1

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

ENCRIPTADO DE INFORMACION EN REDES DE DATOS PARA EL DESARROLLO DEL COMERCIO ELECTRONICO

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N :

GABRIEL ALDAMA RAMIREZ

JOSE FRANCISCO MARES CANALES

DIRECTOR DE LA TESIS:

DR. FRANCISCO GARCIA UGALDE

CIUDAD UNIVERSITARIA 2001

"Conoce al enemigo y conócete a ti mismo;
en cien batallas no correrás peligro.
Si ignoras al enemigo pero te conoces a ti mismo,
tus probabilidades de ganar y perder son idénticas.
Si ignoras tanto al enemigo como a ti mismo,
seguramente correrás peligro en cada batalla."

Sun Tzu

Índice

Agradecimientos

Agradezco a mis padres por haberme proporcionado los principios y apoyo que me han permitido ser el creador de mi circunstancia. A mi madre mi reconocimiento por su aliento, dedicación, protección y guía; a mi padre por su ejemplo y sus invaluables enseñanzas sobre la información, los sistemas y el ejercicio de la profesión de ingeniería; finalmente, a mi hermano por su amistad, por ser un modelo de constancia y perseverancia, y por su enorme capacidad para evaluar, crear y romper paradigmas.

De manera especial quiero agradecerle al Dr. Francisco García Ugalde el haberme dado la oportunidad de compartir sus conocimientos, ideas y experiencia en las clases, en el servicio social, y en el desarrollo de la presente tesis. Mi reconocimiento a su visión, recomendaciones y apoyo para que exploraramos este nuevo territorio formado por la criptografía y el comercio electrónico; a su tiempo invertido y dedicación para guiar, analizar y revisar el proyecto.

Así también, les agradezco a los profesores de la facultad Dr. Rogelio Alcántara, Ing. Jesús Reyes, Dr. Carlos Rivera e Ing Orlando Zaldívar por su tiempo dedicado a la lectura de este documento y por sus recomendaciones que permitiron enriquecerlo.

Al Dr. Eulalio Juárez Badillo, tutor y guía durante mis primeros tres años de estudios en la Facultad; por compartir sus conocimientos, ideas y experiencia en el estudio de la creatividad, de la ingeniería, de la investigación y del campo de las relaciones humanas. Quiero aprovechar este espacio para darle las gracias por enseñarme a sensibilizar e integrar la teoría con la práctica, las personas con las ideas, los problemas con las soluciones, y el impetú con la experiencia.

Mi reconocimiento a la UNAM, en especial, a la Facultad de Ingeniería: a sus profesores, investigadores, administrativos y condiscípulos; quienes en un esfuerzo conjunto fundan y consolidan cada día el espíritu de la comunidad con los valores del esfuerzo y la excelencia que caracterizan a la raza por la cual hablará el espíritu. En especial, agradezco a Gabriel su participación entusiasta para la realización de la presente tesis.

Finalmente agradezco a Probetel su apoyo para la realización de esta tesis; así como también el recibido del programa de alto rendimiento de la Facultad, Fundación TELMEX, Fundación UNAM, INTTELMEX y Jóvenes Científicos de Sedesol, durante el transcurso de mis estudios de licenciatura

José Francisco Mares Canales

¿Agradecer?

Normalmente damos gracias al termino de los ciclos o periodos importantes en nuestra vida. Cuando cumplimos años, cuando concluimos un ciclo escolar o cuando llegamos al fin de un periodo importante de nuestras vidas: una boda, un nacimiento, y porque no, una tesis.

Llegado el momento, damos gracias a alguien, pues reconocemos que el ser humano sólo puede progresar con ayuda de los demás. Pero más importante aún, dar gracias a los amigos y familiares es quizás un momento de esperanza en el que les decimos: "soy lo que soy gracias a ti, pero al mismo tiempo quisiera contar contigo por siempre".

Por esta razón, agradezco a mi hermano Daniel, quien ha sido más que un hermano y amigo, un tutor, maestro, cómplice de travesuras y fuente de esperanza. A mi madre Gabriela por su cariño y sus cuidados. A mi tío Roberto por mostrarme los valores del profesionista independiente y a mis Abuelos (Armando y Guadalupe✞) por ser el origen de mis valores éticos y morales.

Al mismo tiempo, doy gracias por tener amigos como Myriel Cruz, quien ha sido casi como un hermano para mi y Daniel Reyes, una de las pocas personas que me acepta con todos mis defectos. Especialmente doy gracias también a Francisco, quien confió en mí tanto para la planeación de esta tesis como en su elaboración.

Por último, debo agradecer a mis profesores de la Facultad, y muy especialmente al Dr. Francisco García Ugalde por su asesoría y sus acertados consejos

Gabriel Aldama Ramírez

Prólogo

Estamos presenciando una nueva revolución causada por la popularización del Internet, de las computadoras, y de la generación y uso de la información en bits. Aunque en sus orígenes el Internet fue concebido como un mecanismo de seguridad nacional y un paradigma en la investigación académica; su desarrollo e integración con otros productos esta creando un poderoso medio de difusión e intercambio de información El Internet del mañana no sólo será una gran "biblioteca" o un escaparate para millones de páginas "Web" distribuidas en miles de servidores; se transformará en un medio de trabajo colaborativo, negocios virtuales y, finalmente, en un motor de enriquecimiento cultural.

El nuevo medio que apenas empezamos a conocer hoy debe su existencia a múltiples factores; siendo el acelerado desarrollo de la tecnología, la enorme cantidad de información generada y la asimilación social de ambos, los más importantes de ellos. La revolución toma forma en la disponibilidad de medios (dispositivos e infraestructura) baratos e interactivos (con la capacidad para comunicar todo tipo de información, independientemente de su ubicación geográfica y del tiempo en que se haga); provocando que los usuarios ya no se conformen con ser únicamente receptores pasivos de la información, sino que ahora se convierten en generadores de conocimiento y, eventualmente, de riqueza.

Thomas L. Friedman, en su libro *Tradición vs. Innovación*, explica como los factores desencadenantes de la "nueva era informática" se basan en tres premisas básicas: la democratización de la tecnología, la democratización de la información y la democratización de las finanzas. Analizando las ideas de Peter Cohan, Michael Dertouzos, Bill Gates, Armand Mattelart y Nicholas Negroponte; sintetizamos la dirección y evolución de dicha nueva era.

Aunque falta mucho para que la conjunción de computadoras, Internet y el WWW se convierta en el medio de acceso y comunicación universal; sus velocidades de penetración e incorporación social hacen de este nuevo medio de comunicación un elemento fundamental para el entendimiento de la civilización humana en el corto y mediano plazo.

En este sentido, el presente trabajo de tesis intenta analizar uno de los temas de mayor importancia en lo que se refiere a las aplicaciones de negocios sobre Internet: la búsqueda de mecanismos que garanticen la seguridad y confiabilidad en el comercio electrónico. Esta nueva forma de hacer negocios es un área de gran interés en una sociedad cuyas actividades y procesos cada día se basan más en la información electrónica, y en la cual se prevé a corto plazo: una creciente penetración del Internet comercial en la vida diaria y un incremento considerable en la utilización de sistemas de compras electrónicas.

Esperamos que este documento contribuya a despertar el interés en la investigación de temas relacionados con la seguridad informática y el comercio electrónico; sobre todo en la comunidad hispanohablante, tanto por el potencial económico que representa como por la necesidad de contar con mecanismos de seguridad específicos para cada empresa y/o gobierno; y finalmente, para contribuir con ideas originales y novedosas al desarrollo de las sociedades.

Agosto 2001
Gabriel Aldama Ramírez
José Francisco Mares Canales

1 Introducción

Esta tesis presenta un enfoque orientado a la aplicación de herramientas criptográficas para proteger la información que es transportada por las redes de datos, en especial Internet, y utilizada en el comercio electrónico.

La primera fase de este trabajo consistió en analizar la conjunción formada por el desarrollo de la información digital, la red Internet, y la expansión del uso de las computadoras; sobre la cual se sustenta el comercio electrónico. Al conocer todos los sistemas y procesos que conforman al comercio electrónico, se determinaron las necesidades de seguridad informática existentes en esta actividad.

La siguiente fase consistió en sintetizar diferentes ideas sobre la seguridad informática, gracias a lo cual se determinó que una buena metodología para el desarrollo de sistemas informáticos seguros debe considerar todo el ciclo de vida de la información y de los elementos con los cuales está en contacto. Por el alcance de esta tesis, únicamente se evalúan las debilidades y los riesgos a los que está expuesta la información desde su creación, su almacenamiento, su transporte hasta su utilización.

Como tercera fase se creó un modelo de tienda virtual para el comercio electrónico, propuesto por nosotros. A grandes rasgos se planteo un sistema que, en la medida de nuestras posibilidades, emulará un portal comercial cualquiera Para tal efecto, se diseño un sitio comercial para venta de música por las características del mercado, economía y disponibilidad de ancho de banda para los cibernautas en México. A partir de ahí, se desarrollo un modelo en el cual se sintetiza todo el análisis de riesgos y debilidades de seguridad informática posibles para este negocio; para luego proponer los requerimientos de "software" y "hardware", criptográfico y no criptográfico, necesarios para cubrir todas las necesidades detectadas.

Aunque el modelo teórico analiza todo el ciclo de vida de la información, en especial al recorrer el modelo de referencia OSI, al plantear los mecanismos de protección necesarios; nuestro trabajo se enfocó en la implantación a nivel aplicación, funcionamiento del sistema total e interfaz al usuario. Las razones de tomar este acercamiento son: poca teoría y estudios de seguridad en el comercio electrónico, escaso desarrollo y documentación, así como la existencia de muchas lagunas conceptuales. Por ello deducimos que ésta es un área con libertad de innovación y creatividad; resaltando por las características propias de nuestro país.

Para la programación de nuestro modelo se eligió el lenguaje Java y librerías de funciones criptográficas desarrolladas tanto por sus creadores como por grupos de trabajo internacionales. En este documento presentamos la evaluación y uso de dichas herramientas; así como otras utilizadas para el desarrollo del sitio de comercio electrónico, la puesta del servidor correspondiente y la creación de nuevas interfaces para su uso a través de páginas Web.

En resumen:

a) Se diseño un portal comercial para la venta de canciones por Internet.
b) Se plantearon ejemplos de arquitecturas de sistemas de información de un banco, de una casa musical y de una tienda virtual; todos conectados a Internet. Cada arquitectura muestra los mecanismos de seguridad informática necesarios así como los elementos básicos para la realización de operaciones comerciales electrónicas.
c) Se analizaron de librerías y "software" criptográficos desarrollados por distintos grupos de programadores, con el fin de adecuarlos y utilizarlos en nuestro proyecto.

d) Se desarrollaron una serie de interfaces para cifrado de información tanto para su uso didáctico como para la aplicación en nuestro proyecto (el portal comercial).

Desde el inicio, nuestro trabajo de tesis no se concibió para ser un sistema de comercio electrónico genérico ni se planeo su elaboración como un producto comercial. Sin embargo, el valor de este documento se basa en que analizamos, sintetizamos y estructuramos los conceptos mínimos necesarios para todo aquel interesado en explorar y explotar, en forma segura, los beneficios del comercio electrónico. Dado que son pocos los trabajos documentados en esta área, esperamos que este sea un mapa de utilidad, y estimulante para crear muchos más, de este nuevo territorio.

1.1 Estructura y contenido del documento

El presente documento esta conformado por seis capítulos, una sección de conclusiones, ocho anexos, un glosario y un apartado bibliográfico y de referencias. A continuación se describe brevemente el contenido de cada uno.

El primer capítulo es la introducción al presente documento: muestra la motivación y objetivos del trabajo, la estructura del documento y la terminología usada en él; y el marco de referencia en el cual se desarrolla el comercio electrónico y la presente tesis. A grandes rasgos se dan los conceptos básicos de la información, como ha evolucionado hasta nuestros días, su asimilación en la vida cotidiana, y su relación con el comercio electrónico. Mostramos la importancia del medio computadoras-Internet-WWW, y las repercusiones económicas y sociales que esta desencadenando.

Los temas de comercio electrónico y sus necesidades de seguridad son condensados en el segundo capítulo. Se conceptualiza como la sociedad actual ha empezado ha asimilar las tecnologías basadas en la información digital para dar lugar a los actores y condiciones necesarias que motivan el comercio electrónico. Se detallan los diferentes tipos de comercio electrónico posibles, las etapas evolutivas de su implantación y los principales componentes. De igual forma se muestra una metodología para evaluar qué se debe proteger en el comercio electrónico, la cual es utilizada en el cuarto capítulo para desarrollar el modelo desarrollado en el presente trabajo

La criptografía es el tema del tercer capítulo. Se muestran los conceptos básicos y objetivos de la criptografía, la criptografía simétrica y asimétrica, tipos de ataques, sistemas de intercambio de llaves, y la noción y uso de los certificados digitales. Se describen algunos de algoritmos, tanto por su relevancia como por su uso en el presente trabajo De igual forma, se tiene una sección dedicada al estado actual (desarrollo y limitaciones legales) de los productos criptográficos tanto en EE.UU. como en el resto del mundo, tema de gran importancia porque el comercio electrónico se desenvuelve en un medio diferente al limitado por las fronteras físicas.

En el cuarto capítulo se muestra el sistema modelado sobre el cual se trabajo. Es propuesto un sitio de comercio electrónico enfocado a vender música, mostrando las razones por las cuales se comercializa dicho bien, en especial para las circunstancias actuales en México. Se diseña un modelo teórico de cómo puede ser este sitio y el escenario en el cual se va a desarrollar, se definen los bienes a proteger y se utiliza una metodología para analizar los ataques y las correspondiente defensas necesarias con las cuales se esquematiza toda la estructura teórica del sistema modelado

El quinto capítulo contiene la documentación del sitio Web desarrollado en el trabajo de tesis. Se resumen las tecnologías y lenguajes de programación utilizados para el desarrollo del sitio "Web" así como las aplicaciones asociadas. Se esquematiza la estructura y funcionamiento del sitio de comercio electrónico programado a partir del modelo propuesto

Los resultados del presente trabajo de tesis se muestran en el sexto capítulo. Se dan las consideraciones necesarias (evaluación del tamaño de llave y tipo de algoritmo ha usar) para utilizar la criptografía en base al modelo de comercio electrónico desarrollado. También se detallan hechos y problemas de interés surgidos durante la fase de programación de las aplicaciones correspondientes; así como las áreas en las cuales se podrían desarrollar futuras tesis sobre este mismo tema. Por último se muestra la importancia de integrar herramientas criptográficas y no criptográficas para crear una solución cabal a las necesidades de seguridad informática para el comercio electrónico.

Las conclusiones del trabajo realizado se dan en la sección correspondiente.

Los anexos son un conjunto de resúmenes que le permiten al lector conocer con mayor profundidad algunos de los temas importantes de esta tesis, sin necesidad de recurrir a otras fuentes. Los tópicos tratados son:

- *El modelo de seguridad de Java.* Se muestra la evolución, funcionamiento y principales componentes del modelo de seguridad del lenguaje Java para crear aplicaciones distribuidas por Internet.
- *Protección de las comunicaciones en las redes de datos.* Se detallan las principales formas de proteger la comunicación de información a través de redes de datos, desde la perspectiva del modelo de capas OSI.
- *Equipos y dispositivos de seguridad para redes de datos.* Se expone en forma breve el concepto, clasificación y funcionamiento de los "firewalls" y sistemas detectores de intrusos; los cuales empiezan a ser un componente de suma importancia para la defensa de las redes de datos y la información que viaja por ellas.
- *Medios de transporte.* En esta sección se resumen los principales protocolos utilizados para las distintas aplicaciones de Internet.
- *Interfaz Java-JavaScript.* Se explica, en forma breve, como se pueden crear páginas "Web" activas, usando JavaScript como lenguaje interfase para applets y subrutinas escritas en Java
- *Factores a considerar al comprar por Internet* Se enlistan los principales factores, situaciones y características que un cibernauta debe considerar al comprar por Internet.
- *Manejo de audio en Java.* Dado que este trabajo de tesis se basa en manejar música por medio del lenguaje Java, este anexo tiene por finalidad mostrar el funcionamiento de la arquitectura del lenguaje para dicho fin.

Además, el presente cuenta con un pequeño glosario con los términos, y su significado, más utilizados en el ciberespacio y en la seguridad informática.

Al final se tiene la bibliografía y referencias electrónicas utilizadas durante el desarrollo del trabajo de tesis. Esta sección puede ser de utilidad como guía de consulta para los lectores interesados en profundizar en un tema específico, debido a que se utilizaron fuentes de información disponibles al público. La simbología [XX] y [XX,Y ..Y] significa. 'XX' el número asignado a una referencia particular y 'Y ..Y' la página(s), tabla(s), o sección(es) de la referencia marcada.

1.2 Términos utilizados

Dado que usamos el lenguaje para ordenar nuestros pensamientos e información y para comunicarnos con los demás, donde cada uno asigna un siginificado a las palabras empleadas; consideramos necesario mostrar el concepto de los términos más importantes que utilizamos a lo largo del presente trabajo, para crear una base común con el lector y poder alcanzar el objetivo propuesto con este documento.

Es importante señalar que casi toda la información sobre los temas de esta tesis: bits, cifrado, redes de datos y comercio electrónico; han surgido y son ampliamente desarrollados por la cultura angloparlante (destacando los vecinos EE.UU.). Por ello, el lector podrá ver en el presente términos que no fueron traducidos al español mientras que otros sí. La razón es que buscamos preservar la idea y en algunos casos su traducción no existe, es muy rebuscada o ambigua en nuestra lengua.

Utilizando [58, 115] vemos que los términos **autenticar**, **autentificar** y **autentizar** son sinónimos y significan: *acreditar, autorizar o legalizar jurídicamente*. Cualquiera puede ser utilizado para traducir la palabra "authenticate".

El término **implementación** ha sido adoptado por la Real Academia de la Lengua Española en la 21ª edición del *Diccionario de la Real Academia Española* [17, 23]; siendo el mejor equivalente para "implementation" (*llevado a cabo o puesto en práctica*).

Otro término que usamos es el de "cryptographic engine" (a veces abreviado "crypto engine"), el cual se utiliza bastante para definir las herramientas criptográficas necesarias a usar en el modelo del sistema de comercio electrónico propuesto en esta tesis. Jaworski y Perrone establecen las siguientes definiciones:

- Un "cryptographic engine" *representa un algoritmo criptográfico particular y el conjunto de parámetros de dicho algoritmo, el cual realiza una función criptográfica* [12, 42].
- Diferentes clases de "cryptographic engines" existen, y los diferentes algoritmos implementados por estas diferentes clases de "engines" (máquinas) tienen diversas características de seguridad, desempeño, costo de licencia y fuerza o calidad de protección (QOP, Quality Of Protection) [12, 11].

Se puede utilizar **máquina criptográfica** como un término equivalente, pero evaluamos que es más recomendable utilizar el término en inglés porque gran parte de la concepción y documentación de la sección criptográfica del modelo de seguridad de Java (el JCA y el JCE) está definida con dicho término. Ejemplo de ello son los esquemas de encriptación definidos en las figuras 1.2, 1.3, 1.4 y 1.5 de [12] (el anexo A del presente documento es un resumen del modelo de seguridad de Java, y si se desea conocerlo a detalle recomendamos especialmente leer todo [12] así como [48], [49], [50], [51] y [52]).

Como se notó anteriormente, este término fue concebido y utilizado ampliamente en otras culturas; iniciándose y ampliándose su uso al crearse y propagarse las máquinas de cifras basadas en rotor. Su concepción sistémica de "caja negra" ha perdurado hasta nuestros días, donde ya no usamos los dispositivos mecánicos criptográficos, en el diseño y uso de las nuevas herramientas protectoras ("software" y "hardware") de la información.

Los términos **cifrar** y "**cipher**" tienen el mismo significado: escritura secreta (consulta a [58, 224] y [57, 146]). Pero en ninguno de los diccionarios consultados de la lengua española, de la lengua inglesa y de español-inglés e inglés-español se encontraron las palabras **encriptación** o "**encryption**". Sin embargo es IMPORTANTE mostrar lo siguiente: el término "**encryption**" es sumamente utilizado en la cultura anglosajona, en muchos casos como un sinónimo a "cipher", y varios investigadores del área le han asignado una concepción propia; muestra de ello:

- Bruce Schneier define en [18, 1] que
  1. "**Encryption**" es el proceso por el cual se cambia la apariencia de un mensaje (llamado *texto en claro*) para ocultar su substancia (la información). Un mensaje **encriptado** es llamado *texto cifrado*

2. "**Decryption**" es el proceso por el cual un *texto cifrado* se transforma en texto en claro (en forma más detallada: el texto cifrado es transformado en texto descifrado; y si se utilizaron los algoritmos, llaves y parámetros correctos y no estaba dañado el *texto cifrado*, el *texto descifrado* es igual al *texto en claro*).

Es importante destacar que este autor utiliza proceso, lo cual significa [56, 279] [57, 579] [58, 841]: *serie de fases de un fenómeno, evolución de una serie de fenómenos, tratamiento de la información, gestión, serie de acciones u operaciones dirigidas para obtener un resultado particular.*

Jaworski y Perrone también utilizan la idea de proceso en [12, 11]: "En ocasiones el proceso de generar material cryptográfico es referido, en general, como procesamiento criptográfico."

- También se utiliza "**encryption**" para conceptualizar el contexto o marco de referencia y la implementación de los algortimos criptográficos.
  1. El ejemplo más claro lo dan Jaworski y Perrone en [12, 11], quienes unen estas ideas con la de proceso al definir la criptografía como *la ciencia base, atrás del proceso de tomar datos o código y pasarlos a través de una "cryptographic engine" para general material criptográfico* [12, 11]. Y cuando ellos aplicaron esta concepción en la explicación del esquema de un sistema criptográfico, vemos [12, 12]: *Si la salida de una "cryptographic engine" representa los datos de un texto cifrado, uno puede transmitir o almacenar dicha información con la seguridad de que la confidencialidad de dichos datos esta preservada. El proceso inverso puede correr estos datos a través de otra "cryptographic engine" y convertir el texto cifrado en texto en claro... El proceso de creación de texto cifrado en este contexto* (al usar "crypto engines", los cuales implementan algoritmos) *es referido como "**encryptation**", y la conversión de texto cifrado en texto en claro es referido como "**decryption**".* Es importante notar que "context" (contexto) significa: *las circunstancias que engloban un acto o evento* [57, 173].
  2. Otro ejemplo muy demostrativo es Bruce Schneier, quien al hablar del ocultamiento de la información en una situación específica, utiliza el término "**encryption**". Como ejemplo tenemos [18, 216-221] donde define las dos formas básicas de protección de datos en redes de comunicación: "link-by-link encryption" y "end-to-end encryption". Y es él quien utiliza "**cipher**" cuando analiza las características y modos de trabajo de los algoritmos criptográficos a nivel teórico [18, 10-12] [18, 189-211] [18, 379-388].
  3 Menezes, van Oorschot y Vanstone en [15, 11-12] definen a "**cipher**" como un "**encryption scheme**" (esquema de **encriptación**); y la palabra "**encryption**" la utilizan para definir todos los entes resultantes de relacionar elementos con algoritmos criptográficos Consideramos que estos autores también relacionan la idea de proceso e implementación con "**encryption**" en estas definiciones, ya que a "**cipher**" le estan asignando la idea de bosquejo, delineación o plano de la implementación [56, 142] [57, 649].
  4 Es muy importante destacar que todos los autores antes mencionados muestran estos conceptos y definiciones desde la perspectiva de aplicar la criptografía. Son los autores de "Applied Cryptography", "Handbook of Applied Cryptography" y "Java Security Handbook" (en el primer libro se expone código en lenguaje C, en el segundo se plasman los algoritmos tanto en esquemas como en pseudo-código y en el tercero se manejan las implementaciones criptográficas en lenguaje Java).

Por lo cual consideramos muy recomendable analizar la factibilidad de usar los términos **encriptación** y **desencriptación** como la traducción a "**encryption**" y "**decryption**", con el fin de conceptualizar *la implementación de un algoritmo criptográfico para crear un proceso que permita el cifrado o descifrado de datos en un marco de referencia específico* Término sumamente necesario para la ingeniería en donde se deben aplicar los conocimientos a una situación real con características bien definidas

Por otra parte, en lo que respecta al término "applet" que se refiere a las aplicaciones pequeñas o limitadas creadas con el lenguaje de programación Java, podemos decir que este término puede ser traducido como "*aplicacioncita*" [19, 710]. Un "applet" es un programa pequeño diseñado para ser ejecutado desde otras aplicaciones (en este caso, un navegador de Internet). El diminutivo se aplica en el sentido de que el "applet" se baja a la máquina cliente y se ejecuta ahí de una manera segura; es decir, existen candados o limitantes que impiden que el "applet" lea o escriba archivos a los que no esta autorizada a acceder, y también no puede introducir virus o códigos que causen algún daño.

