estos certificados también pueden ser descargados de forma On-Line, en la figura 7.1 encontramos el esquema de transacción SET que a continuación vamos ha describir.

a. Esquema de transacción SET

1. El titular haciendo uso de su wallet se conecta con el servidor de comercio que dispone del Payment Server y le envía los datos necesarios para realizar la compra.
2. El comercio envía a la pasarela de pagos los datos necesarios para llevar a cabo el cobro de la transacción iniciada por el titular.
3. La pasarela de pagos descifra los datos que previamente han cifrado comercio y titular y compone un mensaje que envía a través de las redes bancarias tradicionales para la autorización de la transacción.
4. El banco del titular procede a autorizar la transacción.
5. El banco del comercio procede a abonar en su cuenta el importe de la transacción.

7.2.4 Seguridad del protocolo de Internet (IPSec)

IPSec es un grupo de extensiones de la familia del protocolo IP. Provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. IPSec provee servicios

similares a SSL, pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de IPSec para poder usarlo. Se pueden crear túneles cifrados (VPN), o simple cifrado entre computadoras. Se puede usar como túnel de tráfico para conexiones de redes privadas virtuales (VPN, Virtual Private Networks). Sin embargo, su utilidad va más allá de las VPN. Con un registro central de "intercambio de claves de Internet" (IKE, Internet Key Exchange), cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación de alto grado.

a. Servicios del IPSec:

El protocolo de Internet, IP, también conocido como IPv4, no provee por sí mismo de ninguna protección a las transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. IPSec intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos y ofrece soporte para ambos de un modo uniforme.

a.1 Confidencialidad:

Es necesario asegurarse de que los datos enviados sean difíciles de comprender para todos excepto para el receptor, que nadie pueda leer las contraseñas cuando se ingresa en una máquina remota a través de Internet.

a.2 Integridad:

Hay que garantizar que los datos no puedan ser cambiados durante el trayecto. Si alguien se encuentra en una línea que lleve datos sobre facturación, querrá estar seguro de que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.

a.3 Autenticidad:

Los datos deben firmarse para que otros puedan verificar quién es realmente quien los ha enviado.

a.4 Protección a la réplica:

Necesitamos modos para asegurarnos de que una transacción sólo se puede llevar a cabo una vez, a menos que autoricemos que la repitan. Nadie debería poder grabar una transacción, y luego replicarla al pie de la letra con el propósito de hacer que parezca como si se hubieran recibido múltiples transacciones del remitente original.

b. Protocolos que conforman IPSec:

IPSec provee confidencialidad, integridad, autenticidad, y protección a la réplica a través de dos nuevos protocolos. Estos protocolos se llaman “Cabecera de Autenticación” (AH, Authentication Header) y Carga Útil de Seguridad Encapsulada (ESP, Encapsulated Security Payload).

b.1 AH:

Provee auntenticación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH también asegura partes de la cabecera IP del paquete (como las direcciones de origen o destino).

b.2 ESP:

Proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera en el paquete). La protección a la réplica requiere autenticación e integridad (estas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autenticación y/o integridad. Del mismo modo, se puede usar la autenticación y/o la integridad con o sin la confidencialidad.

7.2.5 Protocolo SOCKS

El uso de cortafugos ha permitido separar estructuras de redes internas del exterior de la misma. Muchos de estos cortafuegos no son equipos físicos sino aplicaciones que actúan sobre la capa de aplicación del modelo OSI, actuando como proxy entre las computadoras que se comunican entre sí. El protocolo SOCKS fue creado para satisfacer esta necesidad que cada vez era mayor, permitiendo una mejor autentificación entre computadores dentro de un entorno (Cliente – Servidor) y logrando así un mejor y mas fuerte control sobre el acceso.