Por último, el término empleado para el conjunto de elementos básicos que toca la presente tesis. En este documento es usado "nuevo medio computadoras-Internet-WWW" pero existen muy diferentes nombres como "Mercado de la Información o Mercado Global de la Información" utilizado por Dertouzos, "Infraestructura Nacional de la Información" para una concepción local de la administración Clinton-Gore, el "medio de la comunicación-mundo" expresado por Mattelart, "Autopista de la Información" acuñado por los ISP, "Sociedad Global de la Información" por los europeos, "ciberespacio" por la comunidad hacker y cracker, o "La Red".

Creo que todos son útiles y correctos porque al usar cada uno palabras muy específicas podemos ver, escuchar, tocar y entender una percepción muy particular de este conjunto:

- El nombre "Mercado de la Información" permite entender la existencia del mismo comercio electrónico, y saber como evaluar los bienes informáticos.
- El de "medio de la comunicación-mundo" muestra el alcance y repercusiones en las relaciones sociales con este nuevo medio y la aplicación de la fórmula de las 5W (la cual se expresa en la sección 1.1.3).
- "La Red" nos da la idea de la gran capacidad de concectividad y la actual evolución en los medios de comunicación.
- "Autopista de la Información" bosqueja la estructura y funcionamiento básico asi como los peligros posibles por este nuevo medio.
- "Ciberespacio" define las nuevas fronteras y comunidades, así como una nueva percepción del tiempo y el espacio.
- "Nuevo medio computadoras-Internet-WWW", plasma los elementos básicos de un nuevo medio para expresarse, relacionarse, buscar, trabajar, recrearse sin limitaciones geográficas y la factibilidad de crear diferentes contenidos y separarlos de los diferentes medios de transporte y expresión

Otro análisis de los nombres se puede ver en [7, 40-41].

1.3 Objetivos específicos

A lo largo de este trabajo, se analizan temas tan variados y complementarios como son el comercio electrónico, la seguridad en redes, la protección de la información a través de algoritmos de cifrado, la evolución de Internet y algunas metodologías comerciales actualmente en uso mediante las que se estructura la seguridad tanto a nivel de lenguajes de programación como a nivel de dispositivos, sin embargo, para no perder el rumbo y contexto de nuestra investigación se decidió establecer los siguientes objetivos específicos:

- Obtener un esquema básico para la puesta en operación de un servicio seguro de comercio electrónico entre una empresa y un gran número de consumidores

- Establecer un marco de referencia mediante el cual se puedan relacionar las diversas necesidades de seguridad existentes en el comercio electrónico y las características de posibles atacantes; con los algoritmos de cifrado, la longitud de las llaves criptográficas a utilizar y los protocolos de seguridad.

1.4 Marco de Referencia

Las revoluciones de las telecomunicaciones y el procesamiento de información están creando una sociedad cuyas actividades y procesos cada día se basan más en la información electrónica. Los avances e interacciones de estos campos se han incrementado aceleradamente en los últimos años y se prevé un mayor desarrollo para los siguientes, con miras a penetrar más en la vida diaria de todos los entes que conforman nuestra comunidad.

El hombre, a lo largo de su historia, se ha preocupado por plasmar y registrar la información (ideas, hechos, conocimiento) fuera de su mente individual, comunicar esta información a sus congéneres, con el fin de que ellos puedan utilizarla en otro lugar y tiempo; y finalmente proteger dicha información, ya que la existencia de la sociedad implica amistad pero también enemistad. Paralelamente, la evolución de las sociedades humanas se ha debido en parte a su capacidad para comerciar productos, intercambiar ideas y experiencias; para lo cual se creo el lenguaje, la escritura y numeración; los sistemas de correo y transporte; los códigos crípticos y la encriptación; el trueque y el dinero.

1.4.1 Evolución de la información

La información es la comunicación o recepción de conocimiento o inteligencia; conocimiento obtenido de la investigación, estudio o instrucción [57, 382]. En la última década ha evolucionado la noción de información, pasando de ser sólo texto, imagen y video, al conjunto de procesos activos que transforman dichos elementos [7, 78] y [9, 36y43].

Los niveles de trato de la información son [7, 79]: recepción, procesamiento, producción, transmisión y almacenamiento. Y estas operaciones se realizan cuando la información se encuentra en dos formatos básicos [16, 78]

- **Formato analógico** cuando la información se almacena en medios tales como periódicos, fotografías y los discos LP; o es registrada a través de señales eléctricas analógicas, como en la TV y radio, así como en las tradicionales cintas magnéticas de audio

- **Formato digital**: donde la información es registrada en medios electrónicos y codificada en bits. Entendiéndose por bit, lo que Nicholas Negroponte define como: "... el elemento más pequeño de información, que describe el estado de algo: encendido o apagado, verdadero o falso. ., para fines prácticos consideramos que un bit es un 1 o un 0" [16, 34].

El gran avance del formato digital es que. **los bits son bits** [16, 69]. No importa el tipo de información representada (una canción, un vídeo, un libro o el reporte del clima local), siempre podrá ser transmitida, recibida, almacenada y/o procesada por cualquier dispositivo que maneje bits (no importa si el equipo fue creado hace 15 años, hoy o dentro de 50 años).

Esta ventaja de la digitalización permite el diseño y uso de sistemas electrónicos digitales escalables (la capacidad de agregar y/o cambiar componentes para obtener una mejora en capacidad o rendimiento) y graduables (la capacidad de dar diferentes resoluciones al usuario final, sin modificar la información), características inexistentes en los medios analógicos (para los cuales

una mejora implica sustituir el viejo sistema por uno nuevo). Permitiendo la existencia de los sistemas abiertos [16, 64-67].

Otras consecuencias de manejar la información en formato digital, y las cuales son gran importancia para el presente proyecto, se presentan en los siguientes apartados

1.4.2 Consecuencias en el manejo de la información

En las últimas décadas se ha vista la trascendencia de manejar la información en formato digital, pues ahora su registro ha cambiado del almacenamiento en papel (letras) a el almacenamiento magnético (bits). Sin embargo, este cambio en la forma de almacenar la información ha transformado la habilidad de manipular (copiar, alterar y/o procesar) la información en este formato [15, 3]:

- Uno puede hacer miles de copias idénticas de un trozo de información almacenado electrónicamente; y cada copia puede sustituir al original sin problema alguno.

- Sobre la misma porción de información se pueden hacer uno o un millón de alteraciones sin que se pueda saber cuales han sido los bits alterados, aumentados o eliminados; ni cuando fueron realizados estos cambios ni quien los hizo.

Al mismo tiempo, la comunicación de la información ha evolucionado radicalmente: de ser transportada en materia (papel) a ser transmitida por energía (ondas libres o guiadas), realizando actividades insospechadas:

- Enviar una misma información a muchos y distantes usuarios distribuidos por toda la faz del planeta, en cuestión de segundos y a un costo bastante bajo.

- La capacidad de comunicación bidireccional y en tiempo real entre dos puntos cualesquiera de la superficie terrestre y espacio cercano.

- La evolución de las redes de comunicación masiva interactivas, donde todos los participantes son emisores y receptores con la capacidad de crear, procesar (filtrar, clasificar, priorizar y manipular), y compartir información y recursos.

De igual forma, la protección y la agresión al secreto de la información se han alterado drásticamente con la aparición de la computadora y las teorías de la información, de la complejidad y de los números:

- Para la defensa se abandonó el uso de la criptografía básica, donde la principal defensa era la ignorancia del adversario; para empezar el diseño y empleo de la criptografía matemática: números, algoritmos y poder de cómputo.

- Pero la capacidad del enemigo también ha evolucionado a pasos agigantados, ya que al desarrollarse nuevas herramientas y conocimientos, y más poder de cómputo; los ataques tienen ahora alcance transfronterizo, así como la detección y explotación de las debilidades y fallas en la implantación de los sistemas de protección, se añaden a las técnicas clásicas de corrupción de personas e intercepción de los mensajes.

1.4.3 Evolución en el contenido de la información

La información en bits permite generar nueva información a partir de la disponible, posibilitando un mejor uso de ella. Por lo cual ahora las fronteras de la economía de usar bits son los medios que la almacenan, la transmiten, la reciben y la procesan.

Antes, con la información en formato analógico, la diversidad de medios (radio, TV, imprenta) equivalía a diversidad de contenidos. Ahora, la información en formato digital permite separar el contenido o idea (información en bruto) de sus medios, de expresión y de transporte, usados para comunicar la idea Esta nueva forma de manipular la información aclara el hecho de que la información no es lo mismo que el soporte físico que la transporta [16, 76-81].

Así, la información en formato digital no esta limitada a un medio específico una vez que abandone el transmisor o estación emisora como bits, se personalizará a las preferencias del receptor para ser almacenada, utilizada y transformada de maneras diferentes por programas de computo distintos.

La separación de la idea de su medio de transporte y su medio de expresión asienta uno de los pilares del comercio electrónico: La información digitalizada permite presentar el mismo contenido en diferentes medios de expresión y a diferentes mercados, y acceder a ellos por uno (optimizando el ancho de banda) o varios medios de comunicación [16, 72].

A partir de la digitalización, aparecen nuevos contenidos, nuevos competidores, nuevos modelos económicos; y probablemente una nueva industria integrada por proveedores de información, servicios y entretenimiento. La digitalización crea el potencial para que se originen nuevos contenidos a partir de una combinación nueva de las fuentes, ya que los bits se pueden combinar sin esfuerzo para ser utilizados y reutilizados juntos o por separado [16, 37-39] [16, 82-83].

Este diferenciación entre el contenido, el medio de transporte y el medio de expresión, asienta el primer paso necesario a realizar para entrar a vender un producto a través del comercio electrónico la necesidad de un análisis que siga la fórmula de las 5W (claves de la comunicación de masas) *"Who says What in Which channel to Whom with What effect?"* (¿Quién dice Qué a Quién por Cuál canal y con Qué efecto?) [14, 108].

1.4.4 Computadoras, Internet y el WWW

Las computadoras, el Internet y el WWW han resultado ser, en conjunto, el fenómeno social y económico más importante de la segunda mitad de la década de los 1990's [4, VIII].

Sintetizando las ideas de [7, 20], [7, 36], [7,64] y [16, 64]; se puede considerar a Internet como un sistema postal para el envío de información en bruto entre los ordenadores de todo el mundo, es decir, el medio de transporte que se ocupa del traslado, a la velocidad de la luz, de bits. Y pensemos en la WWW (World Wide Web) como el mejor medio de expresión y extensión de la era de la información; al ser una manera específica de utilizar este sistema para:

- La búsqueda y obtención de información en espacios informáticos muy remotos.
- La comunicación con alcance mundial, al permitir a un individuo u organización colocar en una o varias "páginas de presentación" la información que le interesa hacer circular
- La asociación de diferentes usuarios, por medio de palabras claves de sus páginas o intereses comunes; sin importar la distancia física entre ellos

La WWW constituye una lección. para el público en general, la eficiencia técnica no significa mucho; lo que en realidad interesa es la facilidad de uso y la simplicidad para hacer circular la información.

1.4.5 Infraestructura de otra infraestructura

Así como la infraestructura eléctrica, generó innovaciones y nuevos productos que aprovechaban las ventajas de la electricidad (tales como el teléfono, la radio y la televisión), los cuales a su vez revolucionaron nuestro sistema económico y nuestro estilo de vida; la infraestructura eléctrica ha permitido el surgimiento de la infraestructura de comunicaciones Internet y el progreso técnico de la informática para crear el movimiento socioeconómico del siglo XXI [9, 144].

Gracias a [7, 25-35], [7, 67-73] y [9, 144] se puede esquematizar rápidamente la infraestructura de Internet, la cual se caracteriza por:

- Amplia disponibilidad para los usuarios.
- Facilidad de uso.
- Multiplicable, escalable y conectable.
- Permite realizar muchas actividades independientes.

Donde los participantes son los sectores convergentes en este medio:

1. Compañías de "hardware".
2. Compañías de "software".
3. Compañías transportadoras de información.
4. Compañías generadoras de información y entretenimiento.
5. Consorcios normalizadores.

Y los millones de usuarios que favorecerán con su dinero a las compañías que entreguen sus voces y les ayuden a comprar, vender, trabajar, vivir y jugar en la misma arena; generando la mayor parte de contenido y tráfico en la Red.

La gran diferencia entre la era de la información y la era industrial radica en que no se pueden fabricar bienes complejos en una casa; pero sí se puede crear información, intercambiarla libremente y venderla (ya no es necesario estar confinado a una oficina).

En el momento en que esta infraestructura de conectividad, haya alcanzado su masa crítica, dará lugar a la aparición de nuevos programas y nuevo equipos físicos que cambiarán la manea de vivir de las personas. Para esas personas, el recurrir a la Red para obtener noticias, para aprender, para distraerse, para comprar y para comunicar será como un reflejo natural.

1.4.6 Surge un nuevo medio

Partiendo de la idea original de [16, 54], existe una evolución de las redes masivas de comunicación de usuarios receptores pasivos a redes masivas interactivas

Las computadoras (en especial las personales), el Internet y el WWW crean un medio de "varios a varios". No es sólo un medio de difusión o de información masiva unidireccional, como la televisión, la radio y la prensa; los cuáles son fundamentalmente medios "uno a varios". Esto significa que cada persona conectada a este medio puede ser tanto emisora como receptora del contenido de otros usuarios conectados al mismo.

La importancia de esta diferencia en la topología red-medio es el reflejo de una distinción fundamental en la concepción de la conducta humana En una "red tradicional" de difusión unidireccional, la gente es receptora pasiva del contenido, en una "red interactiva", la gente

contribuye al contenido y, por tanto, ejercita mayor control sobre éste. Y este concepto en el comercio electrónico significa que tal control aumenta el poder de negociación de los compradores ante los vendedores [4, 13-15]. Este nuevo medio se esta integrando a la sociedad para ser una nueva via de expresión para las masas.

1.4.7 Expandiendo las fronteras de la empresa

Mientras que estamos viviendo en la era de la información, la mayor parte de la misma nos llega en forma de publicaciones en papel, diarios, revistas y libros. Nuestra economía podría estar moviéndose hacia una economía informática, pero medimos el comercio y escribimos nuestros balances pensando en materia [16, 31]. La OMC mide la productividad de un país en base a la producción industrial, la razón de ello es que tradicionalmente el comercio mundial siempre consistió en el intercambio de mercancías. Cuando uno pasa por una aduana, se declaran los bienes materiales que se transportan, no los bits [16, 24].

Esto esta cambiando rápidamente. El lento manejo humano de la mayor parte de la información (envasada en libros, revistas, periódicos, discos ópticos y medios magnéticos) está por convertirse en la transferencia instantánea y a bajo costo de datos electrónicos, que se mueven a la velocidad de la luz. De esta manera, la información se vuelve universalmente accesible [16, 24].

Y el cambio se ha acelerado con el nuevo medio computadoras-Internet-WWW, pues este esta redefiniendo las fronteras entre las organizaciones, y entre personas y organizaciones [9, 171]; ya que el flujo de la información que permite, salta las fronteras físicas entre las organizaciones y dentro de la organización, para que se realicen actividades en un nivel no restringido físicamente [9, 163]. Por lo cual hace posible que una empresa se estructure de la manera más eficiente.

La Red hace posible que las grandes empresas funcionen como si fuesen pequeñas y más flexibles; y que las pequeñas abarquen lo mismo que si fuesen mucho más grandes [9, 171].

La pequeña y la mediana podrán aprovechar la capacidad de trasladar fronteras que tiene el medio computadoras-Internet-WWW, en el sentido de operar como si fuesen mucho más grandes, y ello sin necesidad de contratar más empleados ni de alquilar más despachos. Una compañía pequeña pero dotada de un conocimiento experto puede funcionar virtualmente como una gran compañía, sin el costo fijo que representa una plantilla numerosa de empleados estables [9, 165].

El comercio electrónico motiva la subcontratación de empresas ("outsourcing"): Un principio importante de la ingeniería de procesos es que las empresas deben centrarse en sus competencias troncales o críticas y subcontratar todo lo demás (procesos no críticos). El hecho de acudir a fuentes externas ha significado la posibilidad de moderar el crecimiento de la plantilla fija de una empresa y reducir nuestros gastos generales, sin que ello frene el crecimiento de la capacidad operativa. Según el alcance del proyecto (corto o largo plazo) y su carácter procesal (crítico o no), será si se contrata personal para la plantilla estable, o se deja en manos de servicios externos [9, 163-167]

1.4.8 Cambios para el comercio electrónico

Es importante hacer notar los tres grandes cambios empresariales que sustentan al comercio electrónico [9, 93].

1 Cada vez más transacciones entre empresas y consumidores, entre empresas y empresas, y entre el consumidor y la Administración (gobierno) serán transacciones digitales en autoservicio. Los intermediarios tendrán que convertirse en suministradores de valor añadido o perecer

2. La primera función de valor añadido de cualquier empresa será el servicio al cliente. La intervención humana en dicho servicio pasará de las tareas rutinarias y de bajo valor añadido a otras de asesoría personal sobre temas importantes para el consumidor: sus problemas o sus deseos.

3. El ritmo de las transacciones y la necesidad de dispensar una atención más personalizada al cliente obligará a la adopción interna de procesos digitales por parte de las empresas, si es que no los han adoptado por razones de eficiencia. Las compañías tendrán un sistema nervioso digital que transforme sus procesos operativos internos, con objeto de adaptarse al cambio constante que imponen las demandas de los clientes y la competencia.

Cambios que, poco a poco, están consolidando una nueva economía [16, 36]: **la economía de bits**, determinada en parte por las limitaciones de los medio de almacenamiento, a través de los que son transmitidos o por los cuales son procesados. Donde creamos nuevas actividades y servicios, y consecuentemente, nuevas necesidades de protección.

Por lo anterior, esta sociedad en crecimiento, en la cual se almacena, procesa y transmite la información en forma electrónica, necesita las herramientas que le permitan salvaguardar esta "nueva materia prima", buscando que dicha defensa resida en la propia información digital y sea lo menos dependiente del medio físico en el cual se encuentre. La criptografía es una de estas herramientas y sus aplicaciones se volverán componentes críticos y de gran difusión para este modo de vida intensamente informatizado [15, "forward" y 2]

2 Comercio Electrónico

El comercio, junto con los campos del entretenimiento, de la atención médica, y la informatización de las empresas, explotarán rápidamente las tecnologías de la información. La evolución del mercado de la información debutará en estos sectores, en parte porque la demanda del consumidor es grande, las capacidades de la infraestructura están a la altura de las demandas y ya existe una actitud seria en estas áreas. Al mismo tiempo, estos factores tocan el corazón de la economía industrial.

Las finanzas y la banca se cuentan entre los primeros servicios que se han unido a gran escala al mercado de la información. En EE.UU. han aparecido ya la banca y la bolsa domésticas de valores, las cuales permiten extender cheques, transferir dinero y comprar y vender valores bursátiles desde nuestra casa.

2.1 Empresa digital

Las grandes organizaciones han empleado ordenadores desde la década de los 1980's, tanto para comunicar datos de sus empresa, memorandos electrónicos e incluso imágenes [7, 28]. Pero al mismo tiempo era prohibitivamente caro el conseguir información rica, y además no se disponía de instrumentos para analizarla y difundir masivamente dichos análisis [9, 15].

Las transacciones automatizadas entre organizaciones se desarrollaron a comienzos de los 1990's, y los "primitivos" ordenadores personales de principios de la década de los 1980's se han convertido en máquinas útiles y poderosas, propiedad de pequeñas empresas y multitud de individuos. La automatización de la empresa ha llegado a la mayoría de edad y ha conducido al aumento de la productividad y a reducir el uso del papel y los viajes para ciertas actividades rutinarias [7, 28].

Los instrumentos y la conectividad de la era digital ponen en nuestras manos los medios para obtener información, compartirla, analizarla, sintetizarla y actuar en función de ella de muchas maneras nuevas y notables. Por esta razón, muchas de las tradicionales maneras de hacer negocios están cambiando [9, 15].

2.1.1 Situación actual

Las empresas se enfrentan hoy a competidores de todo el mundo. Todos estos fabricantes emplean la misma materia prima, la mecanizan con las mismas máquinas herramientas, tienen procesos de producción parecidos y soportan costos de transporte semejantes. Las diferencias entre ellas son y serán los procedimientos que hacen uso intenso de la información y que resultan beneficiados con los procesos digitales [9, 34]

Ahora, en este mercado global, la diferencia más importante entre las empresas consiste en como realizan su trabajo con la información. Ganar o perder dependerá de cómo capten, gestionen y utilicen la información para saber si necesitan aumentar sus controles de calidad, rediseñar sus sistemas de producción, mejorar su publicidad, modificar la interacción entre distintos departamentos, cambiar sus canales de venta o transformar su asistencia técnica, etcétera. Los ganadores serán los que integren todos sus sistemas y herramientas informáticas en un solo gran

sistema, de manera que la información circule con facilidad dentro y fuera de sus empresas y se maximice constantemente el conocimiento [9, 25].

Las empresas triunfadoras del próximo decenio serán las que utilicen los medios digitales para reinventar su propio funcionamiento. Esas compañías actuarán con eficiencia y hallarán vías positivas de contacto directo con sus clientes y con su entorno para detectar los cambios [9, 21-23].

2.1.2 Flujo de información y Sistema Nervioso Digital

En el fondo, la mayoría de los problemas de las empresas son problemas de información: nadie sabe obtenerla y/o utilizarla bien [9, 14]; y sin la información necesaria para identificar el problema, es difícil resolverlo. Por ello, las empresas deben construir un flujo de información que les aporte conocimientos rápidos y tangibles en cuanto a lo que ocurre realmente.

En general, se han utilizado los sistemas informáticos para automatizar procesos clásicos (monitorear la producción, llevar la contabilidad). Pero todavía son muy pocas las empresas que utilizan la tecnología digital para crear procesos nuevos que mejoren radicalmente su funcionamiento, extraigan el pleno rendimiento de la capacidad de su plantilla y les confieran la velocidad de reacción que necesitarán con objeto de competir en el emergente mundo empresarial de alta velocidad [9, 13-14].

Esta reingeniería en los procesos para crear el flujo de información no es una moda, es una necesidad; debido al ritmo de las transacciones económicas y la necesidad de una atención al cliente más personalizada (bases para el comercio electrónico), harán necesario adoptarlos internamente [9, 97].

Se necesita un flujo rápido de informaciones fiable para agilizar las actividades, elevar la calidad y mejorar la ejecución operativa; sacar el máximo rendimiento al personal y aprender de los clientes [9, 26].

Cuando el pensamiento y la colaboración reciben una ayuda significativa por parte de las técnicas computarizadas tenemos un Sistema Nervioso Digital, SND (sistemas y herramientas informáticos y digitales integradas en un solo gran sistema), el cual consiste en los procesos digitales avanzados utilizados por los trabajadores de calificación superior para analizar, pensar, mejorar la toma de decisiones, reaccionar y adaptarse [9, 38].

El SND debe sintetizar hechos (por medio de las aplicaciones de análisis) para que los usuarios distingan las tendencias. Además debe hacer posible que los datos y las ideas broten desde los escalones inferiores de la organización, donde se generan y contestan la mayoría de las preguntas del negocio. Por lo tanto el flujo de la información debe integrar a todos los trabajadores de todos los niveles; y en general potenciar a todos sus componentes [9, 17-18].

2.1.3 Estrategias

Condensando [4, 16-17] y [7, 252], tenemos las siguientes estrategias para obtener éxito en el actual mundo, las cuales se basan en los flujos de información y motivan la entrada al comercio electrónico:

- La primera receta para las organizaciones que aspiran a utilizar el mercado de la información para el comercio electrónico: permanecer en contacto con los pares, los grupos de interés común, las asociaciones profesionales e incluso con los competidores, y

desarrollar "e-forms" (formas electrónicas) sencillos en los que todos convengan en que ahorrarán tiempo y dinero a través de la automatización.

- La sobrevivencia de una compañía en este nuevo medio depende de que ésta mantenga contacto constante con los clientes. Y que ésta comunicación debe guiar el rumbo estratégico de la empresa.

- Empiece con el mercado, no con la tecnología. Las empresas triunfadoras estudian primero el mercado para ver si los posibles ingresos serán suficientemente cuantiosos para justificar la inversión.

- Busque clientes que tengan un incentivo para regresar constantemente a un proveedor. Identifique tantas maneras como sea posible de que tales clientes vuelvan continuamente a su compañía, lo cual implica rediseñar procesos. Establecer un sistema con base Web que cree muchos vínculos estrechos con sus clientes.

- Crear una Extranet como una red extensa que abarque a la empresa, sus proveedores y concesionarios y diseñar una Intranet para la interacción entre oficinas centrales y fábricas distribuidas a nivel mundial.