SOCKS es un sistema Proxy equipado con seguridad, auditoria, administración, tolerancia a fallas y notificación de alarmas. Generalmente la aplicación cliente envía la petición al servidor SOCKS, con la dirección de la computadora destino, el tipo de conexión, y la identidad del usuario. SOCKS 5 realiza cuatros operaciones básicas que son negociación, autentificación, petición de conexión, establecimiento del circuito, reenvió de datos. Incluye el protocolo TCP, también soporta UDP y el formato de direcciones IP V6.

7.2.6 Protocolo Secure Sockets Layer (SSL)

Para la transmisión de información confidencial a través de la red utilizaremos el protocolo SSL. El objetivo de SSL es proporcionar autenticación tanto del servidor como del cliente y asegurar la confidencialidad en la comunicación cliente-servidor. La comunicación entre el cliente y el servidor se produce de la siguiente manera:

a. Saludo del cliente:

Tiene por objetivo informar al servidor de los algoritmos de criptografía y compresión que soporta y solicitar el certificado del servidor para verificar su identidad.

b. Saludo del servidor:

Responde al cliente enviando su llave pública del certificado y el conjunto de algoritmos de criptografía y

compresión que se van a usar. En algunas situaciones el servidor puede requerir la identificación del cliente mediante su llave pública.

c. Aprobación del cliente:

El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Para ello desencripta el certificado utilizando la llave pública del servidor y determinando si este proviene de una entidad certificadora de confianza. Después hace una serie de verificaciones sobre el certificado, tales como la fecha, URL del servidor. Una vez verificada la autenticidad del servidor el cliente genera una llave aleatoria y la cifra con la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se envía al servidor y será utilizada para el envío de mensajes entre ambos.

d. Verificación:

Ambas partes conocen la llave secreta que van a utilizar para el envío de mensajes. Es importante tener en cuenta que esta llave tan solo es conocida por el cliente y por el servidor. El cliente la conoce ya que la generó y el servidor porque se le ha enviado utilizando la llave pública de su certificado y es el único capaz de descifrarla, ya que solo es posible con la llave privada que tan solo conoce él. Para comprobar que todo el proceso no ha sido alterado en ningún momento se envían una

copia de la conversación cifrada con la llave secreta. Si ambos confirman que todo es correcto entonces se iniciará el intercambio de información de manera segura. De lo contrario volverían a iniciar el proceso.

e. Intercambio de información:

A partir de este momento toda la información que intercambien cliente y servidor estará cifrada con la llave secreta y, por tanto solo podrán descifrarla y leerla ellos.

f. Fin de la conexión segura:

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

7.3 Redes privadas virtuales VPN

7.3.1 Definición

El uso de Internet por parte de las entidades financieras está llevando a nuevas formas de comunicación y de gestión de la información. Las redes privadas virtuales (del término inglés Virtual Private Network, VPN), consiste en dos máquinas (una en cada "extremo" de la conexión, ver figura 30) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambas máquinas son

cifrados por el Point-to-Point protocol (PPP), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP. Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la entidad financiera y sus sucursales, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Así, las VPNs constituyen una combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y escalable del acceso a través de Internet. Esta combinación hace de las VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier entidad financiera. Las VPNs permiten:

a. La administración y ampliación de la red corporativa al mejor costo-beneficio.

b. La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas de la entidad financiera.

Los requisitos indispensables para esta interconectividad son:

a. Políticas de Seguridad.
b. Requerimiento de aplicaciones en tiempo real.
c. Compartir Datos, aplicaciones y recursos.
d. Servidor de Acceso y Autenticación.
e. Aplicación de Autenticación.