2.2 Definición de Comercio Electrónico

El comercio electrónico es la realización de transacciones electrónicas e intercambios comerciales empleando medios electrónicos como Internet [4, 132]. Es un modelo emergente de ventas y de herramientas de comercio, en el cual los compradores pueden participar en todas las fases de una decisión de compra mientras navegan a través de sitios web. La forma en como opera el comercio electrónico permite al cliente acceder a mayor información del producto que esta interesado en adquirir, comprar bienes que de otra forma no podría, así como utilizar medios de financiación novedosos y seguros.

El acceso del público en general a Internet es el detonador que ha permitido el despegue de este fenómeno, trayendo consigo una verdadera revolución en el ámbito del comercio global y la economía. Su influencia está notándose tanto en las empresas beneficiadas por una presencia global y acceso a nuevos mercados y clientes; como en la sociedad, por un mayor y más rápido acceso a todo tipo de información y productos.

Los mismos medios electrónicos también han permitido el uso de la transacción híbrida, aquella en donde el comprador usa Internet para reunir información, pero realiza su compra por un canal diferente (pedido por teléfono o visitando la tienda física) [4, 133]. Estas transacciones no cuentan como comercio electrónico, aun cuando deben considerarse facilitadas por la Red.

2.2.1 *Etapas y participantes de una transacción electrónica*

Una transacción electrónica debe seguir las siguientes etapas [4, 133]:

1. Una persona se sirve de la WWW para recopilar información que le ayude a decir qué producto o servicio comprar.
2. La persona transmite por WWW la información de pago (por ejemplo, el número de su tarjeta de crédito) al vendedor.
3. El vendedor procesa la información de pago y entrega el producto o servicio al cliente

Estas transacciones se realizan con la participación de 3 entes: negocios (organizaciones empresariales), consumidores (particulares) y la Administración (gobierno).

2.2.2 Beneficios del comercio electrónico

El negocio que vende sus productos a través de Internet se beneficia de una serie de ventajas que los canales tradicionales no ofrecen. Entre ellas se encuentran:

- Los costos de iniciar un sitio en el Internet son menores que los de instalar un establecimiento físico como punto de venta.
- Con el Internet se puede servir a los clientes de manera personal, permitiendo formar una relación estrecha con ellos y ayuda en el establecimiento de una estrategia de crecimiento futuro.
- Acceso al mercado global.
- Presencia mundial, a toda hora y todos los días.
- Menores costos de intermediación.
- Bajo costo en conseguir nuevos clientes a diferencia de medios de publicidad tradicionales (como la radio y TV).

2.3 Cliente Digital: La Perspectiva del Consumidor

Se tiene un cliente digital cuando existe un flujo digital de información que conecta al cliente con los sistemas de soporte informático de una empresa.

En la perspectiva de un cliente, el propósito de un sistema de comercio electrónico es permitirle localizar y comprar un bien deseado o servicio en Internet cuando está interesado en hacer la compra. Su función no es más que una tienda virtual.

La Red permite al consumidor, encontrar con facilidad un producto con determinadas características y dentro de un determinado rango de precio. También beneficiará a las personas que intentan comprar o vender artículos difíciles de encontrar [9, 102].

Los compradores de Internet se comportan de manera diferente que los influidos por otros medios. La gente que compra productos por medio de Internet es mucho menos susceptible a que los proveedores la "convenzan". Los compradores de Internet se autodirigen Deciden que quieren realizar una compra y usan Internet para recopilar información. Esta información contribuye a que concreten mejores tratos de los que lograrían en otras circunstancias [4, 13-15] y administren mejor la economía doméstica [9, 147] La mejor información del comprador también aumenta su poder de negociación y disminuye las utilidades del proveedor, y consecuentemente su rentabilidad [4, 13-15].

Los clientes que compran por Internet son leales a sus propios intereses. El nivel excepcionalmente elevado de rotación de clientes (alrededor del 10%) dificulta mucho fomentar la lealtad en el cliente y, por tanto, hay una batalla encarnizada constante entre los portales WWW y los usuarios de Internet. Los portales WWW invierte recursos cuantiosos en mercadotecnia para atraer a los usuarios de Internet. Por lo cual también se reducen las utilidades del proveedor [4, 13-15].

Hoy, pese a los instrumentos de búsqueda todavía imperfectos, el consumidor puede acudir por su cuenta a la Red y hallará buena parte de la información que busca. La Red también facilita al

comprador una visión panorámica de los productos disponibles en el mercado y facilita las comparaciones de precios y calidades. Además el comprador puede hablarle de sus propias necesidades al vendedor, para que éste ajuste su oferta o le venda otros productos relacionados. La Red es un instrumento maravilloso para que el consumidor busque la mejor transacción posible [9, 100].

2.3.1 ¿Qué atrae a los clientes digitales?

El servicio omnipresente. El servicio al cliente será la función principal de valor añadido en cualquier sector de actividad. Por ello es indispensable diseñar el servicio en-línea a manera de que sea ubicuo, presente en diferentes sitios del mismo medio (Internet), para brindar dicho servicio en cualquier lugar y en cualquier momento [9, 97 y 131].

La virtualidad interactiva. Internet da un nuevo espacio de flexibilidad al cliente, ya que la naturaleza virtual de este medio permite cualquier transacción que el cliente desee [9, 95-96]. Y es esta "virtualidad" la que permite darle el trato interactivo que desea el cliente [9, 130], y ser el gran gancho para atraer clientes. Mientras más dinámico e interactivo sea un sitio, se generará más actividad comercial lo cual implica más reservaciones, pedidos y facturación [9, 132].

Por lo tanto, las compañías que deseen incursionar en el comercio electrónico deberán:

- Desarrollar sus sitios y productos para que funcionen de manera intuitiva [9, 136].
- Dar un servicio personalizado con los criterios del cliente [9, 131].
- Usar aplicaciones con inteligencia artificial y no la automatización en bruto y fija [7, 38].
- Crear el viaje interactivo con ayuda de multimedia. Donde los "software" de uso de datos y de navegación van adaptando dinámicamente el sitio sobre la marcha de la sesión, de manera que cada visitante recibe una experiencia distinta del sitio y siempre la mejor adaptada a sus intereses [9, 131].
- Crear los nuevos servicios o, mejor aún, un sistema combinado de seres humanos y de máquinas que sea útil y más rápido para el cliente [7, 38].

2.4 Vendedor Digital: La Perspectiva del Comerciante

La función de un sistema de comercio electrónico es generar réditos más altos que el mismo comerciante lograría sin el sistema. Para que esto pase, el negocio electrónico deberá emular todos los procesos que el comerciante realiza físicamente para apoyar su tienda y, de la misma forma, la compra por catálogo también debe ajustarse perfectamente a una compra electrónica. La información del producto, sistema de inventario, servicio al cliente y capacidad de transacción, deberán ser iguales en el sistema electrónico y en el sistema real (incluso la autorización del crédito, cómputo del impuesto, el pago financiero y su envío).

Una ventaja del comercio electrónico es que puede ofrecen más servicios y negocios asociados en un mismo sitio. Esto es, se debe aprovechar el flujo de información posible dentro de Internet para contactar directamente con los clientes y crear un nivel de servicio que lleve de forma sencilla a nuevas ventas [9, 121].

Y no se debe de olvidar un hecho importante: se puede realizar publicidad por medio del cliente digital satisfecho, ya que su recomendación personal sigue siendo el medio más poderoso por el cual un producto o una compañía conquistan una reputación [9, 119].

2.4.1 Enfocarse en el cliente

Las compañías están cambiando para que sus organizaciones correspondan a las necesidades del cliente; así las divisiones de servicios especializados evolucionan en conjuntos más integrados de servicios que encajen unos con otros en un esfuerzo por conectar con las necesidades de un individuo, familia o compañía a medida que atraviesan sus fases normales de desarrollo [7, 259]. No siempre es necesario saltarse a los intermediarios, sino que se les debe integrar para satisfacer mejor las necesidades del cliente La compañía puede proporcionar lugares especiales en su sitio Web a los agentes que se enfocan en segmentos muy especializados del mercado [9, 133].

2.4.2 Aprovechar los Multimedios

El comercio vendrá a ser una combinación entre las interacciones a través de Internet (en línea) y el contacto personal; pues ambos se complementan. Los operadores hábiles combinarán ambos contactos en sistemas que proporcionen a los clientes las ventajas de ambos tipos de interacción. Lo cual implica definir claramente las situaciones y servicios a cubrir por cada contacto. Y con una infraestructura adecuada de información se podrá tener un contacto multimedia: navegar por las páginas Web contando con la presencia de un agente vía voz sobre IP [9, 137-138].

Creando un perfil de los clientes y aprovechando la evolución comunicativa de Internet, se puede pasar del monologo al diálogo en un sitio Web, de hablar a los clientes a hablar con ellos Ahora se debe pasar del diálogo al foro. Es decir, construir el perfil de nuestros clientes no sólo permite servirlos mejor, y proporcionarles sugerencias acerca de sus intereses en servicios o productos, sino también poner a nuestros clientes en contacto con otros [9, 132].

2.4.3 El atractivo para el cliente digital: la Domiciliación

Dentro de un par de años, la mayoría de las compañías ofrecerán el servicio de domiciliación electrónica, y las instituciones financieras, serán un sitio único que permitirá al cuenta-habiente (cliente individual o empresa) el despacho de todos sus recibos mensuales. Desde la página Web del banco, el consumidor pulsará sobre el icono de su compañía de tarjetas de crédito, o el almacén donde hace compras; o con la compañía de luz, lo cual le llevará directamente a la página HTML de esa compañía para verificar su estado de cuenta. Recibirá en línea más información acerca de lo que está pagando, en comparación con las actuales facturaciones sobre papel. Podrá buscar en el historial de la cuenta y de los pagos realizados. Para eso no será necesario escribir ninguna carta aparte; bastará con pulsar un botón de e-mail para cualquier consulta sobre un recibo. Y las vendedoras aprovecharán esa consulta para presentarle en su página los productos y servicios que vayan produciendo [9, 148].

2.5 Tipos de comercio electrónico

Existen diferentes criterios para clasificar al comercio electrónico.

1. Por el tipo de producto comercializado, entendiéndose por producto un bien o un servicio.
2. Por el tipo de participantes en la transacción, en especial el tipo de negocio que está presente:
    - vende sus propios productos o servicios,
    - es un sitio de información,
    - vende productos o servicios de otras compañías, y

- utiliza su sitio como otro canal de venta para complementar su negocio físico.

2.5.1 Tipos de comercio electrónico según el producto comercializado

Usando las definiciones de [7, 250-251] tenemos la siguiente clasificación:

Comercio electrónico indirecto. Implica la manipulación de la información que se necesita para el comercio de bienes físicos. Maneja la publicidad, la investigación, la venta, la contratación y otras funciones relacionadas con la información, aunque los bienes reales sean objetos físicos remitidos según los sistemas tradicionales de transporte.

Comercio electrónico directo. Implica bienes que son en sí mismos información y que se remiten directamente a través del mercado de la información. El aumento de la calidad de los dispositivos de salida --impresiones en color, altavoces de alta fidelidad, sistemas de realidad virtual, etcétera-- hará más atractivo este tipo de comercio electrónico. Y puesto que el aumento de la velocidad de entrega satisface la necesidad humana de gratificación instantánea, es probable que el comercio electrónico directo se convierta en un componente importante del mercado de la información.

2.5.2 Tipos de comercio electrónico según los participantes

Negocio a Consumidor ("Business to Customer", B2C). Las transacciones de empresa a consumidor son las que reciben más publicidad. Estos canales venden libros, discos compactos, servicios de noticias y asesoría, boletos de avión, computadoras; así como otros bienes y servicios de consumo [4, 134].

Es el escenario clásico del comercio electrónico: navegando por la red, un consumidor puede elegir cómodamente desde su casa u oficina y a cualquier hora del día entre una infinita variedad de bienes y servicios de compañías distribuidas por todo el mundo. Internet facilita el acceso a productos a su alcance en el mercado local, y a otros que no existen en su mercado (productos informáticos, música, etcétera). En el caso de productos como digitalizados; pueden "descargarlos" de la red después de efectuar el pago con su tarjeta, disponiendo de ellos de forma inmediata.

El gran atractivo de este esquema para los compradores es la disminución de la cadena de intermediarios (distribuidores y minoristas) presentes en los esquemas tradicionales de comercialización. Al no existir tantos intermediarios, ya no se añaden los servicios y cargos correspondientes que se reflejaban un el aumento del precio final del bien o servicio adquirido por el cliente. Por este hecho, los intermediarios deberán convertirse en suministradores de valor añadido (véase el comercio electrónico tipo C2C) o desaparecer [9, 97].

El gran atractivo para los negocios es la factibilidad de la relación fabricante-cliente final, tanto para productos como servicios, ya que Internet le permite al primero:

- tener el equivalente a una puerta de venta directa de fábrica, aprovechando que la mayoría de las operaciones serán transacciones digitales en régimen de autoservicio [9, 97 y 100]
- aumentar sus ventas al beneficiarse de las consecuencias de la disminución de intermediarios
- explotar la enorme capacidad de este medio para difundir información valiosa a escaso costo y sin necesidad de abrir sucursales [9, 100]

Pero la gran desventaja de este esquema es la espontaneidad de la relación vendedor-cliente: en cada transacción es más probable que los consumidores busquen el mejor trato (menor costo, entrega más rápida, etc.) sin importar con cual vendedor hayan comercializado en ocasiones anteriores. La Red ofrece a los consumidores información valiosa para encontrar el mejor precio de

artículos específicos; y en virtud de que los consumidores usan la Red para inclinar a su favor la balanza del poder de negociación, es difícil que las compañías del canal de B2C generen costos de reemplazo de tecnología. Llamamos "costos de reemplazo de tecnología" al desembolso que el usuario (individuo o persona) debe de invertir en la infraestructura necesaria para poder utilizar un servicio en Internet ("software", sistemas de comunicación, equipo, etc; de naturaleza propietaria). Este costo se debe a la carencia de normas o estándares para usar un bien o servicio. Pero si aparece otro vendedor que puede ofrecer el mismo bien o servicio, que obliga a instalar otra infraestructura diferente a la existente, el cliente tendrá que hacer nuevamente un "gasto en el reemplazo de la tecnología", porque es muy probable que de la primera inversión ya no se pueda recuperar. A este término también se le llama "costo de conmutación".

En el canal B2C, el costo principal es el de crear una imagen de marca que sea considerada la mejor en su categoría. Las compañías deben manejar su imagen en televisión, prensa y otros medios electrónicos. Así como también deben suministrar suficiente información a los analistas de inversiones e industriales, administradores de sociedades de inversión y anunciantes con la finalidad de mantener el negocio financieramente sano. El canal B2C tiene barreras de ingreso muy bajas al empezar, pues los costos de formar una marca son muy elevados y es una sangría para la rentabilidad de este canal mientras la marca se afianza. Además, la rivalidad entre los titulares con varios canales de venta y los nuevos participantes que operan exclusivamente por Internet es muy intensa, y los costos de conmutación son relativamente bajos.

Por último, otro problema que se deberá resolver es que, para crear una buena imagen, se depende en buena medida del desempeño de terceras compañías: como transportistas, fabricantes, suministradores, etc., pues la venta implica una solución integral [4, 135-140].

Negocio a Negocio ("Business to Business", B2B). Este canal permite que las compañías vendan y paguen productos y servicios entre sí. Estructuralmente este canal es más atractivo que el B2C. Las barreras de ingreso son moderadas, los costos de conmutación son altos y la intensidad de la competencia entre titulares y nuevos participantes es modesta [4, 134-135].

El costo más significativo en el que se incurre es el de construir sistemas informáticos que creen la integración perfecta entre el los servicios informáticos que la compañía vendedora y los sistemas de la compañía cliente [4, 136].

Este canal tiene mucho más probabilidades de crear costos elevados por reemplazo de proveedor y tecnología. La razón de esto es que las compañías no consideran que sea rentable evaluar a sus proveedores cada vez que quieren comprar un producto o servicio. Las compañías quieren encontrar al "mejor" proveedor de un producto o servicio específico y luego establecer un proceso eficiente para hacer negocios con dicho proveedor durante todo el tiempo que éste continúe siendo el mejor. Tal proceso necesita sistemas para colocar pedidos, darles seguimiento a través del proceso de suministro de productos, obtener servicio de instalación y mantenimiento y realizar pagos. Una vez que se estructuran estos sistemas, resulta muy caro hacerlos a un lado y volver a empezar con un proveedor diferente [4, 139-140]

Esto ha marcado la gran diferencia entre B2C y el B2B: es más rentable para las compañías de Internet atender a organizaciones que a particulares. Los consumidores usan Internet para recopilar información que les ayude a lograr mejores tratos, presionando así las utilidades de los proveedores. Las compañías son clientes más rentables porque avanzan más despacio que los consumidores. Las compañías prefieren crear un proceso de compras permanente una sola vez que reconsiderar y renegociar cada vez que hacen un nuevo pedido del producto o servicio. Por tanto, las compañías tienden a tardar mucho más en tomar una decisión inicial de compra de un nuevo tipo de producto; enseguida, intentan estandarizar sus propios procesos con base en el producto o servicio del proveedor ganador Incluso cuando aparece una tecnología nueva, se muestran renuentes a cambiar de proveedor [4, 13-15]

Una buena práctica, que permite atender mejor las necesidades de nuestra compañía cliente, es crear interfaces específicas para cada organización. Es decir, el cliente de una gran empresa, como los órganos de la Administración o las instituciones de enseñanza, visita una página protegida y especialmente diseñada para esa entidad. Lo cual significa que las opciones de compra que presenta esa página están diseñadas conforme a las normas internas de adquisición de la institución. Exhibe equipos normalizados y precios que se han negociado de antemano, así como información relativa al pedido, antecedentes, contactos bancarios utilizados. Todo esto, con la finalidad de agilizar la ejecución de los pedidos. Por otra parte, existe una segunda página protegida que contiene información confidencial para los directores de compras u otros jefes de los servicios de aprovisionamiento y logística de la institución cliente [9, 125-126].

Consumidor a Consumidor ("Customer to Customer", C2C). Son aquellos negocios que actúan como agentes intermediarios o puntos de encuentro entre distintos particulares con el fin de ponerlos en contacto para el comercio entre ellos; obteniendo una comisión de las transacciones realizadas y de la publicidad que permiten tener en su sitio de Internet [4, 142-147]

Este esquema permite la reingeniería del ente intermediario, de una u otra forma desplazado por el B2C, al convertirlo en un suministrador de valor añadido mediante la distribución de información de los productos [9, 97].

La tarea clave de los agentes intermediarios es poner en correspondencia las necesidades de cada consumidor-comprador con los bienes y servicios disponibles y ofertados por los otros consumidores-vendedores. Para esta actividad se vuelven críticos los servicios de listas informatizadas que se caracterizarán por [7, 258]:

- Tener bases de datos actualizadas con el estado del producto (en venta, liquidado, etc) y de gran confiabilidad para manejar la complejidad que implica un enorme número de usuarios distintos.
- Contar con la capacidad de anexar imágenes o multimedia a los bienes ofertados.
- Permitir tener toda la información asociada a los bienes (como ubicación, costo de mantenimiento, etc.).

Negocio a Gobierno ("Business to Administration", B2A). Los gobiernos del mundo son una categoría importante de las organizaciones humanas, con necesidades especiales y poderes especiales. Su actividad opera en dos niveles: dentro de las naciones y entre ellas [7, 279]. Todo gobierno es gran comprador de bienes y servicios y, en consecuencia, gran candidato al comercio electrónico [7, 281].

En este esquema prevalecerán las licitaciones electrónicas propuestas por el gobierno. Por esta razón se deberán estandarizar las formas electrónicas ("e-forms") con el fin de crear y usar herramientas informáticas que permitan al sector público ejecutar en forma rápida y ágil la comparación de distintas ofertas económicas en los distintos apartados y garantizar la equidad en la designación de los ganadores.

Además, si se analiza al gobierno como un cliente y proveedor de servicios, con características muy propias, se puede concluir que esta creándose un mercado de la información gubernamental En él se empezarán a hacer propuestas al gobierno, cubrir pedidos, facturas y procedimientos de conciliación, mantener programas y revisiones y muchas otras actividades. Estos procesos ya han empezado a reducir el costo de las compras gubernamentales y se prevé que esta tendencia continúe

Ciudadano a Gobierno (Citizen to Administration, C2A). Por último los gobiernos necesitan comunicarse con sus ciudadanos. Su vida se basa en el empleo de formularios y de información estructurada, y siempre pueden permitirse ser más eficientes; razones por las cuales son excelentes candidatos a beneficiarse del mercado de la información. Los gobiernos pueden usar este enfoque para [7, 279]:

- recibir propuestas del pueblo,
- realizar la integración de los diferentes entes gubernamentales,
- realizar consultas y votaciones electrónicas; y
- manejar directamente el pago de impuestos de los ciudadanos.

Sobre todo esta última actividad se ha conceptualizado para [7, 279-282]:

1. la utilización de formas fiscales electrónicas ("e-forms" fiscales)
2. la realización de transacciones financieras electrónicas, de las cuentas de los individuos a las cuentas del gobierno

Ciber-kioscos o Ciber-tiendas. Los ciber-kioscos son el híbrido del comercio físico y el comercio electrónico. Se caracterizan por [7, 35]:

- No tener ni un solo producto, y están totalmente enfocados al consumidor que desea aprovechar el comercio en línea y no tiene el equipo necesario.
- Tiene equipo de computo más avanzado que el disponible por el consumidor promedio, incluyendo Realidad Virtual, escáner tridimensional para tomar medidas antropomórficas e impresoras de muy alta definición.
- Refinado software de búsqueda, mucho más especializado y con mejores resultados, que los tradicionales.
- Flexible política de devoluciones.

Al igual que el C2C, vienen a ser también una revalorización del intermediario; diferenciándose en que sus servicios no serán para contactar o dar conocimiento, sino proveer infraestructura especializada al usuario final.

2.6 Etapas evolutivas en la implantación del comercio electrónico

Las empresas, grandes y pequeñas, tienden a desarrollar su presencia en la Web en etapas o fases. Una vez que una empresa ha hecho acto de presencia en Internet, entonces querrá usar ese sitio para reforzar el servicio al cliente y producir dividendos. En está fase es cuando el comercio electrónico entrará en juego. Muchos negocios pequeños y medianos están esforzándose con el alto costo de entrada al comercio electrónico. Crear un ambiente completo de ventas en línea puede requerir tiempo considerable, dinero y especialización técnica. Muchos negocios están detenidos en el primero o segundo de los tres niveles que llevan a construir una presencia efectiva en Internet para un comercio electrónico eficaz.

Por ello, el desafío más importante es comprender los costos y beneficios progresivos de trabajar en Internet. La pirámide de aplicaciones Web muestra las diversas etapas de la puesta en operación del comercio electrónico, a partir de cómo se realiza el flujo de información [4, 9].

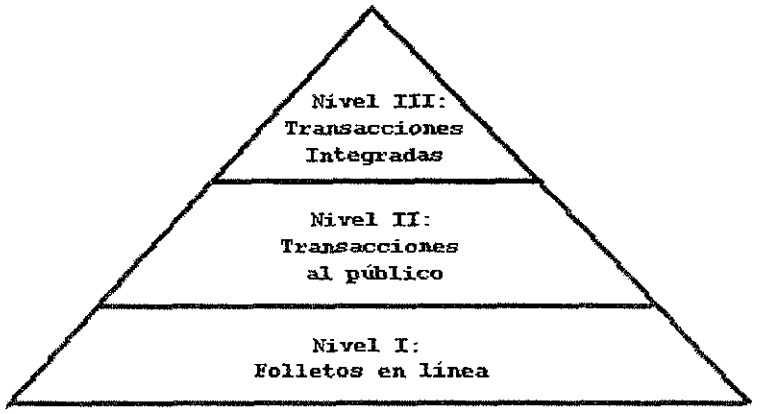


Figura 2-1. Pirámide de la Evolución de las Transacciones Comerciales por Internet

2.6.1 Nivel I: Etapa de folletos en línea.

Colocan en el sitio Web publicaciones sobre los productos, informes anuales y otro tipo de información tradicionalmente impresa. El flujo de información es unidireccional (compañía a clientes), pues siguen utilizando un proceso concebido en papel. Como sólo tiene contenido, únicamente permite las transacciones híbridas o fuera de línea [4, 9-10].

- Ventajas: pueden desarrollar los sitios "Web" fácil y rápidamente a bajo costo.
- Desventajas: esto limita la función de Internet a la promoción y ninguna oportunidad del rédito está envuelta.

2.6.2 Nivel II: Etapa de transacciones al público.

Se utiliza el sitio "Web" como un medio de recepción de formularios de pedidos ("e-forms" propietarios o normalizados). La información de pedidos recopilada por medio de Internet se imprime y emplea como entrada a un proceso inalterado de surtido de pedidos Las compañías en este nivel no integran la información de los pedidos electrónicos directamente a sus procesos internos. El flujo de información es bidireccional (empresa -> cliente -> empresa) pero no es totalmente electrónico, ya que se imprime para seguir un proceso concebido en papel

- Ventajas: Permite las transacciones electrónicas únicamente para la compra-venta de productos No necesita manejar tecnología sofisticada y su catálogo puede manejar un surtido de productos grande. Además permite el flujo de retroalimentación del cliente.
- Desventajas: La construcción del sitio Web (catálogo, herramientas de protección de transacción, etc) incrementa el costo y puede que algunos de los servicios de valor añadido (atención en tiempo real, asistencia técnica, etc.) sólo se puedan manejar por otros canales.

2.6.3 Nivel III: Etapa de aplicaciones integradas.

Hay un gran número de compañías que apenas están instalado aplicaciones de transacciones integradas que explotan todo el poder WWW. Estas aplicaciones usan el Web para intercambiar información con los clientes. Dicha información está estrechamente relacionada con las operaciones internas de la compañías. El flujo de información es bidireccional, constante y electrónico, porque siempre se mantiene dentro de procesos digitalizados.

- Ventajas: pueden manejar un surtido de productos grande y las ventas completas al más bajo costo; todas las transacciones son electrónicas y se permite usar este mismo canal para dar los servicios de valor añadido a todos los clientes.

- Desventajas: La construcción de un sistema de este tipo es la más costosa, y requiere de mayor administración ya que todas las transacciones y servicios de valor añadido requieren de tecnología sofisticada.

Como se observa la mayor parte de las interacciones con los consumidores no serán ventas sino servicios y asistencia técnica [9, 142], a medida que una empresa evolucione a través de estas etapas.

2.7 Componentes de los sistemas de Comercio Electrónico

Un sistema básico de comercio electrónico requiere que el cliente cuente con acceso a Internet, y que el vendedor cuente con el "software" para comercio electrónico (con el cual se crearán los catálogos de ventas y se procesarán las transacciones financieras); así como un servidor de aplicaciones "Web" el cual debe contar con entradas de seguridad para limitar el acceso externo a los sistemas de datos, y "software" especializado que se encargará de "lanzar" los datos de los sistemas de apoyo apropiados en el ambiente del comercio (vea figura anexa).

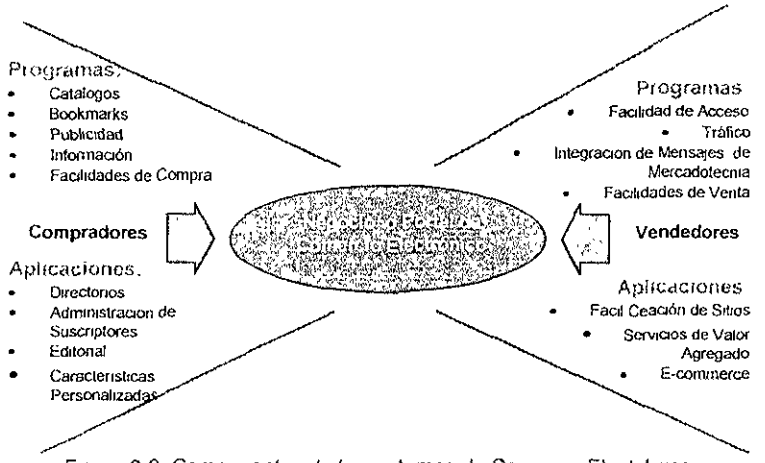


Figura 2-2 Componentes de los sistemas de Comercio Electrónico

2.7.1 Formulario electrónico

Una herramienta simple pero poderosa es el formulario electrónico o "e-form" Ésta permite estandarizar la información de las órdenes de compra y requisiciones de servicios, con la finalidad de automatizar o semiautomatizar la exploración, la negociación, los pedidos, la contratación y la

facturación; y también se pueden reducir las barreras lingüísticas en el comercio internacional [7, 251].

2.7.2 El Servidor de Transacciones

El servidor de transacciones se ocupa de las operaciones de crédito y débito (usando tecnología estándar de seguridad electrónica) en nombre del comerciante y del cliente. Este servidor debe contener una Interfaz Programada para la Aplicación (API, Application Program Interface) que efectúe todos los tipos del pago y funciones: recibir, aprobar, depositar y reintegros.

El servidor de transacciones maneja la autorización necesaria; solicita y guarda la información de la transacción y liquida las transacciones del comerciante, la compañía de tarjetas de crédito, y el cliente. El servidor de transacciones maneja los procesos de pago y comunica la orden de pago generada por el consumidor a la institución financiera elegida por el comerciante. Deben mantenerse archivos de transacciones para facilitar la conciliación e información posterior.

El servidor de transacciones también debe contener un componente para procesar los certificados digitales de una organización que usa el "software" de autoridades certificadoras para permitir la evolución hacia tecnologías de seguridad mejoradas. Múltiples comerciantes pueden operar en un solo servidor de transacciones.

2.7.3 Los Sistemas de Pago.

Los sistemas de pago requieren de componentes localizados en la ubicación del cliente final (casa, computadora personal, etc.), así como en el sitio en el que se ubica el sistema de transacciones del comerciante, y en el lugar donde reside la institución financiera.

Los consumidores deben saber que su información financiera es confidencial; esto se cumple con carteras electrónicas o "software" de tarjeta de crédito en el punto extremo del consumidor. La información del crédito del consumidor se envía a un servidor de transacción que puede aceptar una variedad de pagos electrónicos, así como una tienda física puede aceptar el crédito o información de la tarjeta de débito

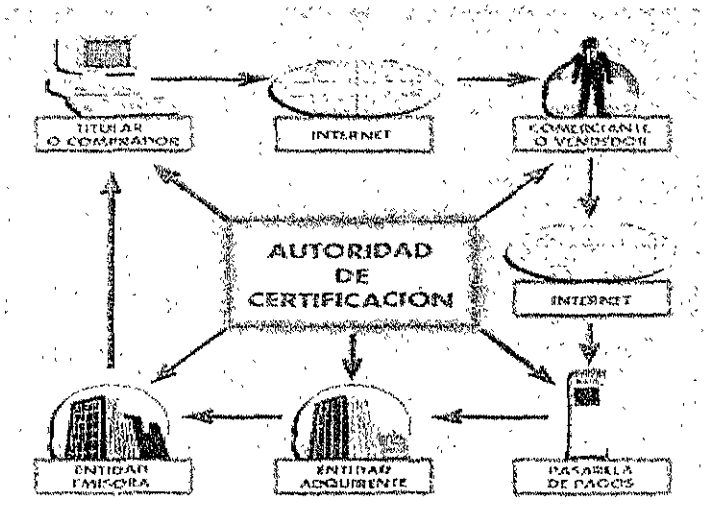


Figura 2-3 La arquitectura distribuida del comercio electrónico

El servidor de transacción también debe manejar el proceso del pago, y se deberá comunicar con la institución financiera para liquidar los bienes adquiridos por el consumidor.

El servidor de transacciones mantiene la información de pago de transacción detallada, mientras permite a las compañías ocuparse de disputas, rebotes de créditos, o ajustes fácilmente.

2.7.4 Construcción de páginas "Web" y su hospedaje

Los Proveedores de Servicio de Internet (ISP's) están empezando a lanzar el hospedaje de tiendas virtuales. Estos servicios posicionan al ISP dentro de la cadena productiva al proporcionar capacidades para el comercio electrónico de sus clientes (tiendas virtuales), además de manejar la gestión de redes y aspectos del servidor de red. Esto les permite a los clientes del ISP concentrarse en su negocio y extender la relación con su ISP. La habilidad de un ISP de ofrecer un ambiente propicio para el comercio electrónico será importante para diferenciar los ISP's de alto y bajo valor agregado, así como aquellos que únicamente proporcionen acceso.

Los proveedores de servicio deben ofrecer una solución de negocios para quien no tenga el presupuesto o la especialización técnica para progresar por ellos mismos. El servidor de transacciones es un aspecto del sistema electrónico que permite a los creadores de directorios electrónicos volverse proveedores de soluciones para comercio electrónico, mientras ofrezcan un servicio completo para transacciones electrónicas y tecnología de seguridad. Al mismo tiempo, los proveedores de servicios pueden incluir en sus servidores el "software" para la creación de sitios "Web"; de forma tal que estas herramientas usen plantillas y métodos simples ("hacer clic" o "pulsar y arrastrar"), así como también tengan la capacidad de completar las ventas manejando un conjunto grande de precios y artículos cambiantes.

Un ISP que construya un servidor de transacciones para soportar múltiples sitios comerciales, necesita poner a disposición de sus clientes (tiendas virtuales), herramientas de construcción de sitios "Web" que les permitan crear páginas electrónicas; y en algunas de ellas, deberá incorporarse una rutina o "botón de compra" creado por las herramientas del servidor de transacción.

Una vez que la página en Internet ha sido completada, el sitio puede publicarse en cualquier servidor que el cliente comercial decida y el ISP permita. El proveedor del servicio de Internet deberá estar listo para proporcionar las funciones de transacción en línea al vendedor.

2.7.5 Modelos de hospedaje para los diferentes tipos de Tiendas Virtuales.

Es probable que los ISP's configuren sus ofertas en cualquier combinación de los modelos siguientes para que sus clientes se organicen en una plataforma tecnológica:

- *Hospedaje Simple*. El cliente es dueño de un sitio Web almacenado en un servidor de Internet compartido por muchos usuarios, el cual tiene un único URL. El cliente no realiza ninguna transacción en línea, pero tiene capacidad para correo electrónico y distribuir información y publicidad.
- *Hospedaje con Capacidad de Almacenamiento Adicional*: El cliente es dueño de una sola tienda en un solo servidor mercantil; es decir, toda su información se hospeda en un solo servidor. La tienda virtual posee un único URL, un banco de datos, y un proceso para registrar los cobros.
- *Centro comercial*. Se ofrece al cliente (o el cliente lo contrata para) tener múltiples tiendas en un ambiente tal que se asemeja a un centro comercial en el mismo URL, presenta la ventaja adicional de poseer un solo banco de datos, con registros compartidos, un solo carrito, caja, etc.,

- *Multihospedaje*: Múltiples tiendas virtuales residen en un servidor, pero cada una de ellas tiene su propio URL, banco de datos, sistema de compra y formato de orden, etc.
- *Servidor de transacciones y contenido dentro del mismo sitio*: No hay una base de datos de transacciones, el sitio web esta hospedado en varios servidores ("multihome") y las transacciones son llevadas a cabo por un servidor mercantil. Estos sitios Web de venta se crean con un botón de compra que envía por separado la información del producto y de la transacción (pero dentro de un mismo ambiente) al servidor.

Las siguientes figuras ilustran a los varios modelos de hospedar una tienda virtual.

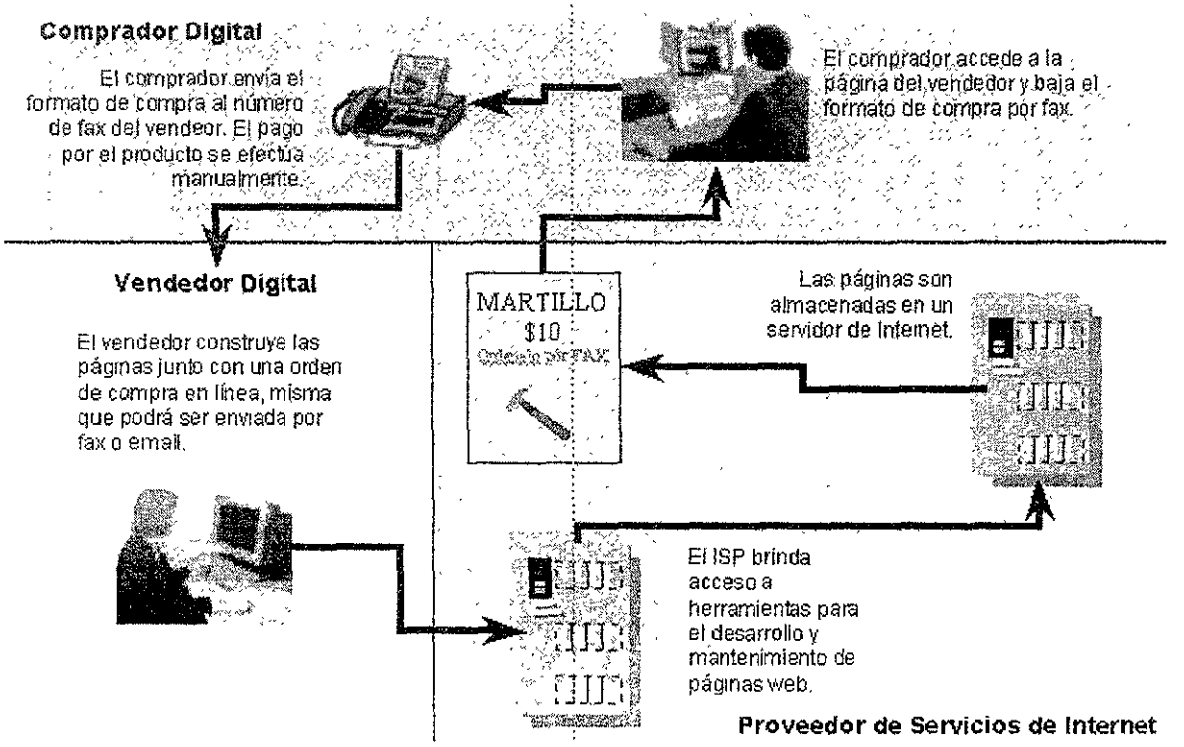


Figura 2-4 Modelo Simple de Hospedaje de Tienda Virtual

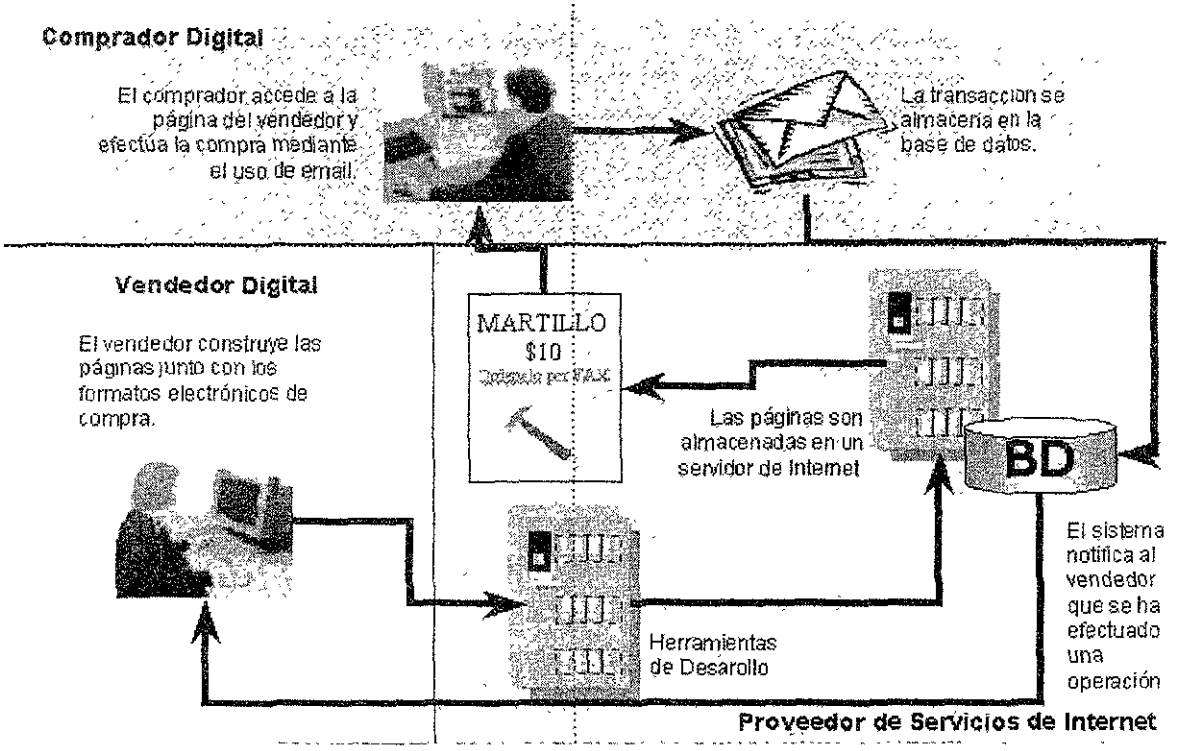


Figura 2-5. Modelo Híbrido de Hospedaje de Tienda Virtual

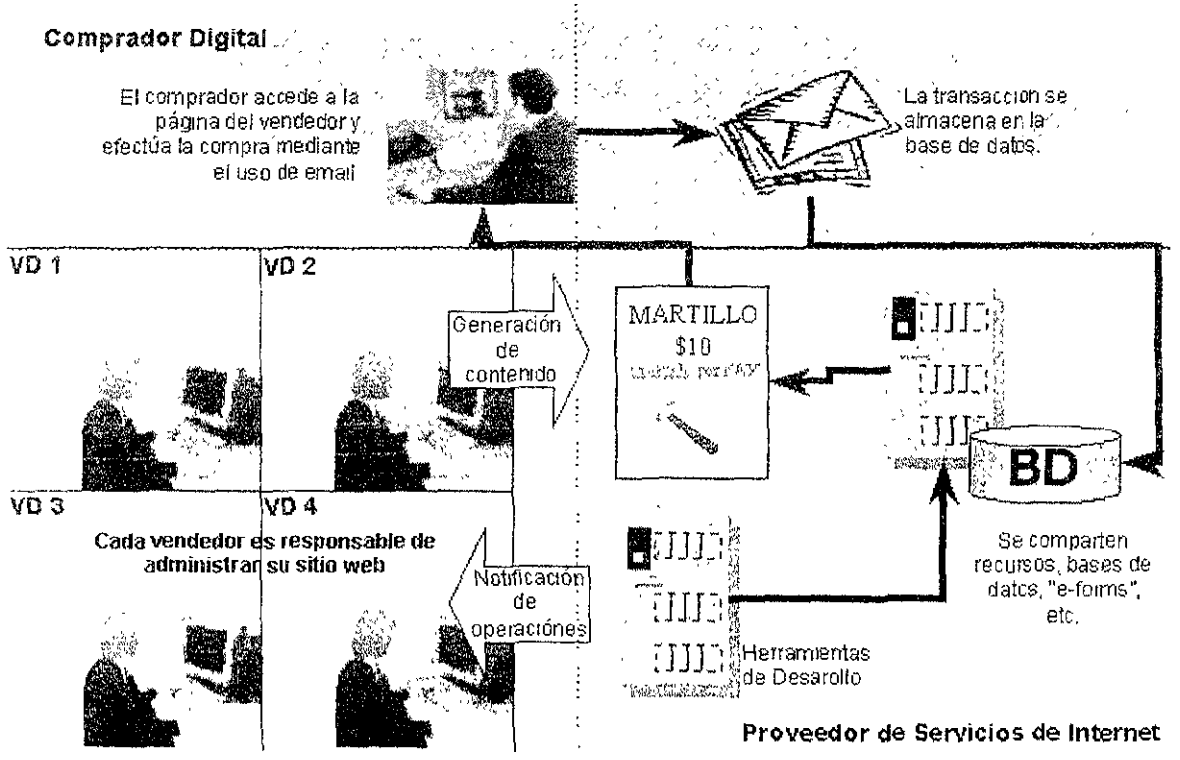


Figura 2-6 Modelo de Hospedaje para Nivel II de Comercio Electrónico

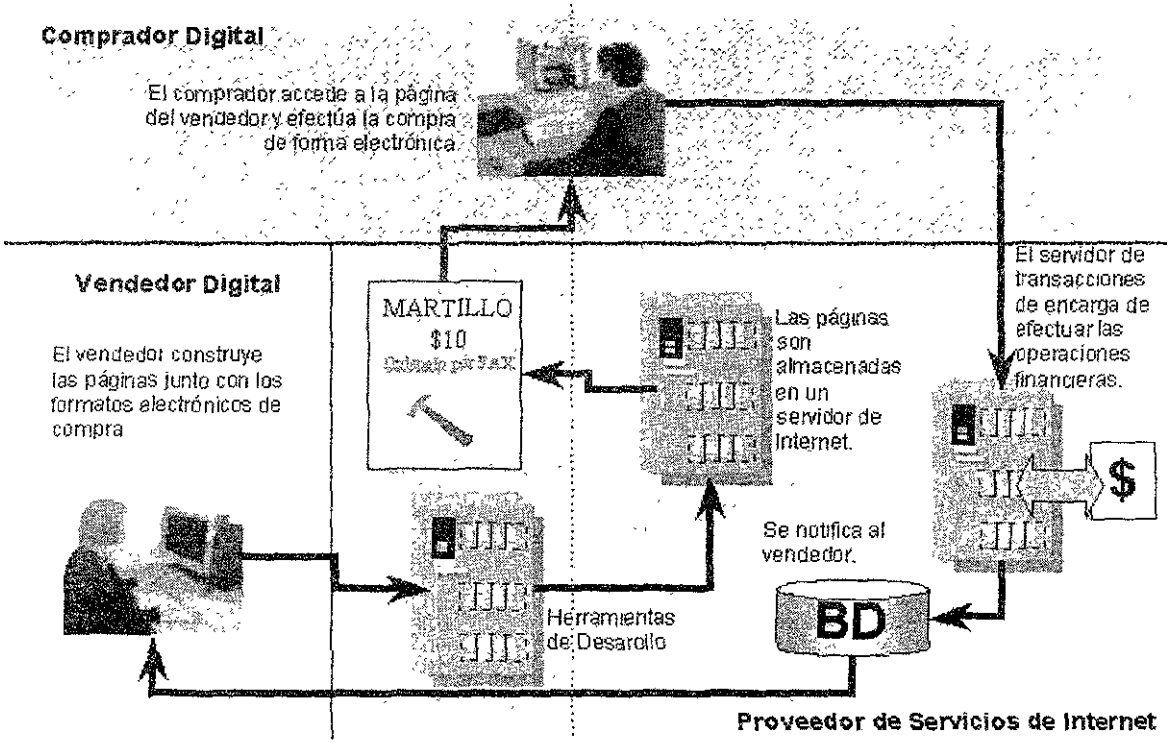


Figura 2-7 Modelo Avanzado de Hospedaje para Comercio Electrónico

2.8 Necesidad de la seguridad en el comercio electrónico

El desarrollo de la tecnología ha llegado a afectar tan profundamente el mundo y se a integrado de tal modo en la actividad humana, que ha dejado de ser una finalidad aislada. De esta forma, cuando los avances tecnológicos son asimilados socialmente, se generan nuevas necesidades y problemas [7, 21]

El mercado de la información hace posible que todo el mundo compre, venda e intercambie bienes y servicios sin tener que registrarse ni ser controlado por una autoridad central omnipresente y omnipotente [7, 56].

El problema central de la seguridad informática en el mercado de la información reside en

1. la gran conectividad de Internet, y
2 la digitalización de la información y el dinero

La gran abundancia de conexiones posibles en la infraestructura de Internet permite a unos acceder electrónicamente a la información de otros (negocio, consumidor o gobierno) con intenciones sospechosas y posibles consecuencias desastrosas [7, 137]

Internet es un medio en el cual se expande rápidamente cualquier error o atentado, y con severas repercusiones en el comercio electrónico (falla en la actualización de precios, cambio no autorizado en los mismos, cambio del destinatario en los pedidos, obtener los numeros de tarjetas de crédito en forma ilegal para realizar delitos financieros, etc) [9, 127]

Con el uso de los procesos digitales, es enorme el crecimiento del volumen de información que los gobiernos, los competidores, los delincuentes o gente simplemente entrometida es capaz de interceptar. Es tan grande el volumen y el alcance de la información en formato electrónico que su posible violación por individuos no autorizados, debe ser tomada en cuenta por individuos, negocios y el gobierno [7, 290].

La manera como se efectúan los pagos en las transacciones electrónicas y en general como se maneja el dinero en el mercado de la información; permite la realización de delitos en magnitud (cifras), alcance (sin fronteras físicas) y cantidad (muchos y muy diversos usuarios) irrealizables apenas hace unos pocos años [7, 143].

2.8.1 ¿Qué se debe proteger en el comercio electrónico?

La información. Al fin y al cabo todo lo que se transmite son bits de información, y no se necesita ser un gran especialista en informática, computación, electrónica o telecomunicaciones para deducirlo. Pero esta simple respuesta provoca más preguntas. ¿se debe proteger el nombre del negocio que vende y aparece en todas sus páginas electrónicas? ¿Es conveniente resguardar todos los manuales de equipos y programas que estén en formato html? ¿Por qué se debe asegurar cada enlace de comunicación lógico y físico entre un servidor de transacciones y toda computadora que lo accese a él?; y ¿eso es o no suficiente? ¿Qué es más importante salvaguardar: los bits de una animación o los bits que representan un número decimal?