7.3.2 Protocolos que Utiliza una VPN

a. Protocolo punto a punto (PPP):

El PPP fue diseñado para enviar datos a través de conexiones de punto a punto de marcación o dedicadas. El PPP encapsula paquetes de IP, IPX, y NetBEUI dentro de las tramas del PPP, y después los transmite a través de un enlace de punto a punto.

b. Protocolo de túnel punto a punto (PPTP):

El PPTP es un protocolo de nivel de enlace del modelo de referencia OSI, encapsula las tramas de PPP (protocolo punto a punto) en datagramas de IP las cuales van a ser transmitidas a través de una red interna de IP, como Internet. El protocolo de túnel de punto a punto (PPTP) utiliza una

conexión de TCP para el mantenimiento del túnel y las tramas de PPP encapsuladas con encapsulación de enrutamiento genérico (GRE) destinadas a los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse. También proporcionan autenticación de usuario, control de acceso y la oportunidad de aplicar perfiles de acceso telefónico para restringir cuidadosamente el uso de ciertos tipos de acceso remoto por parte de usuarios específicos. PPTP proporciona al cliente remoto una configuración de dirección interna, de modo que pueden participar en la red interna como si estuvieran conectados directamente. PPTP ofrece compresión y opciones de cifrado RC4 estándar y seguro (una llave de secuencia simétrica) para el tráfico que es llevado al interior del túnel.

c. Transmisión de nivel 2 (L2F):

Es un protocolo de transmisión que permite a los servidores de acceso por marcación estructurar el tráfico de marcación en un PPP y transmitirlo a través de enlaces WAN a un servidor L2F. Después, el servidor L2F "abre" los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, el L2F sólo funciona en túneles obligatorios.

d. Protocolo de tunneling de nivel 2 (L2TP):

Este es un protocolo de red que encapsula las tramas de PPP para enviarlas a través de redes de IP, X.25, Relé de trama o de modo de transferencia asíncrona (ATM). Cuando se configura para utilizar el IP y su transporte de datagrama, el L2TP puede utilizarse como un protocolo de túnel a través de Internet. El L2TP a través de redes internas de IP utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. El L2TP también utiliza al UDP para enviar tramas de PPP encapsuladas L2TP como los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

7.3.3 Requerimientos Básicos de una VPN

Por lo general, cuando se desea implantar una VPN hay que asegurarse de que esta proporcione lo siguiente:

a. Autenticación del usuario:

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Asimismo, debe proporcionar registros de auditoria y contabilidad que muestren quién acceso, qué información y cuándo.

b. Administración de direcciones:

La VPN debe establecer una dirección de cliente en la red privada y debe cerciorarse que ias direcciones privadas se conserven así.

c. Codificación de datos:

Los datos que se van a transmitir a través de la red pública deben ser previamente cifrados para que no puedan ser leídos por clientes no autorizados de la red.

d. Administración de llaves:

La VPN debe generar y renovar las llaves de codificación para el cliente y el servidor.

e. Soporte a protocolos múltiples:

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX), entre otros.

7.4 Cortafuegos (Firewalls) y proxys

7.4.1 ¿Qué es un cortafuegos?

Un Cortafuegos o Firewall es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes. e utiliza para proteger la red interna (red local). Lo que hace el cortafuegos es cortar o dejar pasar los intentos de comunicación que tiene todo el mundo (Internet) hacia nuestro computador o hacia nuestra red, según la

situación del cortafuegos. El cortafuegos también puede controlar el tráfico generado desde nuestro computador o red hacia Internet. El cortafuegos actúa a base de normas que establece el administrador de seguridad o en su defecto el administrador de red, o bien el usuario final. Estas reglas definen lo que tiene que hacer el cortafuegos cuando encuentre un paquete que cumpla las características que nosotros le digamos. Aquí es donde se diferencian la mayoría de cortafuegos.

Para poder entender mejor el tipo de políticas (reglas) que se podrían definir en el cortafuegos serían necesarios conocimientos de protocolos, por lo menos de la estructuración de niveles del modelo de referencia OSI. La mayoría de cortafuegos personales nos permiten filtrar tramas creando reglas de nivel 3 (IP), 4 (TCP/UDP) ó 7 (Aplicaciones). Por ejemplo, podríamos definir una regla que no dejara pasar ningún paquete proveniente de Internet, cuyo destino fuese nuestro computador y, más concretamente, el puerto 80 (HTTP) de nuestro computador.