Para responder a estas preguntas, pensemos en todos los productos (bienes y servicios) que nos rodean, y clasifiquémoslos en la forma más simple: o son bits (información) o son átomos (físicos). Llamemos productos finales a los productos consumidos por el público y productos intermedios a aquellos que conducen a nuevos bienes y servicios [7, 305].

Dado que son consumidos directamente por los compradores, todos los productos finales (sean bits o átomos) son económicamente similares: su valor se basa en los deseos humanos que satisfacen y en su escasez, la tan conocida ley de la oferta y la demanda [7, 305-306]

Cada día más y más productos intermedios de bits se agregan a la economía, extendiendo así su participación en el mercado. Estos productos informáticos son valiosos pues conduce a millones de bienes y servicios (tanto de información como físicos) e incluyen todo el trabajo de oficina Pero la comercialización de este tipo de productos se dificulta enormemente en comparación de los productos intermedios de átomos ya que los segundos siempre se les encuentra en una forma estándar (como la harina, el hierro, etc), valuable independientemente de la organización a la que pertenezcan. Por el contrario, los productos intermedios son información más personalizada, dependiente de la organización e infraestructura de la empresa y de las intrincadas combinaciones de procedimientos humanos y mecánicos, carecen de utilidad excepto para sus propietarios y el pequeño conjunto de personas o instituciones estrechamente ligados a ellos, o sus competidores inmediatos Por lo cual su valor está determinado en gran medida por el valor de los bienes y servicios a los que conducen (los economistas lo llaman demanda derivada) [7, 300-301 y 305-306].

Todo lo anterior permite sustentar que el valor de la información (bits) puede determinarse con 2 parámetros:

Por su capacidad de ser utilizados una y otra vez [16, 95]
Por su capacidad de satisfacer los deseos humanos [7, 306]

Una pequeña porción esta formada por bienes finales, cuyo valor deriva de la oferta y la demanda Mientras que, con mucha frecuencia, la porción mayor es la de los bienes intermedios, cuyo valor deriva sustancialmente del valor de los bienes y servicios a los que conducen

Este pequeño análisis nos da una mejor respuesta a la pregunta de esta sección: lo que se debe proteger en el comercio electrónico principalmente son los productos de información intermedia por su importancia y su volumen, y en un grado menor, los productos finales de información. Esto, porque son los bits del primer tipo los que en manos incorrectas y con el equipo necesario, pueden causar las terribles pesadillas de todo administrador.

Un ejemplo tan simple es el número de la tarjeta de crédito (un bien de información intermedio enormemente requerido en toda transacción de cualquier tipo de comercio electrónico) cuyo producto al cual conduce es el dinero. Y si alguien puede manejar el dinero de otros con toda libertad, varias veces, en grandes cantidades y sin represión legal, el comercio electrónico tiene un problema bastante complicado.

Y un ejemplo un poco más especializado donde no intervenga solo el dinero es aquel escenario en donde una organización pueda acceder a la información de otra competidora por medio de los servicios electrónicos que la segunda contrata con un tercero (factible en el B2B). Malograr campañas publicitarias, copiar proyectos (con el consecuente ahorro de tiempo y dinero); alterar estados financieros, nóminas y depósitos; son sólo algunas muestras de lo que sucede al no cubrir las necesidades de seguridad en el comercio electrónico.

De forma general, los expertos establecen cuatro requisitos a cubrir para que una transacción por Internet, y la información que debe ser protegida, sea considerada segura:

1. *Identificar al comprador y vendedor; y en los casos necesarios, de terceros participantes.*
2. *Asegurar la integridad de la información que se intercambia.*
3. *Asegurar la confidencialidad de dicha información y así evitar que otros hagan mal uso de ella.*
4. *Garantizar el no rechazo por ninguno de los participantes.*

Los 4 tipos de comercio electrónico (B2C, B2B, C2C y B2A) comparten estás necesidades de seguridad; y las cuales pueden ser satisfechas mediante la criptografía, un conjunto de protocolos y algoritmos matemáticos que permiten cifrar y descifrar mensajes. Pero son los servicios de valor agregado y el alcance del flujo de información generado por estos servicios los que generan una amplia gama de escalas en dichas necesidades de seguridad. Por ello se debe tratar de abordar cada necesidad de seguridad con el "software" y, en algunos casos, el "hardware" adecuados [7, 137] a la gama de requerimientos.

2.8.2 Herramientas existentes en el mercado

Del conjunto de técnicas existentes en el mercado, cabe destacar dos tipos de sistemas: SSL y SET. Mientras que SSL ofrece un nivel aceptable de seguridad en las compras por Internet, pues garantiza que la información que se transmite viaja de forma cifrada, SET ofrece un nivel de seguridad óptimo ya que, además, permite la identificación unívoca de las partes (comprador, vendedor, etcétera) involucradas en la transacción.

Independientemente del sistema de seguridad implementado, tendrá la certeza de que un comercio es seguro cuando se den las siguientes condiciones.

1. Hay un candado cerrado (o una llave) en la parte inferior del navegador
2. La dirección de la página comienza por https:

2.8.2.1 SSL

En la actualidad, la mayoría de los comercios que venden a través de Internet cuentan con un sistema que utiliza el protocolo SSL Para que resulte operativo, el consumidor sólo precisa disponer de un navegador (Internet Explorer, Netscape Communicator, etc) En el comercio

deberá instalarse un certificado en el servidor donde se tenga alojado el sitio "Web", certificado que podrá obtener a través de su Entidad Financiera o de una Autoridad de Certificación acreditada.

2.8.2.2 SET

Por otra parte, el protocolo SET es un conjunto de normas o especificaciones de seguridad desarrollado por VISA y MasterCard junto a otras empresas (IBM, Microsoft, Netscape, SAIC, GTE, RSA, Verisign, Terisa Systems). Esta especificación permite realizar compras por Internet, con tarjeta, bajo máximas garantías de seguridad:

- Asegura la confidencialidad e integridad de la información transmitida.
- Permite la autenticación de los compradores, vendedores y Entidades Financieras involucradas en la transacción.
- Garantiza el no rechazo de las operaciones realizadas.

Su empleo requiere que cada uno de los participantes en la transacción disponga de un certificado SET, así como de un "software" específico. Estos elementos se podrán conseguir a través de una Entidad Financiera:

- El comprador dispondrá de un aplicativo, denominado "Electronic Wallet" o "Cartera Electrónica", en el cual dará de alta las tarjetas con las que desee realizar pagos: cada una de estas tarjetas se asociará en el proceso de alta de un certificado.

- El vendedor dispondrá de un aplicativo, denominado "Merchant Software" o "Programa Gestor", que se instalará en la "Web" del comercio y gestionará las operaciones de compra bajo el protocolo SET.

Sin embargo, existen otros partícipes en las operaciones de compra realizadas con SET.

- Pasarela de Pagos ("Payment Gateway"): es un sistema de comunicaciones que permite procesar y autorizar las transacciones de pago con tarjeta.
- Autoridad de Certificación: tercera parte confiable que, a través de las Entidades Financieras, emite certificados SET.
- Emisor: Entidad Financiera emisora de la tarjeta del comprador
- Adquirente: Entidad Financiera con quien trabaja el comercio, para la solicitud y liquidación de los pagos.

2.8.3 ¿Qué no se debe olvidar?

Es indudable que siempre habrá tentativas de delito en el mercado de la información (Internet es un medio en el cual se refleja y se extiende la naturaleza humana [7, 55]) y que algunos de dichos delitos nunca se detectarán [7, 49].

Las tecnologías que producen una buena seguridad (criptografía y contrainteligencia) también producen buenos ataques (criptoanálisis e inteligencia). Todos los participantes en el comercio electrónico se enzarzarán en una serie de medidas, contramedidas y re-contramedidas para obtener alguna ventaja en el conocimiento del otro y proteger el propio [7, 285].

Con independencia de la dificultad matemática para quebrantarlo, todo esquema criptográfico es vulnerable a otros tipos de ataque En primer lugar, los violadores pueden infiltrarse en nuestro campo bajo la forma de aliados y comprometer las maneras de hacer, compartir y disponer de los códigos al poner todo eso en conocimiento del enemigo. Lo más destructivo es que una persona a la que se ha confiado la empresa criptográfica sea sobornada o atraída al campo enemigo [7, 138].

Los tecnicistas cautivados por las nuevas técnicas matemáticas para cifrar harían bien en recordar que las mismas antiquísimas debilidades humanas que ayudaron a ganar y a perder guerras en todos los tiempos han llegado intactas al moderno mercado de la información [7, 138].

3 Criptografía

Criptografía. Es el arte y la ciencia de mantener la información segura. Es el estudio de las técnicas matemáticas relacionadas con algunos aspectos de la seguridad informática como la confidencialidad, la integridad de los datos, la autenticidad de los entes y la autenticidad de los datos[15,4]. Una persona que trabaja, practica o esta interesada en esta área se le llama ***criptógrafo.***

Por su parte, la ciencia o arte que se ocupa del estudio sistemático de los métodos para desencriptar información encriptada se denomina ***criptoanálisis***, y es practicada por los ***criptoanalistas*** (ambas disciplinas, el criptoanálisis y la criptografía se engloban en una rama de las matemáticas conocida como ***criptología***, cuyos especialistas son los ***criptólogos***).

Sistemas de Encriptado. Es un término general para referirse a un conjunto de primitivas usadas para proveer servicios de seguridad informática. Los requerimientos para los sistemas de encriptado fueron establecidos por Kerckhoff en 1883 y actualmente siguen siendo útiles para el diseño de estos sistemas, dichos requerimientos son[15.14] :

1. El sistema debe ser inquebrantable en la práctica, aunque en teoría no lo sea.
2. La revelación de los detalles del sistema no debe ser un inconveniente para las partes involucradas.
3. La llave o llaves utilizadas deben ser recordadas sin registrarlas en papel (un medio inseguro) y su cambio no debe presentar ningún problema.
4. El criptograma o texto cifrado debe ser transmisible por un medio de telecomunicaciones.
5. El aparato de encriptación (implementación) debe ser portátil y operable por cualquier persona.
6. El sistema debe ser fácil de utilizar, sin requerir el conocimiento de una larga lista de reglas ni gran capacidad mental.

3.1 Objetivos de Criptografía

De todos los objetivos de seguridad informática, los siguientes cuatro forman un soporte básico del cual los otros se pueden derivar, y son:

Confidencialidad o Privacidad	Es un servicio para mantener la información secreta de todos aquellos que no estén autorizados a verla o usarla. Secreto es un sinónimo de confidencial y privado. Existen muchas formas de proveer confidencialidad, desde la protección física hasta la protección por algoritmos matemáticos los cuales convierten los datos en información ininteligible.
Integridad de los datos	Es un servicio enfocado a la no alteración de datos por personas no autorizadas. Para asegurar la integridad de los datos, uno debe tener la habilidad para detectar la manipulación de los mismos por entes no autorizados. La manipulación de datos incluye insertar

	información, borrar la existente y/o sustituirla.
Autenticidad	Es un servicio relacionado a la identificación. Esta función se aplica a todos los entes y a la propia información. Dos entes que sostienen una comunicación deben poder identificarse el uno al otro. La información transportada por un canal debe poder ser autentificada por el origen, fecha del origen, contenido de los datos, tiempo de envío, etc. Por estas razones, este objetivo criptográfico es dividido en 2 grandes clases: autenticidad del ente y autenticidad de los datos. La autenticidad del dato por origen provee implícitamente la integridad de los datos (si el mensaje es modificado, significa que la fuente ha cambiado).
No repudio	Es un servicio el cual previene que un ente niegue haber realizado transferencias o acciones previas. Este servicio es necesario cuando se presenta una disputa en la cual un ente niegue ciertas acciones realizadas. Normalmente se requiere un procedimiento en el cual se involucre a una tercera parte confiable.

Tabla 3-1 Objetivos Criptográficos [13,4]

3.1.1 Mecanismos de seguridad

Para proporcionar los servicios de seguridad citados, es necesario incorporar en los niveles adecuados del modelo de referencia OSI los siguientes mecanismos de seguridad[19,578]:

1. cifrado: el cifrado puede hacerse mediante el uso de criptosistemas simétricos o asimétricos y puede aplicarse extremo a extremo o a cada enlace del sistema de comunicaciones. El mecanismo de cifrado soporta el servicio de confidencialidad de los datos y puede complementar a otros mecanismos para conseguir diversos servicios de seguridad.

2. firmado digital. la firma digital se puede definir como un conjunto de datos que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello, se cifra la unidad de datos junto con alguna componente secreta del firmante, y se obtiene un valor de control ligado al resultado cifrado. El mecanismo de cifrado digital soporta los servicios de integridad de los datos, autentificación del emisor y no repudio con prueba de origen. Para que se pueda proporcionar el servicio de no repudio con prueba de entrega, hay que forzar al receptor para que envíe un acuse de recibo firmado digitalmente.

3 control de acceso. se usa para verificar la capacidad de un ente para acceder a un recurso dado. El control de acceso se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación.

4 integridad de datos. hay que distinguir entre la integridad de una unidad de datos individual y la integridad de una secuencia de unidades de datos. Para lograr integridad de una unidad de datos, el emisor añade datos suplementarios a la unidad de datos. Estos datos suplementarios se obtienen en función de la unidad de datos y, generalmente, se cifran. El receptor genera los mismos datos suplementarios a partir de la unidad original y los compara con los recibidos. Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, algún mecanismo de ordenación, tal como el uso de números de secuencia, un sello temporal o un encadenamiento criptográfico entre las unidades.

5. intercambio de autentificación, que tiene dos grados:
   - autentificación simple: el emisor envía su identificador y una contraseña al receptor, el cual los comprueba.
   - autentificación fuerte: utiliza propiedades de los criptosistemas de clave pública. Un usuario se autentifica mediante su identificador y su clave privada. Su interlocutor debe verificar que aquel, efectivamente, posee la clave privada, para lo cual debe obtener, de algún modo, la clave pública del primero. Para ello deberá obtener su certificado. Un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el periodo de tiempo determinado, que asocia una clave pública a un usuario.

3.2 Comunicaciones seguras sobre redes inseguras

El crecimiento exponencial de los usuarios y organizaciones conectadas a Internet ha originado el tránsito a través de ella de informaciones de todo tipo, desde noticias y correos electrónicos, hasta complejas transacciones que requieren medidas específicas de seguridad que garanticen la confidencialidad, la integridad y constaten el origen de los datos.

En una comunicación entre dos máquinas, se supone la existencia de un emisor y un receptor, los cuales quieren intercambiar mensajes. El posible enemigo que quiere interferir de algún modo en la comunicación se denomina intruso. Este intruso puede ser pasivo, si sólo escucha la comunicación, o activo si trata de alterar los mensajes.

Es aquí donde aparece la criptografía con objeto de proporcionar comunicaciones seguras sobre canales inseguros. Los mensajes sin transformar de ninguna manera se denominan texto en claro. El proceso mediante el cual la información contenida en el mensaje es ocultada se denomina encriptado. Un mensaje encriptado también se denomina, texto cifrado. El proceso mediante el cual se revierte el proceso de ocultación, obteniéndose el texto en claro a partir del texto cifrado se denomina desencriptado.

La criptografía trata de permitir que dos entidades, ya sean usuarios o aplicaciones, puedan enviarse mensajes por un canal que puede ser intervenido por una tercera entidad, de modo que sólo los destinatarios autorizados puedan leer los mensajes.

Pero la criptografía no es en sí seguridad; simplemente es la herramienta utilizada por mecanismos más complejos para proporcionar no sólo confidencialidad, sino también otros servicios de seguridad, ya que, en el contexto de Internet, la confidencialidad es, a menudo, un factor secundario Generalmente estaremos más interesados en el mantenimiento de la integridad de los mensajes y en los mecanismos de autentificación que, implícitamente, proporciona la criptografía. En efecto, un mensaje encriptado sólo puede ser desencriptado si la clave que vamos a utilizar para ello pertenece a quien ha ocultado previamente el mensaje. La criptografía no es una panacea, solo un instrumento.

El texto en claro se representa como **M** (por "message") o también por **P** (de "plaintext"). **M** es simplemente un dato binario. El texto cifrado se designa por **C** (de "ciphertext"). No existe relación directa entre los tamaños de ambos mensajes. Unas veces su tamaño coincide. Otras, el del texto cifrado es mayor que el del texto en claro. Puede ocurrir, incluso, que texto cifrado sea de menor tamaño. Esto sucede cuando, además de las técnicas de cifrado, se emplean técnicas de compresión.

La función de encriptado, $\mathbf{E}_k$, opera sobre M para producir **C**. En notación matemática [18,3]:

$$E_k (M) = C$$

Inversamente, la función de desencriptado, D_k, se aplica a **C** para producir **M**:

$$D_k (C) = M$$

En todo caso, debe cumplirse la siguiente igualdad:

$$D_k (E_k (M)) = M$$

Un algoritmo criptográfico es una función matemática utilizada para el cifrado y descifrado de mensajes. Generalmente, hay dos funciones relacionadas: una para el cifrado y otra para el descifrado.

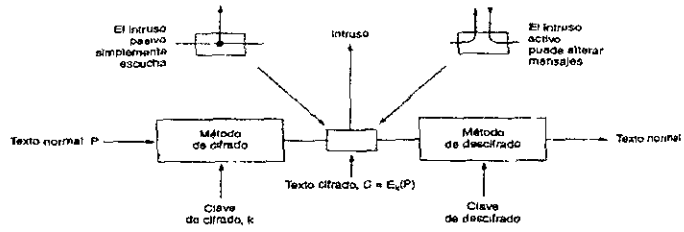


Figura 3-1 El modelo de cifrado

3.3 Tipos de ataques

Una comunicación, protegida o no mediante sistemas criptográficos, está sujeta a una gran variedad de ataques, de los cuales son más habituales los siguientes[41]:

A) ataque sólo al criptograma: es el más desfavorable para el intruso o criptoanalista. En este caso, sólo tiene acceso al texto cifrado. El trabajo del intruso consiste en recuperar el texto en claro de tantos mensajes como sea posible. En tales condiciones, y aunque conociera el algoritmo de cifrado, sólo puede intentar vulnerar dicho algoritmo, realizar un análisis estadístico de los criptogramas o probar todas las claves posibles del algoritmo. Este último caso, por motivos obvios se conoce como búsqueda exhaustiva o también como ataque basado en fuerza bruta.

B) ataque mediante texto en claro conocido: en este ataque se tienen pares de texto en claro y su equivalente encriptado, o ha adivinado, de algún modo, el contenido del mensaje (muchos mensajes encriptados, correspondientes a protocolos normalizados, reproducen la misma estructura o poseen las mismas palabras en los mismos sitios del mensaje). Estas parejas pueden ser usadas para llevar a cabo el criptoanálisis y averiguar la clave, lo cual será útil si se usa la misma clave para posteriores comunicaciones.

C) ataque mediante texto en claro escogido: el intruso es capaz de conseguir que un texto elegido por él sea cifrado con la clave desconocida. Por tanto hay que diseñar el sistema criptográfico de modo que nunca un intruso pueda introducir mensajes propios.

D) ataque adaptable mediante texto en claro escogido: el intruso no sólo puede elegir el texto que quiere cifrar, sino que puede tomar decisiones sobre el texto que será encriptado basándose en resultados anteriores.

E) ataque mediante criptogramas escogidos: el atacante puede obtener el descifrado de diversos mensajes encriptados escogidos por él.

Por otra parte, en el marco de una comunicación entre dos entidades, se puede hablar de los siguientes ataques[15,41]:

a) escucha pasiva ("passive eavesdropping"): el intruso simplemente escucha el tráfico que circula por el canal.

b) tercero interpuesto ("man-in-the-middle"): el intruso, de alguna forma, se coloca entre los dos interlocutores y hace creer a cada uno de ellos que es su interlocutor.

c) retransmisión ciega ("replay"): el intruso intercepta un mensaje legítimo, lo almacena (sin eliminarlo) y lo reenvía un tiempo después.

d) cortado-y-pegado ("cut-and-paste"): dados dos mensajes cifrados con la misma clave, a veces es posible combinar partes de los dos para producir uno nuevo. El intruso no sabe lo que dice este nuevo mensaje, pero puede utilizarlo para confundir a los interlocutores legítimos e inducir a alguno de ellos a hacer algo beneficioso para él.

e) puesta a cero del reloj ("time-resetting"): en protocolos que utilizan de alguna forma la hora actual, el intruso puede tratar de confundir acerca de cuál es la verdadera hora.

Y en cuanto a los atacantes, la siguiente tabla resume los grupos de personas más comúnmente propensos a cometer ataques a sistemas informáticos y las razones por las que lo hacen.

ADVERSARIO	META
Estudiante	Divertirse husmeando el correo de la gente
Hacker	Probar el sistema de seguridad de alguien; robar datos
Representante de ventas	Hacerse pasar por alguien más
Hombre de negocios	Descubrir el plan estratégico de mercadeo de un competidor
Ex empleado	Vengar su despido
Contador	Estafar dinero de una compañía
Corredor de bolsa	Negar une promesa hecha a un cliente por correo electrónico
Timador	Robar números de tarjeta de crédito
Espía	Conocer la fuerza militar de un enemigo
Terrorista	Robar secretos de guerra bacteriológica

Tabla 3-2 Algunas personas que causan problemas de seguridad, y por qué [19,578]

3.4 Historia

Los usos más primitivos de la criptografía se encuentran documentados desde la época de Julio César (nos referimos al cifrado de César, aunque hay constancia también de su uso por persas y espartanos). Estos mecanismos de cifrado se basaban en técnicas de transposición de caracteres y fundamentan su eficacia en el secreto del algoritmo empleado para el cifrado. Algoritmos de este tipo son sólo de interés histórico.

Los algoritmos modernos usan una clave para controlar el cifrado y descifrado de los mensajes. Generalmente, el algoritmo de cifrado es públicamente conocido y sometido a escrutinio por parte de expertos y usuarios. Se acepta, por tanto, la denominada hipótesis de Kerckhoffs, que establece

que la seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave y no en el del mecanismo de cifrado.

3.4.1 Criptografía de clave simétrica

Las técnicas de clave única, secreta o simétrica tienen fundamentos de complejidad diversa, pero todas usan una misma clave ***k*** que es conocida por el remitente de los mensajes y por el receptor, y mediante la cual se encripta y desencripta el mensaje que se quiere proteger[41].

Los cifradores simétricos pueden dividirse en dos grupos:

I. cifradores de flujo, los cuales cifran un único bit del texto en claro cada vez.
II. cifradores de bloque, que toman un grupo de bits y lo cifran como si se tratase de una unidad.

Las ventajas de la criptografía de clave simétrica es la existencia de algoritmos muy rápidos y eficientes, especialmente si se implementan en hardware. Si ***k*** es lo bastante larga (típicamente se usan valores de 56 a 128 bits), resulta casi imposible romperlas usando la fuerza bruta.

Dado que en un sistema de clave simétrica el principal inconveniente radica en que todas las partes conozcan ***k***, la clave tiene que ser distribuida mediante una transacción separada, lo cual hace vulnerable el sistema.

3.4.2 Criptografía de clave asimétrica

La solución al problema de la distribución de claves apareció en 1976 cuando Whitfield Diffie y Martin Hellman demostraron la posibilidad de construir sistemas criptográficos que no precisaban la transferencia de una clave secreta entre emisor y receptor, evitando así los problemas derivados de la búsqueda de canales seguros para la transferencia. Se trata de la "criptografía de clave asimétrica o pública".

Se considera un esquema de encriptación como asimétrico, cuando cada conjunto o pareja de transformaciones de encriptado y desencriptado poseen un par de llaves (***e*** y ***d***) que únicamente sirve para una sola operación. En dicho esquema, una llave ***e*** es hecha pública, mientras la segunda se mantiene en secreto ***d***. Para que el esquema sea seguro, debe ser computacionalmente in factible obtener ***d*** a partir de ***e***. [15, 25]

3.4.3 Dos principios criptográficos fundamentales

Aunque estudiaremos muchos sistemas criptográficos diferentes en las siguientes páginas, hay dos principios que los sostienen a todos y que es importante entender [19, 585]:

1. Todos los mensajes deben contener redundancia para evitar que los intrusos activos engañen al receptor y lo hagan actuar ante un mensaje falso. Sin embargo, esta misma redundancia simplifica mucho la violación del sistema por parte de los intrusos pasivos, por lo que se recomienda usar una cadena aleatoria de palabras como mensaje de redundancia.

2. El segundo principio criptográfico es que deben tomarse algunas medidas para evitar que los intrusos activos reproduzcan mensajes viejos. Una de tales medidas es la inclusion en cada mensaje de una marca de tiempo válida durante un determinado tiempo

3.5 Criptografía de clave simétrica o única

3.5.1 DES

En enero de 1977, el gobierno de Estados Unidos adoptó un cifrador de bloque desarrollado por IBM como su estándar oficial para información no clasificada. Este cifrado, el DES (Data Encryption Standard, estándar de cifrado de datos), se adoptó ampliamente en la industria para usarse con productos de seguridad. Ya no es seguro en su forma original, pero aún es útil en una forma modificada.

En la figura 3-2 se muestra un esbozo del DES. El texto normal se cifra en bloques de 64 bits, produciendo 64 bits de texto cifrado. El algoritmo, que se parametriza mediante una clave de 56 bits, tiene 19 etapas diferentes. La primera etapa es una transposición, independiente de la clave, del texto normal de 64 bits. La última etapa es el inverso exacto de esta transposición. La etapa previa a la última intercambia los 32 bits de la izquierda y los 32 bits de la derecha. Las 16 etapas restantes son funcionalmente idénticas, pero se parametrizan mediante diferentes funciones de la clave. El algoritmo se ha diseñado para permitir que el descifrado se haga con la misma clave que el cifrado. Los pasos simplemente se ejecutan en el orden inverso.

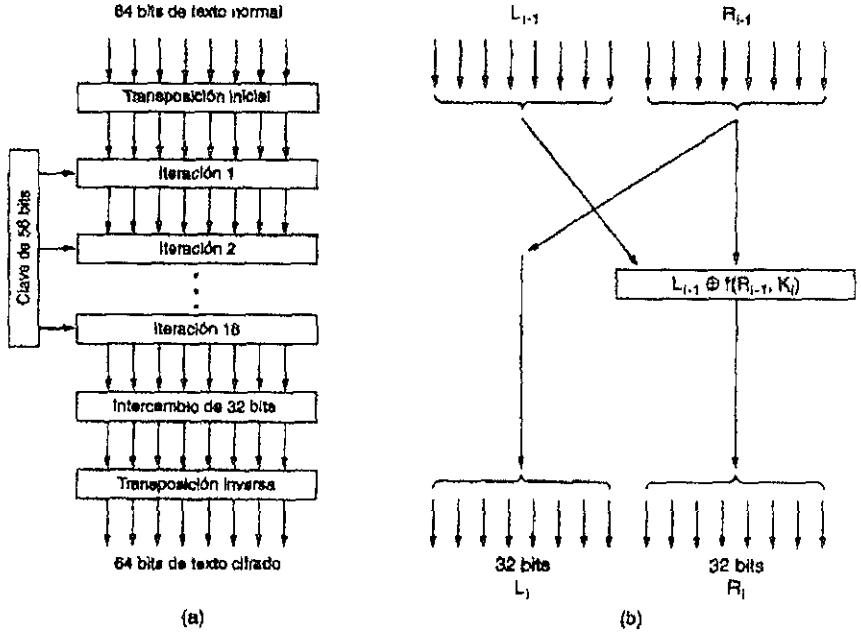


Figura 3-2 DES (a) Esbozo general (b) Detalle de una iteración

La operación de una de estas etapas intermedias se ilustra en la figura 3-2(b). Cada etapa toma dos entradas de 32 bits y produce dos salidas de 32 bits. La salida de la izquierda simplemente es una copia de la entrada de la derecha La salida de la derecha es el OR EXCLUSIVO a nivel de bit de la entrada izquierda y una función de la entrada derecha y la clave de esta etapa, K_i Toda la complejidad reside en esta función.

3.5.1.1 Encadenamiento DES y Modos de Operación

A pesar de toda esta complejidad, el DES básicamente es un cifrado por sustitución monoalfabética que usa un carácter de 64 bits. Cada vez que entra el mismo bloque de texto normal de 64 bits por el frente, sale el mismo bloque de texto cifrado de 64 bits por atrás. Un criptoanalista puede explotar esta propiedad como ayuda para violar el DES.

Para ver la manera en que esta propiedad de cifrado por sustitución monoalfabética puede usarse para subvertir el DES, consideremos el cifrado de un mensaje grande de la manera obvia: dividiéndolo en bloques consecutivos de 8 bytes (64 bits) y cifrándolos uno tras otro con la misma clave. El último bloque se rellena a 64 bits, de ser necesario. Esta técnica se conoce como modo de libro de código electrónico.

En la figura 3-3 tenemos el comienzo de un archivo de computadora que lista los bonos anuales que ha decidido otorgar una compañía a sus empleados. Este archivo consiste en registros consecutivos de 32 bytes, uno por empleado, en el formato que se muestra: 16 bytes para el nombre, 8 bytes para el puesto y 8 bytes para el bono. Cada uno de los 16 bloques de 8 bytes (numerados del 0 al 15) se cifra con el DES.

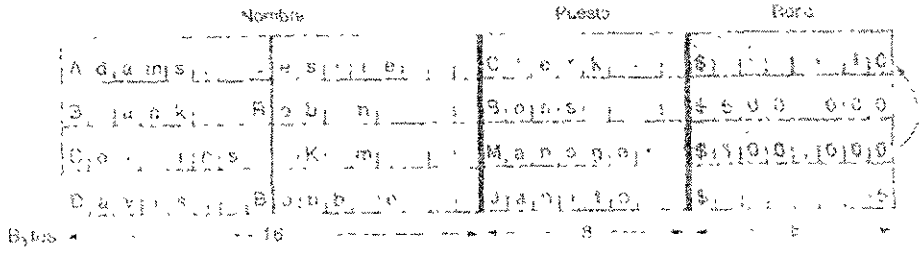


Figura 3-3. El texto normal de un archivo cifrado como 16 bloques DES [19,590].

Como puede verse, dado que el cifrado de la información se efectúa por bloques, un empleado malicioso puede, en un momento dado, tomar únicamente un bloque de información del archivo de la nomina y sustituirlo por otro. Con lo cual, estaría efectuando un fraude electrónico.

Para frustrar este tipo de ataque, el DES (y todos los cifradores de bloque) puede encadenarse de varias maneras para que el reemplazo de un bloque haga que el texto normal descifrado comenzando por el bloque reemplazado sea basura. Una forma de encadenar es por encadenamiento de bloque cifrado. En este método, que se muestra en la figura 3-4, a cada bloque de texto normal se le hace un OR EXCLUSIVO (#) con el bloque de texto cifrado previo antes de cifrarse. En consecuencia, el mismo bloque de texto normal no corresponde con el mismo bloque de texto cifrado, y el cifrado ya no es un cifrado por sustitución monoalfabética grande. Al primer bloque se le hace un OR EXCLUSIVO con un **vector de inicialización, IV**, seleccionado al azar, que se transmite junto con el texto cifrado.

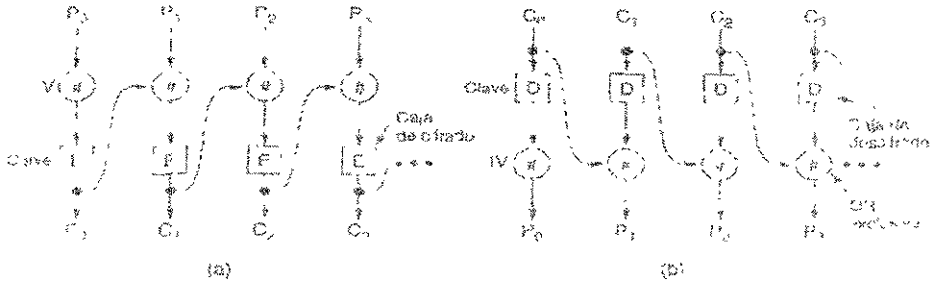


Figura 3-4. Encadenamiento de bloques cifrados [19,591]

Podemos ver cómo funciona el encadenamiento de bloques cifrados examinando el ejemplo de la figura 3-4. Comenzamos por calcular $C_0 = E(P_0 \text{ XOR } IV)$. Después calculamos $C_1 = E(P_1 \text{ XOR } C_0)$. etc. El descifrado funciona de la manera opuesta, con $P_0 = IV \text{ XOR } D(C_0)$, etc. Nótese que el cifrado del bloque *i* es una función de todo el texto normal de los bloques 0 a *i* - *1*, por lo que el texto normal genera un texto cifrado diferente dependiendo de dónde ocurre.

El encadenamiento de bloques cifrados también tiene la ventaja de que el mismo bloque de texto normal no produce el mismo bloque de texto cifrado, dificultando el criptoanálisis. De hecho, ésta es la razón principal de su uso.

Sin embargo, el encadenamiento de bloques cifrados tiene la desventaja de requerir la llegada de un bloque completo de 64 bits antes de poder iniciar el descifrado. Para el cifrado byte por byte puede usarse el modo de realimentación de cifrado, que se ilustra en la figura 3-5. Al llegar el byte de texto normal 10, como se aprecia en la figura 3-5(a), el algoritmo DES opera con el registro de desplazamiento de 64 bits para generar un texto cifrado de 64 bits. Se extrae el byte de la izquierda de ese texto cifrado y se le aplica un OR EXCLUSIVO con P_{10} Ese byte se envía por la línea de transmisión. Además, el registro de desplazamiento se desplaza a la izquierda 8 bits, causando la expulsión de C_2 por la izquierda y la introducción de C_{10} en la posición que C_9 dejó vacante a la derecha. Nótese que el contenido del registro de desplazamiento depende de la historia previa completa del texto normal, por lo que un patrón que se repite varias veces en el texto normal se cifrará de manera diferente en cada ocasión. Como ocurre con el encadenamiento de bloques cifrados, se requiere un vector de inicialización para echar a andar el mecanismo

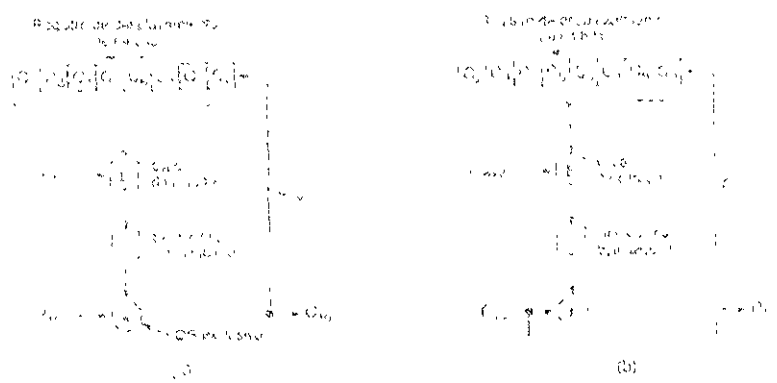


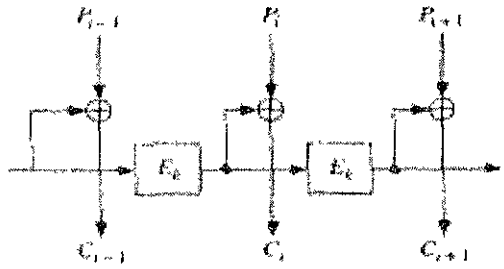
Figura 3-5 Modo de realimentación de cifrado [19,591]

El desencriptado con modo de realimentación de encriptado simplemente hace lo mismo que el encriptado. Mientras los dos registros de desplazamiento permanezcan idénticos, el descifrado funcionará correctamente.

Como nota al margen, debe indicarse que, si un bit del texto cifrado accidentalmente se invierte durante la transmisión, los 8 bytes descifrados cuando el byte malo esté en el registro de desplazamiento tendrán error. Una vez que el byte equivocado sea expulsado del registro de desplazamiento, se generará nuevamente texto normal correcto. Por tanto, el efecto de un solo bit invertido está bastante delimitado y no arruina el resto del mensaje.

Sin embargo, existen aplicaciones en las que un error de transmisión de 1 bit que arruina 64 bits de texto normal es un efecto demasiado grande. Para estas aplicaciones existe una cuarta opción, el modo de realimentación de salida, que es idéntico al modo de realimentación de cifrado, excepto que el byte realimentado por el lado derecho del registro de desplazamiento se toma justo antes de la caja de OR EXCLUSIVO, no justo después.

El modo de realimentación de salida tiene la propiedad de que un error de 1 bit en el texto cifrado causa un error de 1 solo bit en el texto normal resultante. Por otra parte, es menos seguro que los otros modos, y debe evitarse su uso de propósito general. El modo de libro de código electrónico también debe evitarse excepto en circunstancias especiales (por ejemplo, el cifrado de un solo número aleatorio, como una clave de sesión). Para la operación normal, debe usarse el



encadenamiento de bloques cifrados cuando la entrada llega en unidades de 8 bytes (por ejemplo, para cifrar archivos de disco) y el modo de realimentación de cifrado debe usarse para cadenas de entrada irregulares, como la entrada de un teclado.

Figura 3-6 Modo de realimentación de salida [18,204]

3.5.1.2 Descifrado del DES

El DES ha estado rodeado de controversias desde el día en que se propuso; se basó en un cifrado desarrollado y patentado por IBM, llamado Lucifer, excepto que el cifrado de IBM usaba una clave de 128 bits en lugar de 56 bits. Cuando el gobierno federal de Estados Unidos quiso estandarizar un método de cifrado para uso no confidencial, "invitó" a IBM a "debatir" el asunto con la NSA (*"National Security Agency"*. Agencia Nacional de Seguridad).

Tras estos debates, la IBM redujo la clave de 128 a 56 bits y decidió mantener en secreto el proceso de diseño del DES. Mucha gente sospechó que la longitud de la clave se redujo para asegurar que la NSA pudiera descifrar el código, pero no así alguna otra organización de menor presupuesto. El objetivo del diseño secreto supuestamente era esconder una puerta secreta que pudiera facilitar aún más el descifrado del DES por la NSA.[19,592]

DES puede ser atacado mediante la fuerza bruta, probando todas las claves posibles (2^{56}), siendo este algoritmo de una complejidad $O(2^{55})$. A pesar de los rumores que aseguraban que el NSA modificó el algoritmo para hacerlo más débil, aún no ha sido roto públicamente más que por la fuerza bruta

Probablemente la idea más innovadora para descifrar el DES es la lotería china (conceptualizada por Quisquater y Girault en 1991). En este diseño, cada radio y televisión tiene que equiparse con un chip DES barato capaz de realizar 1 millón de cifrados por segundo en "hardware". Suponiendo

que cada una de las 1.2 mil millones de personas de China tiene un radio o televisión, cada vez que el gobierno quiera descifrar un mensaje codificado con DES, simplemente difunde el par texto normal / texto cifrado, y cada uno de los 1.2 mil millones de chips comienza a buscar su sección preasignada del espacio de claves. En 60 segundos se encontrarán una o más correspondencias. Para asegurar que se informen, los chips podrían programarse para desplegar o anunciar el mensaje: ¡FELICIDADES! ACABA DE GANAR LA LOTERÍA CHINA. PARA COBRAR EL PREMIO, POR FAVOR LLAME AL 1-800-GRAN-PREMIO.

La conclusión que se puede obtener de estos argumentos es que el DES ya no debería usarse para nada importante. Sin embargo, aunque 2^{56} es 7×10^{16}, 2^{112} es 5×10^{33}. Aun con mil millones de chips DES efectuando mil millones de operaciones por segundo, se requerirían 100 millones de años para examinar detalladamente un espacio de claves de 112 bits. Por tanto, surge la idea de simplemente ejecutar el DES dos veces, con dos claves de 56 bits diferentes.

Desgraciadamente, Merkle y Hellman (1981) han desarrollado un método que hace sospechoso al doble cifrado. Se llama ataque de encuentro a la mitad ("meet-in-the-middle") y funciona como sigue (Hellman 1980). Supóngase que alguien ha cifrado doblemente una serie de bloques de texto normal usando el modo de libro de código electrónico Para unos pocos valores de i el criptoanalista tiene pares igualados (P_i, C_i) donde

$$C_i = E_{K2}(E_{K1} (P_i))$$

Si ahora aplicamos la función de descifrado, D_{K2}, a cada lado de esta ecuación, obtenemos:

$$D_{K2} (C_i) = E_{K1} (P_i) \qquad (I)$$

porque el cifrado de x y su descifrado posterior con la misma clave produce x.

El ataque de encuentro a la mitad usa esta ecuación para encontrar las claves DES, *K1* y *K2*, como sigue.

1. Calcular $R_i = E_i (P_1)$ para los 2^{56} valores de i, donde E es la función de cifrado DES. Ordenar esta tabla en orden ascendente según R_i.

2. Calcular $S_j = D_j (C_1)$ para todos los 2^{56} valores de j, donde D es la función de descifrado DES. Ordenar esta tabla en orden ascendente según S_j.

3. Barrer la primera tabla en busca de un R_i igual a algún S_j de la segunda tabla. Al encontrar un par, tenemos un par de claves (i, j) tal que $D_j (C_1) = E_i (P_1)$. Potencialmente, i es *K1* y j es *K2*.

4. Comprobar si $E_j (E_i (P_2))$ es igual a C_2. Si lo es, intentar todos los demás pares (texto normal, texto cifrado) De no serlo, continuar buscando pares en las dos tablas.

Ciertamente ocurrirán muchas falsas alarmas antes de encontrar las claves reales, pero tarde o temprano se encontrarán. Este ataque requiere sólo 2^{57} operaciones de cifrado o descifrado (para construir las dos tablas), mucho menos que 2^{112}; sin embargo, también requiere un total de 2^{60} bytes de almacenamiento para las dos tablas, por lo que actualmente no es factible en su forma básica, pero Merkle y Hellman han mostrado varias optimizaciones y concesiones que permiten menos almacenamiento a expensas de más cómputo. En conclusión, el cifrado doble usando el DES probablemente no es mucho más seguro que el cifrado sencillo.

3.5.2 Triple-DES (3DES)

Para 1979, IBM se dio cuenta de que la longitud de la clave DES era demasiado corta y diseñó una manera de aumentarla efectivamente usando codificación triple (modificación ideada por Tuchman). El método seleccionado, que se ha incorporado al estándar internacional 8732, se ilustra en la figura 3-6. Aquí se usan dos claves y tres etapas. En la primera etapa, el texto normal se cifra con *K1*. En la segunda etapa, el DES se ejecuta en modo de descifrado, usando *K2* como clave. Por último, se hace otro cifrado usando *K1*.

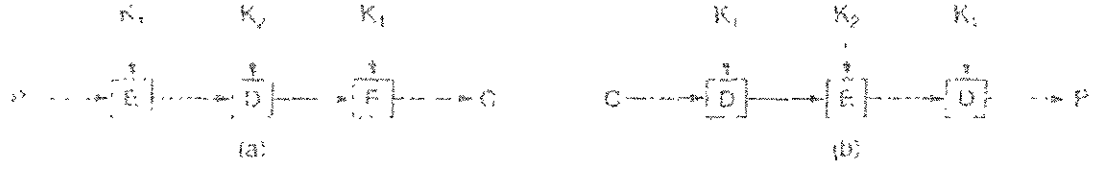


Figura 3-7. Cifrado triple usando el DES. [19,594]

Este diseño inmediatamente da pie a dos preguntas. Primero, ¿por qué sólo se usan dos claves en lugar de tres? Segundo, ¿por qué se usa EDE (cifrado-descifrado-cifrado) en lugar de EEE (cifrado-cifrado-cifrado)? La razón de que se usen dos claves es que incluso los criptógrafos más paranoicos coinciden en que 112 bits son suficientes para las aplicaciones comerciales por ahora. Subir a 168 bits simplemente agregaría la carga extra innecesaria de administrar y transportar otra clave.

La razón para cifrar, descifrar y luego cifrar de nuevo es la compatibilidad en reversa con los sistemas DES de una sola clave. Tanto las funciones de cifrado como de descifrado son correspondencias entre grupos de números de 64 bits. Desde el punto de vista criptográfico, las dos correspondencias son igualmente robustas. Sin embargo, usando EDE en lugar de EFE, una computadora que usa cifrado triple puede hablar con otra que usa cifrado sencillo simplemente estableciendo *K1 = K2*. Esta propiedad permite la introducción gradual del cifrado triple, algo que no interesa a los criptógrafos académicos, pero de importancia considerable para IBM y sus clientes.

No se conoce ningún método para descifrar el DES triple en modo EDE. Van Oorschot y Wiener (1988) han presentado un método para acelerar la búsqueda de EDE en un factor de 16, pero aun con su ataque, el EDE es muy seguro. Para cualquiera que desea nada menos que lo mejor, se recomienda el EEE con tres diferentes claves de 56 bits (168 bits en total).

Antes de dejar el tema del DES, vale la pena cuando menos mencionar dos recientes avances del criptoanálisis. El primero es el criptoanálisis diferencial (dado a conocer por Biham y Shamir en 1993). Esta técnica puede usarse para atacar cualquier cifrado en bloques; funciona comenzando por un par de bloques de texto normal que difieren sólo en una cantidad pequeña de bits y observando cuidadosamente lo que ocurre en cada iteración interna a medida que avanza el cifrado. En muchos casos, algunos patrones son mucho más comunes que otros, y esta observación conduce a un ataque probabilístico.

El otro avance que vale la pena mencionar es el criptoanálisis lineal (ideado por Matsui en 1994). Que puede descifrar el DES con sólo 2^{43} textos comunes conocidos. Funciona haciendo un OR EXCLUSIVO entre ciertos bits de texto normal y texto cifrado para generar 1 bit. Al hacerse repetidamente, la mitad de los bits deben ser ceros y la otra deben ser unos. Sin embargo, con frecuencia los cifrados introducen un sesgo en una dirección o en la otra, y este sesgo, por pequeño que sea, puede explotarse para reducir el factor de trabajo.

Existen varias implementaciones de triple DES:

- DES-EEE3. Se cifra tres veces con una clave diferente cada vez.

- DES-EDE3. Primero se cifra, luego se descifra y por último se vuelve a cifrar, cada vez con una clave diferente.
- DES-EEE2 y DES-EDE2. Similares a los anteriores con la salvedad de que la clave usada en el primer y en el último paso coinciden.

Se estima que las dos primeras implementaciones, con claves diferentes, son las más seguras. Si se quiere romper el algoritmo usando la fuerza bruta, la complejidad asciende a $O(2^{112})$.

3.5.3 IDEA

En este punto, es válido preguntarse con toda razón: "si el DES es tan débil, ¿por qué no ha inventado nadie un mejor cifrado de bloques?". La realidad es que se han propuesto muchos cifrados de bloques, incluidos BLOWFISH (creado por Schneier en 1994), Crab (ideado por Kaliski y Robshaw en 1994), FEAL (conceptualizado por Shimizu y Miyaguchi en 1988), KHAFRE (creado por Merkle en 1991), LOKI91 (ideado Brown y otros en 1991), NEWDES (conceptualizado por Scott en 1985), REDOCII (creado por Cusick y Wood en 1991), y SAFER K64 (diseñado por Massey en 1994). Para obtener más información de cada uno de estos algoritmos, se recomienda consultar la bibliografía [18]. Probablemente el más interesante e importante de los cifrados de bloques posteriores al DES es el IDEA (International Data Encryption Algorithm, algoritmo internacional de cifrado de datos diseñado por Lai y Massey, fue propuesto en 1990 y rediseñado para 1992).

IDEA fue diseñado por dos investigadores en Suiza, por lo que probablemente está libre de cualquier "asesoría" de la NSA que podría haber introducido una puerta secreta; usa una clave de 128 bits, lo que lo hará inmune durante décadas a los ataques de la fuerza bruta, la lotería china y a los ataques de encuentro a la mitad. También se diseñó para resistir el criptoanálisis diferencial. No hay ninguna técnica o máquina conocida actualmente que se crea que puede violar el IDEA.