7.4.2 ¿Qué es un Proxy?

Un Proxy es un programa (trabajando en el nivel de aplicación de OSI) que permite o niega el acceso a una aplicación determinada entre dos redes. Hace de intermediario

entre los usuarios, normalmente de una red local, e Internet, lo que hace realmente un Proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet podemos conectar varios usuarios. Normalmente, un Proxy es a su vez un servidor de caché. La función de la caché es almacenar las páginas Web a las que se accede más asiduamente en una memoria. Así cuando un usuario quiere acceder a Internet, accede a través del Proxy, que mirará en la caché a ver si tiene la página a la cual quiere acceder el usuario. Si es así le devolverá la página de la caché y si no, será el Proxy el que acceda a Internet, obtenga la página y la envíe al usuario. Con la caché se aceleran en gran medida los accesos a Internet, sobre todo si los usuarios suelen acceder a las mismas páginas.

El Proxy es "transparente" al usuario, lo pongo entrecomillado porque el usuario tendrá que configurar su navegador diciéndole que accede a Internet a través de un Proxy (deberá indicar la dirección IP del proxy y el puerto por el que accede), pero una vez realizado esto, el usuario actuará de la misma manera que si accediera directamente a Internet. Los últimos Proxies que han aparecido en el mercado realizan además funciones de filtrado, como por ejemplo, dejar que un usuario determinado acceda a unas determinadas páginas de Internet o que no acceda a ninguna. Con esta función podemos

Internet o que no acceda a ninguna. Con esta función podemos configurar una red local en la que hayan usuarios a los que se les permita salir a Internet, otros a los que se les permita enviar correo, pero no salir a Internet y otros que no tengan acceso a Internet. Esta característica muchas veces hace que se confundan con un cortafuegos.

Los proxies se clasifican según la aplicación de trabajo y estos son: Proxy WWW, Proxy http (servidor con caché, soporta peticiones HTTP, FTP y SSL), proxy FTP (proporciona acceso a servidores FTP), proxy POP3 (permite el acceso a servidores POP3 de Internet para recoger correo electrónico), proxy RealAudio (permite escuchar ficheros de servidores RealAudio),

7.4.3 Diferencias entre un cortafuegos y un proxy

El cotafugos (firewall) y el proxy son diferentes, pero deberían estar siempre combinados. El firewall sin embargo, es únicamente un método de protección de la red local o de un computador personal, con el que podemos cerrar o dejar abiertos ciertos puertos, IPs, aplicaciones, etc. El Proxy se usa para redirigir las peticiones que recibe de varios usuarios a Internet de forma transparente y se encarga de devolverles las respuestas (las páginas Web). También se puede utilizar para FTP, POP3, SMTP, IMAP, TELNET, etc.

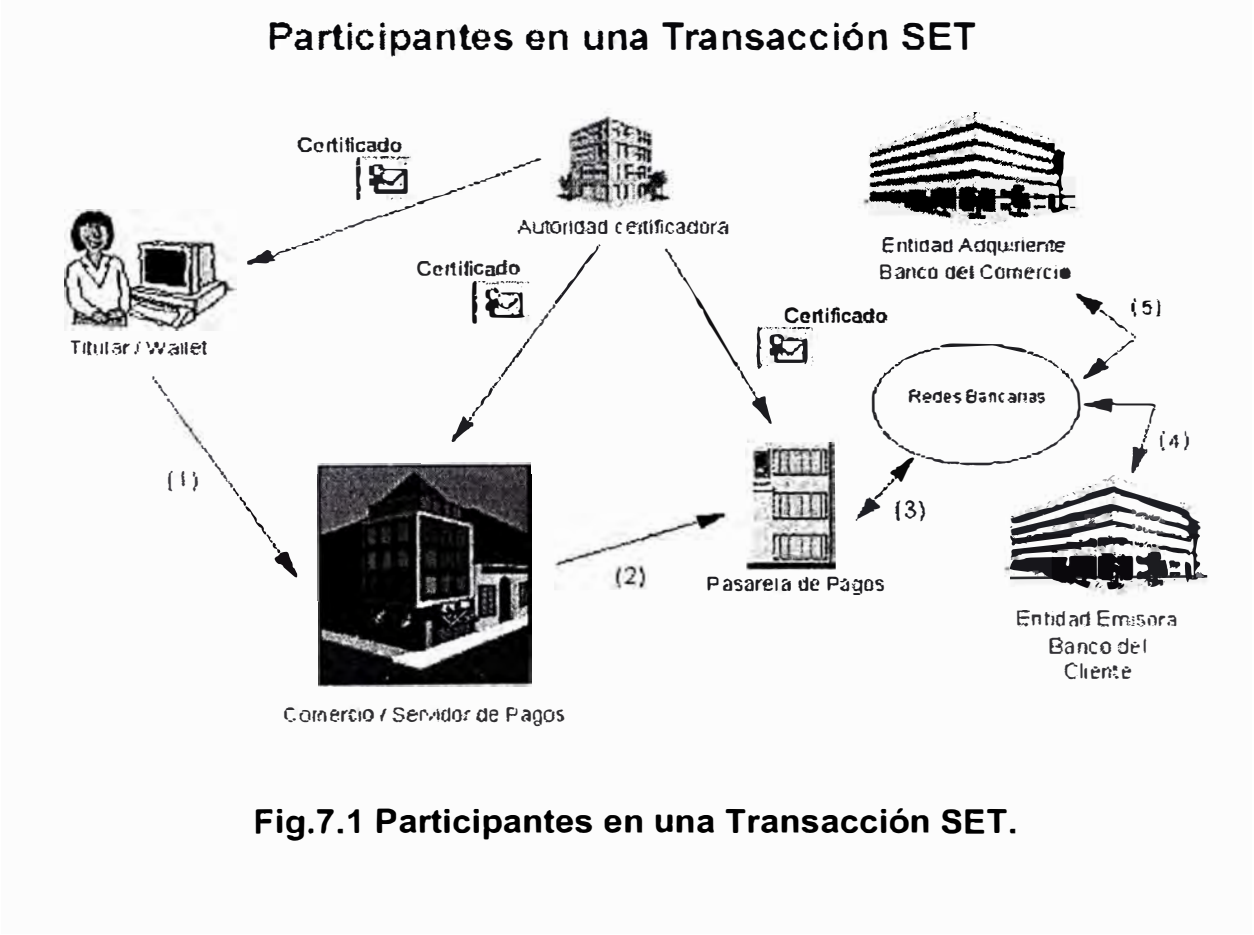

Fig.7.1 Participantes en una Transacción SET.