La estructura básica del algoritmo semeja al DES en cuanto a que se alteran bloques de entrada de texto normal de 64 bits en una secuencia de iteraciones parametrizadas para producir bloques de salida de texto cifrado de 64 bits, como se muestra en la figura 3-7(a). Dada la extensa alteración de bits, basta con ocho iteraciones. Como con todos los cifrados de bloque, el IDEA puede usar cada uno de los modos de operación del DES

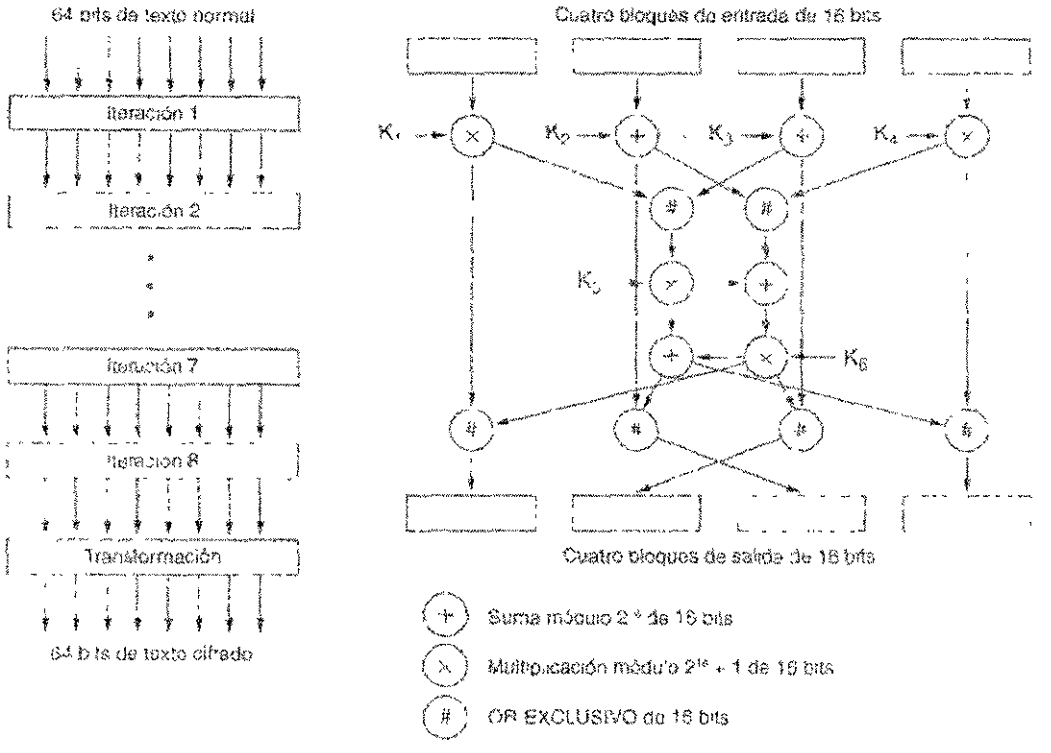


Figura 3-8. (a) IDEA (b) Detalle de una iteración

Los detalles de una iteración se presentan en la figura 3-8(b). Se usan tres operaciones, todas sobre números sin signo de 16 bits. Estas operaciones son OR EXCLUSIVO, suma módulo 2^{16} y multiplicación módulo $2^{16} + 1$. Las tres se pueden efectuar fácilmente en una microcomputadora de 16 bits ignorando las partes de orden mayor de los resultados. Las operaciones tienen la propiedad de que ningunos dos pares obedecen la ley asociativa ni la ley distributiva, dificultando el criptoanálisis. La clave de 128 bits se usa para generar 52 subclaves de 16 bits cada una, 6 por cada una de las ocho iteraciones y 4 para la transformación final. El descifrado usa el mismo algoritmo que el cifrado, sólo que con subclaves diferentes.

3.5.4 RC-2 y RC-4

RC-2 y RC-4 fueron desarrollados por Ron Rivest, uno de los coautores del algoritmo RSA, en 1989 y 1987, respectivamente. Durante varios años, se ha tratado de algoritmos con propietario y sus detalles no fueron hechos públicos. De este modo, su seguridad se basaba en el prestigio de su autor y en el respaldo que les daba RSA Data Security, Inc. Sin embargo, en 1994 RC4 fue sometido a ingeniería inversa y los resultados publicados en Internet. Las pruebas hechas a dicho diseño se ajustan a los resultados esperados por lo que es razonable pensar que el diseño publicado es correcto. RC2 fue finalmente publicado como "Internet Draft" en 1997.

RC-2 es un cifrador de bloque con una longitud de clave variable. Tiene definido los mismos modos que DES y, con una clave de 64 bits, su implementación en "software" es dos o tres veces más rápida que la de DES

RC-4, al igual que RC-2, tiene una longitud de clave variable. Sin embargo, se trata de un cifrador de flujo.

Como el resto de productos criptográficos desarrollados en EE.UU., las restricciones a su exportación son muy fuertes. RC-2 y RC-4 tienen un estatus especial que facilita la concesión de licencias de exportación de productos basados en ellos, pero limitando la longitud de su clave a 40 bits. RC-4 y RC2 se usan en centenares de productos comerciales. El protocolo SSL también los usa.

3.5.5 Blowfish

Blowfish es un algoritmo de encriptado de bloque creado por Bruce Schneier [18,336]. Inicialmente pensado para construirse en "hardware", sus criterios de diseño se centraron en lo siguiente:

1. **Velocidad.** Blowfish encripta un byte en 26 ciclos de reloj, en un microprocesador de 32 bits.

2. **Memoria.** Sólo requiere 5 kB.

3. **Simplicidad.** Blowfish utiliza operaciones sencillas: suma, XOR y búsquedas en tablas de 32 operandos.

4. **Longitud de llave variable**. Por último, la longitud de la llave para Blowfish puede ser hasta de 448 bits.

Blowfish es un cifrador de bloque de 64 bits con una llave de longitud variable. El algoritmo consiste de dos partes: la expansión de la llave y el encriptado de datos. La expansión de llave convierte una llave de a lo más 448 bits en varios arreglos de llaves totalizando 4168 bytes.

La encriptación de datos consiste simplemente en una función iterada 16 veces. Cada iteración consiste de una permutación dependiente de la llave y una sustitución que depende tanto de la llave como de los datos.

En la figura 3-9 (a) se muestra el detalle de iteraciones del algoritmo, mientras que en la figura 3-9 (b) se observa el detalle de una función F.

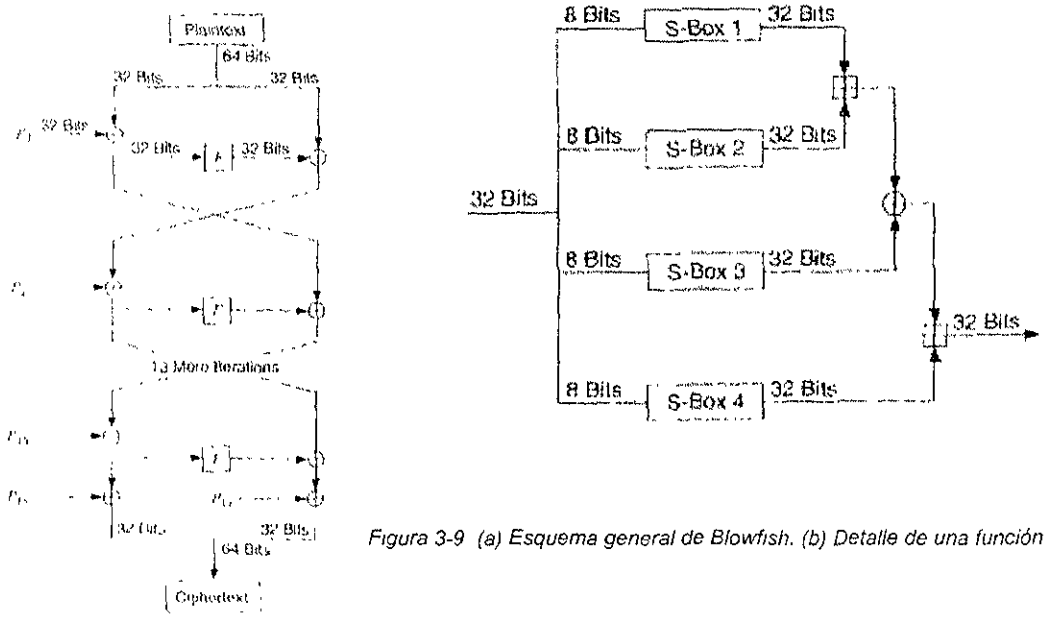


Figura 3-9 (a) Esquema general de Blowfish. (b) Detalle de una función F [18,337]

3.6 Uso de Funciones Resumen (o de "hash") para Criptografía

Una función resumen o de "hash" *H* es una transformación que, tomando como entrada una cadena *x* de bits de longitud variable, produce como salida una cadena *h* de bits de longitud fija (*h* = *H(x)*). Para que una función de este tipo pueda usarse con propósitos criptográficos, se debe cumplir una serie de requisitos[41]:

- la entrada puede tener cualquier longitud. Deben proveerse mecanismos para evitar el desbordamiento ("overflow").
- la salida debe ser de longitud fija, independientemente de cual fuera la longitud de la entrada.
- para cualquier entrada, su resumen (o valor de "hash") debe ser sencillo de calcular.
- la función resumen debe ser de un "único sentido", entendiendo por este concepto que, dado *f(x)*, debe ser computacionalmente difícil encontrar un valor *y* (tal vez el mismo *x*) tal que *f(y)* = *f(x)*.
- es difícil encontrar dos entradas *x* e *y*, tales que *H(x)* = *H(y)* (colisiones).

Al resumen o valor de "hash" de un mensaje *M* se le llama generalmente huella digital de *M*. Si la salida de la función tiene una longitud de *n* bits, entonces existen $k = 2^n$ salidas diferentes. Las funciones resumen son también extensivamente utilizadas como parte de los mecanismos que generan números aleatorios. Ejemplos de funciones resumen usadas en criptografía son MD2, MD4, MD5 o SHA-1.

3.6.1 Ataque de las funciones resumen

Como se desprende de las condiciones que debe presentar una función resumen, el ataque a dichas funciones puede verse desde dos puntos de vista.

Si, dado un mensaje *x* y su resumen *H(x)*, sólo mediante una búsqueda exhaustiva es posible hallar un mensaje y tal que *H(x)* = *H(y)*, entonces, la función resumen *H* se denomina débilmente libre de colisiones. La búsqueda exhaustiva consiste en calcular el resumen de cada entrada posible y hasta que se obtenga el valor *H(x)* conocido. Este ataque aparece en un escenario con dos actores en el cual una tercera parte intenta engañar a una de las otras calculando una entrada con un valor resumen igual al del mensaje cuyo resumen ha interceptado.

Una función resumen fuertemente libre de colisiones es aquella para la que no es posible hallar dos mensajes *x* e *y* tales que *H(x)* = *H(y)*. En este caso es una de las dos partes implicadas la que trata de engañar a la contraria, tratando de atacar la integridad de los mensajes cuyo resumen se ha calculado.

Generalmente, el ataque a funciones resumen aparece en el primero de los escenarios, en el que se utilizan huellas digitales para firmar un mensaje. Un típico ataque es el conocido como ataque del cumpleaños, el cual se basa en una curiosa paradoja, que da nombre al ataque Se trata de la paradoja del cumpleaños, que establece que la probabilidad de que dos o mas personas de un grupo de 23 compartan la misma fecha de cumpleaños es mayor que 1/2

Matemáticamente, supongamos una función, alimentada con una entrada aleatoria, que produce *k* salidas equiprobables. Entonces, probando repetidamente diferentes entradas, esperamos obtener la misma salida después de probar $(2k)^{1/2}$ entradas y no, como cabría esperar $k^{1/2}$

Teniendo en cuenta que $k = 2^n$ (en donde *n* es la longitud en bits de la salida) debemos elegir valores de *n* lo suficientemente grandes como para impedir este cálculo inverso.

Estos resultados no son significativos cuando se utiliza una función resumen para otros propósitos. El más usado de estos cometidos es la generación de números aleatorios. El descubrimiento de colisiones en una función no parece afectar de un modo práctico a la utilidad de estas funciones.

3.6.2 MD4 y MD5

MD4 y MD5 son funciones resumen usadas en criptografía. Su nombre proviene de "Messages Digest" (resumen de mensajes) y fueron diseñados por Ron Rivest. Se emplean fundamentalmente en la generación de huellas digitales de documentos, mensajes de correo electrónico y objetos similares. Los dos algoritmos generan huellas con una longitud de 128 bits[41].

MD4 fue introducida en 1990 con el objetivo fundamental de ser una función rápida. Sin embargo, ya en 1995 se demostró que era posible hallar colisiones para MD4 en menos de un minuto utilizando un simple PC. Consecuentemente, MD4 ya no es considerado seguro.

MD5 es una versión mejorada (aunque algo más lenta) de MD4, desarrollada por Ron Rivest en 1991. Su fortaleza es grande y, dado que la longitud de la salida es 128 bits, la probabilidad de obtener dos mensajes con el mismo resumen es de 2^{64}, en tanto que la dificultad de obtener un mensaje cuyo resumen sea igual a uno dado es de 2^{123}.

Aunque se ha avanzado en su estudio y se ha demostrado que es posible hallar colisiones para la función de compresión que utiliza el algoritmo, no se ha demostrado que puedan hallarse para el algoritmo entero. De momento es considerado seguro, aunque se recomienda que, "por lo que pudiera pasar", se debe actualizar cualquier producto que lo utilice a otros algoritmos como SHA-1.

3.6.3 SHA y SHA-1

SHA ("Secure Hash Algorithm") fue desarrollado en 1993 por NIST ("National Institute for Standards and Technology") junto con NSA ("National Security Agency") en EE.UU. para su uso en la norma estadounidense de firma digital. En 1994, el propio NIST publica una revisión de este último, conocida como SHA-1, la cual corrige un defecto no publicado de SHA.

SHA es muy similar en su modo de operación a MD5. Utilizan como entrada mensajes de menos de 2^{64} bits y generan salidas de 160 bits, más largas que las producidas por cualquier otra función resumen utilizada anteriormente. Este algoritmo es ligeramente más lento que MD5, pero la mayor longitud del resumen del mensaje lo hace más seguro frente a la búsqueda de colisiones usando la fuerza bruta [41]

3.7 Criptografía de clave asimétrica o pública

El principal problema que presenta el uso práctico de la criptografía de clave simétrica es la distribución de las claves. La criptografía de clave asimétrica o pública, sin embargo, usa claves diferentes para cifrar y descifrar un mensaje Lo único que se transmite de un usuario a otro es el mensaje cifrado.

En 1976, Whitfield Diffie y Martin Hellman publican la idea de que cada usuario tenga dos claves. una pública (P_i, conocida por cualquiera) y otra privada (S_i, sólo conocida por su dueño).

Entre estas claves existe una relación particular que permite a una de ellas cifrar un mensaje mientras que la otra es empleada para descifrarlo. Las claves privadas deben ser conservadas por su propietario del modo más seguro posible.

Supongamos un algoritmo de cifrado *E* y otro de descifrado *D*, aplicados a un mensaje *M*. Debe cumplirse que [15,25]:

$$D(E(M, P_i), S_i) = M$$

La seguridad de un sistema de este tipo depende de que las funciones de cifrado y descifrado, *E* y *D*, cumplan una serie de condiciones:

- dados el mensaje *M* y la clave pública *P* que vayamos a utilizar, el mensaje cifrado, *C*, debe ser fácil de calcular.
- dado *C*, el mensaje original, *M*, no debe ser obtenible de forma sencilla.
- dados *C* y la clave privada, *S*, debe ser sencillo descifrar el mensaje original
- para que sea práctico el uso de criptografía de clave asimétrica, debe ser sencillo calcular parejas aleatorias de claves *P* y *S*.

La criptografía de clave asimétrica posee, sin embargo, dos inconvenientes:

1. el primero se refiere a la velocidad. Los sistemas basados en clave asimétrica son notablemente más lentos que sus equivalentes de clave simétrica (por lo general y como mínimo, unos dos órdenes de magnitud). Por tanto estos sistemas no suelen ser adecuados para el cifrado masivo de datos.
2. el segundo está relacionado con la validación de la clave. La discusión sobre la fortaleza de un algoritmo de clave asimétrica es irrelevante sin una discusión previa sobre el protocolo de validación de las claves.

3.7.1 Algoritmo Rivest-Shamir-Adleman (RSA)

El algoritmo RSA se fundamenta en el hecho de que la factorización de números primos es un problema de resolución computacionalmente difícil. El algoritmo RSA está descrito en infinidad de libros y páginas Web; y se basa en lo siguiente:

Primero es necesario calcular las claves.

a. encontrar dos números primos grandes (de 100 cifras o más), ***p*** y ***q***.
b. definir ***n*** (conocido como módulo) como: ***n = pq***
c. definir ***z*** como: ***z = (p-1)(q-1)***
d. encontrar un número primo aleatorio ***e*** menor que el módulo y tal que ***e*** y ***z*** sean primos entre sí.
e. determinar un valor ***d*** tal que se cumpla que ***(ed - 1)*** es divisible entre ***z*** (***d*** existe y es único).

El cifrado del mensaje M se obtendrá según la siguiente operación: $C = M^e \pmod n$

Y el descifrado mediante la siguiente: $M = C^d \pmod n$

Por tanto, la clave pública estará constituida por el par ***(n,e)***, mientras que la clave privada la constituirán ***(n,d)***

3.7.1.1 Ejemplo

Supongamos ***p=47*** y ***q=57***
Por tanto, ***n=pq=2773***

De estos datos, se calcula ***(p-1)(q-1)=2668***

Eligiendo ***e=17***, calculamos ***d*** utilizando algoritmos de factorización ***(d=157)***

Por tanto, la clave pública ***P*** será el par (17, 2773), mientras que la privada, ***S***, la constituirá el par (157, 2773).

3.7.1.2 Funcionamiento

Como ya hemos señalado, el algoritmo RSA se fundamenta en el hecho de que factorizar números muy grandes es un problema de difícil resolución. Si un intruso que quisiera quebrar el algoritmo fuese capaz de factorizar ***n*** (parte de la clave pública), entonces podría utilizar estos factores para deducir rápidamente ***e*** y ***d***. Por lo tanto, si fuese fácil factorizar números grandes, sería fácil romper RSA. Lo contrario, es decir, si por ser difícil factorizar números muy grandes es difícil romper RSA no se ha demostrado (de hecho, tampoco se ha demostrado que factorizar números muy grandes sea en realidad un problema difícil).

Para lograr la máxima seguridad, es necesario utilizar enteros de más de 100 dígitos de longitud, pues factorizar números más pequeños es posible. Según Bruce Schneier [15], un número de 129 dígitos decimales está en el borde de las tecnología y técnicas de factorización. Además, se debe asegurar que el producto ***(p-1)(q-1)*** no tiene factores primos pequeños.

3.7.1.3 Rapidez

Fruto de los requerimientos para hacer seguro RSA, surge su principal problema: su lentitud. En general, se elige como clave pública el menor de los dos exponentes a fin de conseguir que el proceso de cifrado sea el más rápido (más que el descifrado, el cual, a su vez lo es más que la generación de claves). El cifrado, que utiliza la clave pública, tiene una complejidad de $O(k^2)$, el descifrado $O(k^3)$ y la generación de claves $O(k^4)$, en donde ***k*** es la longitud en bits del módulo.

Una práctica habitual es elegir como clave pública un exponente pequeño, típicamente 1001 ó 10001, variando el módulo.

3.7.1.4 Patentes

Como consecuencia de la precipitada publicación del algoritmo RSA (ante el temor de que la administración de seguridad de EE.UU no permitiera que se diera a conocer), la solicitud de patente se realizó posteriormente a su publicación Expiró el 20 de septiembre de 2000.

3.7.1.5 Sumario

Clave pública	***n*** : producto de dos números primos, ***p*** y ***q*** (que deben permanecer secretos).
	e : relativamente primo a ***(p-1)(q-1)***.
Clave privada	***n*** : mismo componente que para la clave pública.
	$d : e^{-1} \bmod ((p-1)(q-1))$
Cifrado	$c = m^e \bmod n$
Descifrado	$m = c^d \bmod n$

3.7.2 Algoritmo ElGamal

El algoritmo ElGamal (también conocido como algoritmo Diffie-Hellman, variante ElGamal) se basa en la dificultad de calcular algoritmos discretos en un campo finito.

3.7.2.1 Par de claves

Para generar un par de claves, se elige un número primo, p, y dos números aleatorios, g y x, de modo que sean más pequeños que p. Calculando:

$$y = g^x \bmod p$$

La clave pública es y, g y p (grupos de usuarios pueden compartir g y p, diferenciándose sólo en y). La clave privada es x.

3.7.2.2 Firmas digitales

Para firmar un mensaje, M, una vez generado el par de claves, el algoritmo es el siguiente:

- se elige un número aleatorio, k, tal que k es relativamente primo a $p-1$.
- se calcula a como: $a = g^k \bmod p$
- se despeja b en la ecuación: $M = (xa + kb) \bmod (p-1)$
  (para lo que se usa una herramienta matemática conocida como algoritmo extendido de Euclides)
- la firma digital del mensaje está compuesta de a y b. El valor aleatorio k que se ha usado para calcular la firma digital, debe permanecer en secreto.
- para verificar la firma se debe cumplir la siguiente igualdad: $y^a a^b \bmod p = g^M \bmod p$

Cada firmado debe utilizar un valor aleatorio k distinto. Si un intruso es capaz de averiguar cual ha sido el valor de k utilizado, puede obtener x (la clave privada). También si intercepta dos mensajes firmados (o cifrados) que sepa a ciencia cierta que provienen del mismo valor k, incluso si no sabe cual es, puede obtener también la clave privada.

3.7.2.3 Cifrado

El proceso de cifrado de un mensaje es muy similar al de firmado:

- se elige un número aleatorio, k, tal que k es relativamente primo a $p-1$.
- se calcula a como: $a = g^k \bmod p$
- se calcula b como: $b = y^k M \bmod p$
- el mensaje cifrado está compuesto de a y b. El tamaño del texto cifrado es el doble que el del texto original.
- para descifrar el mensaje, hay que calcular: $M = b/a^x \bmod p$

El resultado es el mismo que el del algoritmo de intercambio de claves de Diffie y Hellman, excepto en que y es parte de la clave y que lo cifrado se multiplica por y^k.

3.7.2.4 Patentes

El algoritmo ElGamal no se encuentra patentado. Sin embargo, PKP considera que este algoritmo se encuentra cubierto por la patente del algoritmo Diffie-Hellman. De todas formas, esta patente expiró el 29 de abril de 1997, por lo que ya es de libre uso.

3.7.2.5 Sumario

Clave pública	p : primo.
	$g < p$: puede compartirse entre grupos de usuarios.
	$y = g^x \bmod p$
Clave privada	$x < p$
Cifrado	k : elegido aleatoriamente, de modo que sea relativamente primo a $p-1$
	a (texto cifrado) = $g^k \bmod p$
	b (texto cifrado) = $y^k M \bmod p$
Descifrado	M (texto en claro) = $b/a^x \bmod p$
Firmado	$c = m^e \bmod n$

Verificado	$m = c^d \bmod n$

3.8 Autentificación mediante criptografía de clave asimétrica

La criptografía de clave pública puede ser utilizada para identificar sin ambigüedades al remitente de un mensaje. Esto es posible teniendo en cuenta que, si el remitente encripta con su clave privada el mensaje que envía, éste solamente puede ser desencriptado en el destino utilizando la clave pública del remitente.

Si el mensaje no puede ser desencriptado con la clave pública de quien afirma ser el remitente, éste no ha sido el remitente del mensaje. La posibilidad de descifrar el mensaje es prueba fehaciente de la identidad del remitente.

La probabilidad de que dos personas diferentes tengan la misma combinación clave pública / clave privada es insignificante.

La desventaja de la utilización de cualquier algoritmo de clave pública es su lentitud, por lo que resulta poco práctico el cifrado asimétrico del mensaje entero.

3.8.1 Códigos de integridad

Como acabamos de señalar, resulta poco práctico la aplicación de técnicas asimétricas a un mensaje entero. En tal caso, se utilizan funciones resumen que derivan una huella digital (en ingles, MAC, "Messages Authentication Code") a partir de un cierto volumen de datos [41]

Esto es debido a que las funciones resumen poseen dos propiedades que las hacen ideales para este trabajo La primera es que su resultado es relativamente corto (típicamente una huella tiene entre 128 y 160 bits). Segundo y más importante, aunque sea teóricamente posible encontrar dos mensajes con idéntica huella, la probabilidad de que esto ocurra es ínfima. Si se manipulan los datos, la huella cambia. Modificar los datos de forma tan sabia como para obtener la misma huella es algo computacionalmente inabordable.

3.8.2 Firmas digitales

La firma manuscrita como medio para acreditar la identidad del firmante de un documento ha sido, y sigue siendo, ampliamente usada por las sociedades humanas desde hace siglos. Su equivalente en la actual sociedad de la información es lo que se conoce como firma digital.

Además de la capacidad de autentificar al signatario de un mensaje, la firma digital posee otra cualidad interesante, que consiste en mantener la integridad del mensaje firmado. Dado un mensaje, basta calcular su huella digital y cifrarla con la clave privada del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). El procedimiento que se utiliza es el siguiente:

1. Se aplica una función resumen ***f*** al mensaje ***M***. El resultado ***f(M)*** es la huella digital del mensaje.
2. A continuación, se encripta con su clave privada el resultado del paso anterior
3. Posteriormente es enviado tanto el mensaje como la firma digital (la huella digital cifrada con su clave privada) al receptor

4. El receptor, que conoce la función resumen utilizada y la clave pública del emisor, realiza dos operaciones: aplica la función resumen al mensaje y descifra la firma digital.
5. Si ambos resultados coinciden, el receptor tiene la certeza de dos hechos: que el mensaje no ha sido modificado en su tránsito por la red; y que el mensaje ha sido emitido, efectivamente, por quien dijo ser el emisor.

El problema ahora es de otro tipo. ¿Cómo aseguramos que el par clave pública / clave privada que asociamos al emisor es realmente suya y no de un intruso? Nos referimos al problema de validación de la clave.

3.9 Certificados Digitales

Los certificados son documentos digitales que atestiguan que una clave pública corresponde a un individuo o entidad determinados. De este modo evitamos que intrusos utilicen una combinación de claves asegurando ser otra persona.