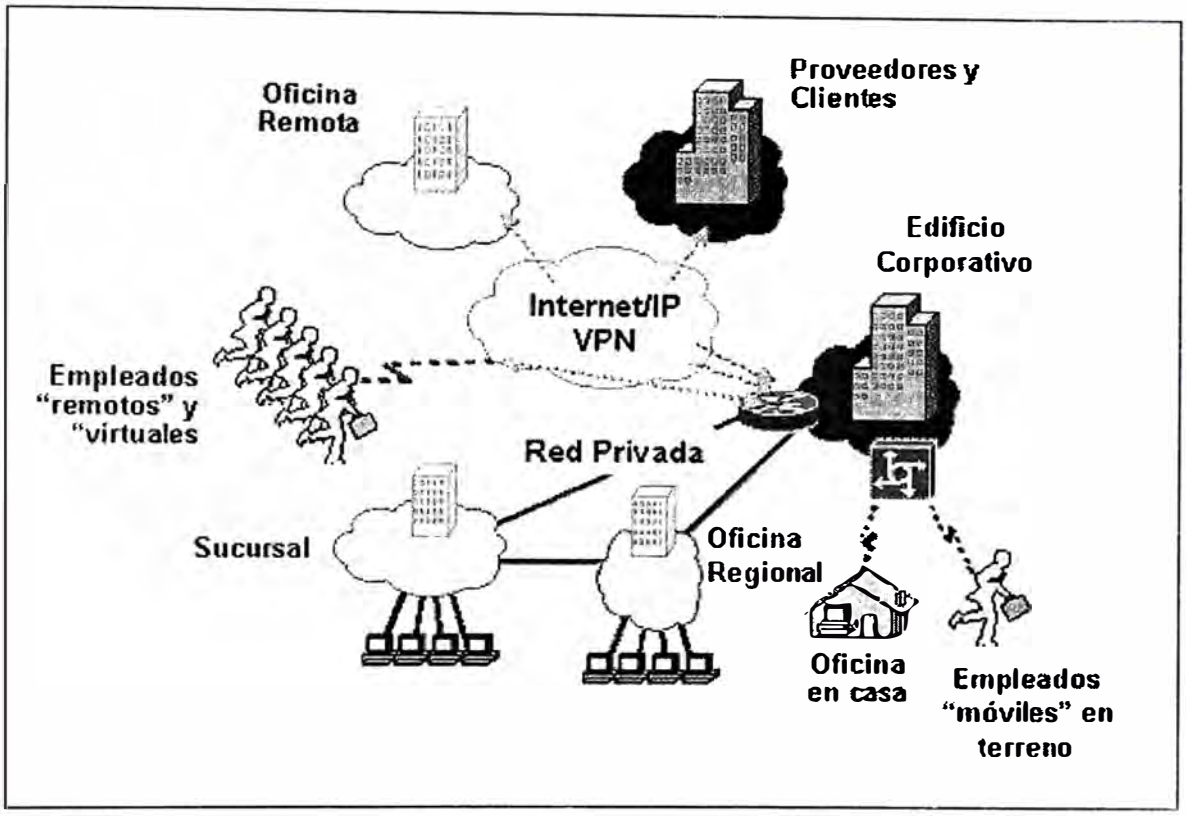

Fig.7.2 Red Privada Virtual VPN

CONCLUSIONES Y RECOMENDACIONES

1. Es prácticamente imposible erradicar todas la vulnerabilidades y amenazas a las que se ven sometidas los servicios y aplicaciones de las redes de datos de las entidades financieras y bancarias. Se recomienda entonces realizar periódicamente Auditorias de Seguridad, porque permiten conocer el nivel de seguridad y las acciones a emprender para corregir los posibles fallos.
2. El uso de Internet o de cualquier otra red insegura para el intercambio de información plantea dos grandes problemas que son la autenticación, es decir, asegurar que el emisor y receptor son realmente quienes dicen ser y la privacidad e integridad de los datos que circulan, o sea, que un tercero no pueda observar, copiar o modificar el contenido de la información mientras se transmite. Para solucionar a ambos problemas recomiendo el uso de la criptografía digital, es decir, de sistemas de cifrado.
3. Los cortafuegos o firewalls son una buena alternativa contra amenazas en la seguridad de la red, pero no son una solución de seguridad completa, por lo que se recomienda

instalar un servidor de antivirus en la red y revisar constantemente las estadísticas de acceso, de uso y de acceso físico a los recursos.

4. La seguridad se trata de una función que no sólo depende de los dispositivos, sino del personal de la entidad financiera o bancaria y de los procesos que configuran, administran y monitorear. Por lo que se recomienda considerar de manera integral todos los elementos que componen la seguridad de una red, es decir conectividad segura, seguridad en el perímetro, monitoreo, identidad y administración.
5. El uso de servidores seguros es un elemento imprescindible en todos los servicios que utilicen información confidencial, como operaciones bancarias, comprar por Internet, acceso a servidores de datos sensibles, etc., por lo que se recomienda conseguir la confidencialidad e integridad de datos basados en el uso de sistemas criotográficos mixtos, que combinan la criptografía de llave pública con la llave simétrica. Y para garantizar al usuario su autenticidad, los servidores seguros deben de hacer uso de los certificados digitales.
6. Cuando hablamos de información, su riesgo y su seguridad, siempre se debe considerar al elemento humano, ya que podría definir la existencia o no de lo más altos grados de

riesgo. Por lo cual se recomienda considerar la idiosincrasia del personal de la entidad financiera o bancaria, al menos de los cargos de mayor dependencia o riesgo.

7. Las políticas de seguridad son parte fundamental de cualquier esquema de seguridad eficiente. Por lo que se recomienda que las políticas tienen que ir acompañadas de sanciones, las cuales deberán también ser redactadas, revisadas, autorizadas, aplicadas y actualizadas.
8. El principal requisito en una transacción de comercio electrónico de una entidad financiera y bancaria es la seguridad, como en todas las transacciones que implican el manejo de dinero. Por lo que se recomienda que el costo de una buena gestión de seguridad siempre sea menor que el valor de los datos internos.

ANEXO A

GLOSARIO DE TÉRMINOS

El glosario contiene los términos y expresiones utilizadas en este informe que frecuentemente se emplean en le campo de la Teleinformática, la mayoría de las definiciones se han extraído de las publicaciones pertenecientes al CCITT, simplificando en algunos casos las mismas.

Ancho de Banda: Cantidad de volumen de información expresada en bits por segundo (bps) que se pueden transmitir en un tiempo concreto de conexión.

Autenticación: Mecanismos del sistema de información para poder identificar a los usuarios que acceden a sus recursos y asegurar la autenticidad de los datos.

Bajar Fichero (download): Sirve para expresar la posibilidad de trasmitir ficheros desde el lugar al que estamos conectados hasta nuestro computadora.

B2B (business to business): Término utilizado en el ámbito Internet con el fin de reflejar las relaciones comerciales entre empresas. Fundamentalmente se centra en el proceso de

compras y suministros entre organizaciones, aunque puede recoger todo tipo de transacciones comerciales.

Browser: También denominado Navegador consiste en un programa con el que el usuario accede a los documentos de la Web. Permite la visualización y manipulación de la información. (Ej. Explorer , Netscape, Mosaic, etc.)

Buscador: Programas que estructuran la información de manera sistematica facilitando así la búsqueda de datos por palabra llave o por algún otro método.

Business-to-Customer (B2C): Comercio por medios electrónicos dirigido a usuarios finales.

Cliente/Servidor: Arquitectura de red en la que cada computadora o proceso en la red es un cliente o un servidor. Los servidores son computadoras o procesos de gran capacidad dedicados a administrar los discos, las impresoras y el tráfico de trabajo en la red. Los clientes son computadoras personales en las que los usuarios corren las aplicaciones.

Comercio Electrónico (e-commerce): Intercambio de bienes y servicios realizado a través de las Tecnologías de la Información y las Comunicaciones, habitualmente con el soporte de plataformas y protocolos estandarizados.

Contraseña (password): Es la parte privada de identificación de usuario. El nombre y la contraseña forman una pareja

inseparable en los sistemas que identifican a sus usuarios a través de este mecanismo.

Correo Electrónico (e-mail): Es una de las aplicaciones mas populares de Internet. Es el sustituto del correo tradicional.

Data Mart: Un data warehouse de un tema específico.

Data Warehouse: El conjunto de datos que presentan una visión coherente de la situación del negocio en un momento determinado, diseñado para soportar la toma de decisión gerencial.

Dominio: Es la forma ideada para que cada computadora tenga una única dirección, agrupados por jerarquias simplificando asi su identificación. (Ej. Perú -> .pe).

Enlaces (Links): Dispositivo de software capaz de relacionar información incluso localizada en distintos ordenadores.

EDI (Electronic Data Interchange): Protocolo creado a principios de los años 70 para permitir que las grandes compañías pudieran transmitir información a través de sus redes privadas, y está siendo adaptado en la actualidad a los Webs corporativos.

Extranet: Es una Intranet que permite el acceso controlado a usuarios externos mediante la autenticación.

HTML: Lenguaje usado para programar en el Internet

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronic Engineers).

IGMP (Internet Group Management Protocol): Protocolo de Administración de Grupos de Internet.

Interactivo: Un diálogo bilateral entre el usuario y una computadora.

Internet: Red mundial de computadoras compartiendo información.

Intranet: Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

Java: Un conjunto de tecnologías para crear y correr programas de software de forma segura.

JavaScript: Lenguaje parecido a Java que se diferencia en que los programas están incorporados en el fichero HTML.

Lenguaje de Marcado de Hipertexto (HTML): Lenguaje que se utiliza para crear los documentos los que se accede a través de navegadores WWW.

Localizador Uniforme de Recursos (URL): es una dirección unica para referirse a documentos concretos de la Web.

Nombre (login): Identificador del usuario para poder acceder a los datos de un sistema. Suele ser público.

Moneda Electrónica (e-cash): La implementación resulta complicada por motivos de seguridad. Se estan creando diversos tipos de cyberdinero para pagar en la red.

Negocio Electrónico (e-business): Utilizar la Internet para realizar negocios, generar ingresos y/o compartir información.

Protocolo de Transferencia de Hipertexto (http): Protocolo usado para la transferencia de documentos WWW.

Multimedia: Información digitalizada que combina texto, gráficos, imagen fija y en movimiento, así como sonido.

Sitio (Size): Punto de la red con una dirección unica y al que pueden acceder los usuarios para obtener información.

Suma de chequeo (checksum): Contador que recoge la suma de los resultados de aplicar un determinado algoritmo a cada octeto de la información a comprobar.

Telnet: Protocolo de Internet que sirve para conectarse a otras computadoras remotas en red, permitiendo usar sus programas y su información.

UIT (Unión Internacional de Telecomunicaciones): Organismo internacional, con sede en Ginegra, cuya misión es definir estándares para las redes de comunicación.

WAN (Red de Área Amplia): red que permite conectar físicamente varios ordenadores, y cuya titularidad es pública. Son las Redes Públicas de Datos, normalmente. En ellas se basa la Red Internet.

Web (World Wide Web o WWW): Colección de ficheros que dan lugar a un sitio Web o páginas de Web, que incluyen información multimedia: texto, gráficos, sonidos y vídeos,

además de vínculos con otros Web. La Web se identifica por un localizador universal de recursos (URL) que especifica el protocolo de transferencia, la dirección de Internet de la máquina y el nombre de la página a que se desea acceder.

Website: Colección de página vinculadas entre si, que utiliza el protocolo HTTP para enlazar páginas mediante mecanismos de hipertexto (lenguaje HTML).

BIBLIOGRAFÍA

[1] Casselberrry R, Baker D, Benett G, Calabria J. Running a Perfect Intranet. QueMAcmillan Computer Publishing. 1996.

[2] John R. Vacca. "Los secretos de la Seguridad en Internet". Ediciones Anaya Multimedia, S.A, 1997.

[3] Karanjit Siyan, Chris Hare. Firewalls y la Seguridad en Internet. Prentice-Hall, Segunda Edición. 1997.

[4] John Ray. Edición especial TCP/IP. Prentice Hall, 1999.

[5] Marcus Goncalves and Steven Brown. Check Point Firewall-1 Administration Guide. Mc GrawHill, 1999.

[6] Tom Shaughnessy con Toby Velte. Manual CISCO, Diseñe y Configure redes usando hardware y software de CISCO. Mc Graw Hill, 2000.

[7]. Robert L. Ziegler. Linux Firewalls. New Riders, 2nd edition, 2001.

[8]. PC WORLD. Revista de informática para los negocios. Editorial Perú. Edición mensual.

[9]. PC MAGAZINE. Revista de guía independiente para la tecnología. Editorial Televisa. Edición Mensaual.