En su forma más simple, un certificado consiste en una clave pública y el nombre de su propietario. Este certificado es firmado por una autoridad de certificación ("Certification Authority", CA), cuya clave pública es fácilmente verificable. Adicionalmente, puede contener la fecha de expedición del certificado, la de expiración de la clave, el nombre del notario electrónico que emitió el certificado y un número de serie. De todo ello calcula la huella digital con la función de "hash" adecuada y la cifra con su clave privada.

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma del ITU-T X.509 (versión 3), la cual forma parte del servicio de directorio diseñado por ISO para el modelo OSI. En el certificado se incluyen[41]:

- versión de la norma X.509 usada.
- número de serie del certificado.
- algoritmo utilizado por la autoridad de certificación (algoritmo de clave asimétrica y función de resumen usada).
- nombres que identifican univocamente al dueño del certificado y a la autoridad de certificación.
- la clave pública del dueño del certificado, junto con la información de los algoritmos utilizados.
- la firma digital de la autoridad de certificación

Las autoridades de certificación deben ser entes fiables y ampliamente reconocidos que firman (con conocimiento de causa y asunción de responsabilidades legales) las claves públicas de las personas, rubricando con su propia firma la identidad del usuario. El destinatario de un mensaje no recibe la clave pública del remitente sino su certificado

Debido a la posición comprometida que ocupan las autoridades de certificación, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento.

Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada. No podemos olvidar que la autoridad de certificación es la responsable, en última instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su "negocio" en la credibilidad que inspire en sus potenciales clientes.

3.9.1 Ciclo de vida de una clave

Las claves deben tener una fecha de expiración. De esta forma, es más difícil que los algoritmos que las utilizan sufran algún ataque. Cuando una clave ha sido averiguada por intrusos, se dice que ha sido comprometida.

El ciclo de vida de una clave incluye los siguientes periodos[41]:

a) **Generación** y, quizá, **registro** de la clave o par de claves. La clave o par de claves debe ser generada por su propietario o por la entidad que vaya a utilizar la(s) clave(s) para proteger sus comunicaciones con el usuario. Un problema frecuente radica en que los algoritmos generadores aleatorios de claves no son suficientemente "buenos". Si la clave es utilizada con algoritmos de criptografía de clave asimétrica, la clave pública puede ser registrada (generando un certificado).
b) **Distribución** de las claves. En el caso de criptografía de clave simétrica, la clave debe ser entregada al interlocutor de forma que no pueda ser interceptada por terceros. En caso de utilizar claves asimétricas, la distribución de esta clave está libre de problemas. Sin embargo, debe poder asegurarse que la clave corresponda a quien dice ser su propietario (mediante un certificado, o bien obteniendo la clave de una organización en la que se tenga plena confianza).
c) **Emisión y expiración**. La fecha de emisión determina a partir de qué instante va a ser válida la clave. En general, se trata del momento en el que ha sido generada (o certificada, en su caso). La expiración puede tener lugar al final de una comunicación concreta o en una fecha determinada. En el caso de la criptografía de clave pública, debe verificarse siempre en el certificado que la clave siga siendo válida.
d) **Retirada**. Si se sospecha, por cualquier motivo, que la clave ha sido comprometida, ha de acudirse a la autoridad de certificación para comunicárselo y que ésta proceda a certificar una nueva clave.
e) **Terminación**. Una vez que la clave finaliza su ciclo de vida, se almacena y es reemplazada por una nueva.

3.9.2 Almacenamiento y gestión de las claves

Uno de los problemas principales que aparece a la hora de utilizar criptografía es el de almacenamiento de las claves. El grado de seguridad con el que se almacena una clave debe ser directamente proporcional a la importancia de los mensajes que deben ser cifrados con dichas claves. Un método idóneo puede ser el uso de tarjetas inteligentes, que acceden al sistema mediante el "hardware" adecuado.

3.9.3 Recuperación de claves ("Key Recovery")

Uno de los argumentos del gobierno de los EE.UU. para impedir la exportación de productos criptográficos "fuertes" es la posibilidad de que éstos sean utilizados por gobiernos enemigos, terroristas o criminales en general, con lo que se vería amenazada la seguridad nacional. Sin embargo, la presión de la industria informática de los EE.UU. es fuerte y se vislumbra una relajación de las restricciones. La contrapartida es la introducción de mecanismos de recuperación de claves que permitan, bajo estricto mandato judicial, levantar las protecciones criptográficas de comunicaciones determinadas.

Con este trasfondo, y no ligadas específicamente a la política del gobierno de EE.UU., se han desarrollado dos técnicas, conceptualmente muy similares, para asegurar la gestión y almacenamiento de las claves (y, eventualmente, su recuperación) [41]:

1. *custodia de claves ("key escrow")*: es el usuario u organización quien genera su clave o claves y las entrega a otra parte que la guarda para él. Variantes de este mecanismo consisten en fragmentar la clave y confiar cada fragmento a custodios diferentes. De este modo, la protección de la clave queda en otras manos.
2. *tercera parte de confianza ("trusted third-party")*: en este caso, es una tercera parte la que genera la clave correspondiente a requerimiento del usuario, la distribuye a los receptores correctos y almacena una copia para sí misma. La seguridad de la clave queda de nuevo en otras manos diferentes a las de los usuarios.

3.10 Intercambio de claves simétricas (sistemas híbridos)

Dado que los algoritmos criptográficos de clave pública (como el ya citado RSA) son excesivamente lentos, se han desarrollado sistemas híbridos que utilizan criptografía de clave simétrica y de clave pública. El mecanismo, a grandes rasgos, es el siguiente:

1. Se genera una clave aleatoria que servirá de clave a un algoritmo simétrico (por ejemplo, DES).
2. Esta clave es cifrada con la clave pública del receptor y es enviada (criptografía de clave asimétrica).
3. El receptor toma el mensaje y, con su clave privada, procede a descifrarlo, obteniendo así la clave para el algoritmo simétrico.
4. El resto de comunicaciones entre el emisor y receptor se lleva a cabo usando algoritmos simétricos con la clave transmitida.

Con estos métodos híbridos se eliminan los problemas que origina la distribución de claves. Ahora bien, aparecen problemas nuevos, debidos fundamentalmente a la posibilidad de suplantación de alguno de los interlocutores. Esto solamente puede evitarse intercambiando certificados en lugar únicamente de claves cifradas.

3.10.1 Algoritmo de intercambio de claves Diffie-Hellman

Este algoritmo permite que dos usuarios intercambien una clave a través de un medio inseguro. Se utilizan dos parámetros públicos, p y g. El primero de ellos, p, es primo. El segundo, conocido como generador, se define como:

$$\forall\, n \in [1..(n-1)]\ \exists\, x \,/\, n = x^g \pmod{p}$$

El funcionamiento del protocolo se describe a continuación. Cuando Pepe y Manolo desean intercambiar una clave llevan a cabo el siguiente proceso:

I. Pepe genera aleatoriamente un valor privado a.
II Manolo hace lo propio, generando b.
III. Pepe genera un valor público $g^a \bmod p$.
IV. Manolo hace lo mismo generando $g^b \bmod p$.
V. Manolo y Pepe intercambian estos valores públicos.
VI. A continuación, Pepe calcula $K_a = (g^b \bmod p)^a = g^{ab} \bmod p$.
VII. Manolo hace un cálculo similar. $K_b = (g^a \bmod p)^b = g^{ab} \bmod p$.
VIII En este momento, ambos poseen una clave común K:

$$K = K_a = K_b = g^{ab} \bmod p$$

El fundamento de este algoritmo consiste en que es difícil calcular ***K***, aún conocidos los valores públicos p, g, $g^b \pmod p$ y $g^a \pmod p$.

Como ya hemos comentado para el caso general, el inconveniente principal de que adolece este algoritmo es la posibilidad de que un intruso intercepte las comunicaciones entre los dos interlocutores. Para evitarlo será necesario, simplemente, utilizar certificados.

3.11 Fortaleza de un algoritmo criptográfico

Un buen sistema criptográfico debe ser diseñado de modo que su rotura sea tan difícil como sea posible. En la práctica, un buen sistema es aquel que no puede ser roto en la práctica (aunque teóricamente pueda serlo). Sin embargo, esto no es, a menudo, fácil de demostrar. Un algoritmo criptográfico es considerado seguro si [41]:

- no existen puertas traseras. Es decir, no hay ningún método para recuperar un mensaje en claro a partir del mensaje cifrado sin utilizar búsquedas exhaustivas de la clave.
- el número de claves posible es lo suficientemente grande como para que la búsqueda exhaustiva no sea práctica.

Teóricamente, cualquier algoritmo basado en el uso de una clave puede ser roto probando todas las claves posibles. Este método es conocido como ataque basado en la fuerza bruta (como ya hemos señalado). Si este es el único método posible (se asume la inexistencia de puertas traseras), la potencia de computación necesaria crece exponencialmente con la longitud de la clave. Centrándonos en algoritmos de clave simétrica, por ejemplo, una clave de 32 bits de longitud requiere 2^{32} operaciones (aproximadamente 10^9).

Existe una regla empírica, conocida como la Ley de Moore, que establece que la potencia de computación disponible para una inversión monetaria fija se dobla, aproximadamente, cada año y medio. Por tanto, para mantener los actuales parámetros de protección, habría que añadir un bit a la clave cada dieciséis meses. Sistemas con claves de 64 bits son invulnerables en la actualidad, pero serán atacables en pocos años. Finalmente, sistemas con claves de 128 bits permanecerán resistentes a ataques basados en la fuerza bruta en un futuro previsible. Es de destacar, además, que el costo derivado de usar claves seguras (de 128 o más bits de longitud) no es significativamente mucho mayor que en el que incurren cifrados con claves "débiles".

En el caso de los algoritmos de clave asimétrica, las claves son mucho más largas. El problema no es ahora adivinar la clave, sino deducir la clave privada a partir de la pública. En el caso del algoritmo RSA, esto es equivalente a factorizar un entero muy grande con dos factores primos también grandes.

3.12 Otras técnicas de autentificación

Los esquemas de identificación son métodos mediante los que una entidad (un usuario, una máquina, etc.) puede probar su identidad a alguien distinto a sí mismo, sin revelar ningún dato propio esencial que permita que un intruso o su mismo interlocutor le suplanten.

Los esquemas de identificación implican que el aspirante:

- demuestra saber algo: palabras de paso.
- demuestra tener algo: una tarjeta magnética, por ejemplo.
- muestra algo característico e indeleble: retina, ADN, ritmo de teclado, ...
- está en un cierto sitio.
- existe un tercero de confianza que lo avala: certificados.

El método tradicional de identificación es el uso de una palabra de paso ("password"). Pepe se identifica a sí mismo frente a un servidor introduciendo su palabra de paso cuando trata de acceder a su cuenta. Desgraciadamente, este esquema es inseguro. La palabra de paso puede ser obtenida mediante:

- exposición no autorizada (robo de la palabra de paso).
- adivinación: es un hecho que los usuarios tienden a elegir palabras de paso inadecuadas, que pueden ser fácilmente adivinadas (utilizando "cracks")
- escucha en tránsito: mediante "sniffers", por ejemplo.
- reproducción ciega ("replay"): un intruso que haya interceptado las comunicaciones entre Pepe y el servidor puede repetir el mensaje previo (es decir, la palabra de paso) de Pepe, de modo que gane acceso a la cuenta o al recurso del usuario interceptado.
- alteración del verificador de la palabra de paso.

La autentificación mediante palabra de paso es un ejemplo de esquema de identificación unilateral, ya que sólo la entidad de uno de los extremos de la comunicación se identifica a si misma, sin obtener identificación desde el otro extremo.

Un mecanismo mucho más común consiste en el uso de firmas digitales y de criptografía de clave pública usando esquemas reto-respuesta: Pepe envía retos a Manolo con diferentes preguntas y verifica las respuestas hasta que considera que la persona que responde a sus retos es, efectivamente, Manolo.

En uno de tales esquemas (similar, conceptualmente, al utilizado por el "Handshake Protocol" de SSL), Pepe genera un número aleatorio y se lo transmite a Manolo Éste genera un nuevo número aleatorio y firma digitalmente un mensaje, el cual contiene ambos números aleatorios. Entonces envía el mensaje firmado, junto con su número aleatorio a Pepe. Pepe verifica la firma para asegurarse de que se está comunicando, efectivamente, con Manolo. Este esquema es resistente frente a intrusos interceptando la línea. También previene la suplantación de Pepe por Manolo más adelante. Hasta este punto, el protocolo es unilateral.

Para identificarse a si mismo, Pepe puede también firmar el mensaje que contiene ambos números aleatorios y devolver el mensaje firmado a Manolo. Manolo verifique la firma para convencerse de la identidad de Pepe. Este es un ejemplo de un esquema de identificación mutua.

3.13 El estatus de los productos criptográficos

3.13.1 Las restricciones de exportación de EE.UU.

Hasta el 31 de diciembre de 1996, los productos criptográficos eran considerados como armas por la legislación de EE.UU. Como tales figuraban en la Lista de Municiones de EE.UU. ("U.S Munition List"). Una serie de leyes como la Ley de Control de Exportación de Armas, agrupadas bajo el nombre genérico de Regulaciones sobre Tráfico Internacional de Armas, ("International Traffic in Arms Regulations", ITAR) establece estrictas limitaciones a la exportación de productos "software" o desarrollos basados en algoritmos de cifrado.

En el caso concreto de productos basados en DES, la clave de 56 bits se ve acortada a 40 produciéndose una sensible reducción de la seguridad que ofrece este algoritmo. Esto además repercute en el grado de seguridad que ofrece cualquier producto que incorpore este algoritmo. Similares limitaciones se establecían para cualquier otro algoritmo.

En la fecha citada, el gobierno de los EE.UU. reconoció la naturaleza comercial de los productos criptográficos, transfiriendo la jurisdicción de la concesión de licencias de exportación del Departamento de Estado al Departamento de Comercio. Junto con esto se ofrece una relajación en las limitaciones a la exportación de productos basados en algoritmos simétricos. Todo ello dentro de la ofensiva del gobierno de EE UU. en favor de sistemas de custodia de claves. De este modo, las licencias eran concedidas si la empresa en cuestión aceptaba desarrollar sistemas de recuperación de claves y apoyar su uso.

En el caso del algoritmo RSA hay que remarcar que éste ha sido, desde la fecha de su publicación, el único sistema de criptografía de clave pública ampliamente aceptado. El principal inconveniente del sistema es la existencia de una patente sobre este algoritmo, que obliga a cualquiera que desee utilizarlo dentro de EE.UU. a pagar los correspondientes derechos a RSA Data Security, Inc. El tema de la exportación sigue el mismos camino que en el caso de algoritmos de clave simétrica. Teniendo como límite llaves de 512 bits.

3.13.2 La situación en el resto del mundo

Como ya hemos señalado, la criptografía ha sido y es vista por muchos gobiernos como una grave amenaza a la seguridad nacional. Ello ha llevado a un deseo de controlarla y restringirla.

Una de estas primeras iniciativas fue crear en 1949 el Comité de Coordinación Multilateral para Control de Exportaciones (CoCom). CoCom estuvo formado por los países de la OTAN excepto Islandia, España, Australia y Japón. La finalidad de este acuerdo era establecer una serie de restricciones que impidieran la transferencia de tecnología sofisticada, entre ella la tecnología criptográfica, a la URSS y a cualquier país de la órbita soviética.

Terminada la Guerra Fría, los países firmantes consideraron que era necesario reorganizar la situación, y tras varios años de negociaciones se llegó a la firma del Tratado de Wassenaar.

En este tratado, los países miembros establecen restricciones a la exportación de criptografía que pueda considerarse "material de doble uso", es decir, criptografía con uso tanto civil como militar, pero hay una gran variación de políticas. Algunos permiten la exportación bajo autorización, otros imponen restricciones al tipo de criptografía exportada... y otros países, como Francia, Rusia, Estados Unidos, Nueva Zelanda y Australia van más allá de los principios recogidos en el tratado e incluyen la criptografía de uso general (programas como por ejemplo, PGP) en las restricciones.

Para la mayoría de los cuerpos de seguridad de muchos Estados, la limitación del uso de la criptografía es necesaria para prevenir delitos en Internet. Según este punto de vista, entregar nuestras claves privadas a un tercero de confianza es una manera de evitar la gran amenaza que suponen los delitos informáticos, suponiendo sólo un insignificante riesgo de comprometer nuestra privacidad en las redes informáticas.

Sin embargo, este razonable argumento tiene varios fallos.

En primer lugar, el informe de octubre de 1997 de la Comisión Europea titulado "Towards A European Framework for Digital Signatures And Encryption", afirma que "la mayoría de los (pocos) delitos relacionados con el cifrado que son puestos como ejemplo de la necesidad de regulación de ésta tienen que ver con un uso "profesional" del cifrado. Parece poco probable que en tales casos el uso de cifrado pueda ser controlado con efectividad a través de la regulación".

En segundo lugar, el riesgo que supone un sistema obligatorio de almacenamiento centralizado de claves no es ni mucho menos insignificante. Inevitablemente, estos sistemas introducen vulnerabilidades en los protocolos criptográficos, dando oportunidades a abusos y ataques a la privacidad con fines delictivos. Los funcionarios del Gobierno encargados de almacenar las claves las guardarían en una sistema de archivo centralizado que sería un objetivo muy tentador para delincuentes. Y estos delincuentes potenciales no sólo serán "hackers" que intenten entrar desde el exterior, sino también funcionarios corruptos que podrían vender las claves privadas a criminales, o incluso utilizarlas ellos mismos en actividades delictivas. Más aún, los archivos centralizados de claves privadas son una gran tentación para agentes de los cuerpos de seguridad que quieran espiar determinadas comunicaciones sin una autorización judicial. Los sistemas obligatorios de almacenamiento centralizado de claves incitan a cometer varias clases de delitos, y es una tentación difícil de evitar una vez que las claves privadas están en manos de terceros.

En tercer lugar, una vez que existe este riesgo, surgen graves problemas para el comercio electrónico. Los usuarios no utilizarán sistemas comerciales en Internet tan masivamente como lo harían en otras circunstancias, debido al temor a que información confidencial (como el número de su tarjeta de crédito) puede terminar en manos de delincuentes.

En cuarto lugar, los criminales y los terroristas no van a ver impedidas sus actividades con una ley así. Desarrollar un "software" criptográfico no es tan difícil como parece. De hecho, existen centenares de programas que pueden descargarse en Internet. Los delincuentes podrían fácilmente conseguir ilegalmente esta clase de "software", de la misma manera que obtienen ilegalmente armas o drogas, y usarlo sin entregar su clave privada a ningún organismo público. Sólo los ciudadanos corrientes entregarían sus claves privadas, poniendo así en peligro su privacidad, mientras que terroristas y criminales podrían utilizar criptografía sin ningún problema. Más aún, ocultando sus mensajes en otros mensajes sin ninguna información sobre hechos delictivos, o en archivos de imágenes (la técnica conocida como esteganografía), los delincuentes podrían evitar que se detectara su uso ilegal de criptografía.

Asimismo, por lo observado recientemente en Estados Unidos y el Reino Unido, ninguna empresa está de acuerdo con los sistemas de almacenamiento centralizado de claves. Consideran que es una gran amenaza al comercio electrónico y quieren que el gobierno americano retire sus borradores de leyes de almacenamiento de claves.

Concluyendo, se puede afirmar que la tecnología criptográfica fuerte sin sistemas obligatorios de almacenamiento centralizado de claves es la única protección para aquellos que quieran defender su privacidad en Internet. También es el único método eficiente para crear un sistema de comercio electrónico que sea realmente seguro y en el que se pueda confiar.

4 Modelo del Sistema para Comercio Electrónico

En este capítulo se definirá un modelo por medio del cual se ejemplifique un ambiente de comercio electrónico con todas las características y circunstancias por las cuales requiere la protección de su información; así como los análisis y consideraciones necesarios para determinar y diseñar las soluciones correctas.

4.1 El negocio a desarrollar

Proponemos un negocio enfocado a vender música digitalizada a través de Internet. Durante el resto del modelo lo llamaremos "Tienda Virtual". Su mercado es toda persona con acceso a Internet, una cuenta de banco y posea una o más computadoras; cada una de estas personas será llamado "Cliente o Usuario Final". Como ejemplificación de dicho mercado, tenemos la ciber-comunidad de usuarios de "Napster".

Este negocio deberá entablar relaciones con las diferentes casas musicales, genéricamente nombradas como "Casa Musical", las cuales le proveerán de la mercancía a vender: canciones en formato digital. Y también deberá establecer contacto con los bancos, para poder realizar las operaciones financieras consecuentes a la compra-venta de canciones con los usuarios finales.

Por su giro, venta de música digitalizada, la Tienda Virtual puede tener una naturaleza dual en cuanto al producto comercializado:

1. Es un comercio electrónico directo, al vender sus canciones (mercancía) totalmente en formato bit. Es decir, que el usuario final selecciona, compra y descarga las canciones, todo por medio de Internet.
2. Es un comercio electrónico indirecto, si utiliza la información para comerciar las canciones en formato físico (átomos). Lo cual significa que el usuario seleccionará y pagará sus canciones a través de Internet, y el negocio se encargará de:
   a) vender él o los CD-ROMs como álbumes comerciales completos provistos por las diferentes casas musicales (siguiendo el ejemplo de Amazon.com)
   b) quemar uno o varios CD-ROMs con sus canciones seleccionadas (de diferentes cantantes y casas musicales),

   para después enviarle a su domicilio vía un servicio de mensajería o paquetería.

Aunque los dos tipos de comercio son factibles y viables de manejar en el ciber-negocio, nos enfocaremos a la venta de mercancía en formato bit ya que ésta puede ser transmitida al comprador por una red de datos (en este caso: Internet); mientras que en formato átomo saldría del alcance de la presente tesis debido al hecho de ser transportada por redes de transporte de bienes materiales.

Si analizamos la operación de la Tienda Virtual, observamos la necesidad de realizar operaciones financieras en línea y en tiempo real; pues deben cobrarse las canciones vendidas. Por lo cual requiere establecer mínimo un contacto con un banco. En el presente modelo se considerará que sólo es necesario establecer relación con un banco, al cual llamaremos "Banco", en el cual la Tienda Virtual se da de alta como cuentahabiente empresarial. Supondremos que a dicho Banco se pueden canalizar todas las transacciones consecuentes de la venta de canciones, y será este quien verifique las autorización correspondientes y haga las transferencias entre los diferentes bancos. Además, se considerará que la comunicación entre bancos se realiza en un ambiente seguro y cerrado (líneas dedicadas, sistemas propietarios, EDI)

4.2 Motivación del negocio

La razón de enfocarnos a la venta de música se justifica por las siguientes razones:

- *El actual desarrollo y despliegue tecnológico,* han creado diversos factores:

    1. información en formato digital, en formato normalizado, y sus respectivas ventajas;
    2. equipos de computo con interfaces para uso popular (ambientes gráficos) y capacidad suficiente para realizar muchas y muy diversas actividades (MS-Windows y Linux);
    3. proliferación del uso de la tecnología, empezando a iniciar un ascenso para alcanzar el nivel de "popular";
    4. redes de comunicación omnipresentes, que permiten conectar una gran diversidad de equipos y permiten la comunicación de sus usuarios por todo el planeta.

    Los cuales permiten el surgimiento de una interesante frontera: si la información digital almacenada en átomos (cd-rom, disquetes, etc.) solo permite una piratería comercial de alcance local (requiriendo elevada inversión, limitada por su localización geográfica y número de contenedores átomos disponibles); almacenada en un medio electrónico y transmitida por una red pública como lo es Internet (una simple PC con su módem y cuenta a un ISP), es totalmente vulnerable ante delitos que antes no eran posibles en contra de los bienes y servicios de una persona, así como la existencia de una piratería de alcance mundial (baja inversión, sin limitaciones físicas o de número de copias o mercado).

- *El caso "Napster".* En el cual se utilizó el Internet para transportar cualquier canción en formato digital, por todo el mundo y sin limitaciones; hizo factible otra vez el beneficio de que la tecnología permitiera un consumo masivo de un bien a nivel mundial y con pocas restricciones de tiempo. Como primeros casos tenemos la radio y la televisión, pero a diferencia de ellos, Napster creo el ambiente en èl cual los consumidores no pagan remuneración alguna a los creadores de la música (recordemos que en la radio y la televisión, los consumidores pagan los gastos de transmisión al comprar los productos y servicios anunciados)

- *Las actuales velocidades de transferencia de las conexiones a Internet provistas para domicilios nacionales*: de 1kbps-4kbps (velocidades mínimas provistas a los usuarios cuando el "ISP" tiene tráfico máximo) hasta 42 kbps cuando el usuario que entra a la hora de más bajo tráfico con el ISP de mejor calidad de servicio. También es importante considerar que el cibernauta mexicano que se conecta por línea telefónica, en promedio permanece 1 hora diaria navegando.

    La variable "velocidad de transferencia" es de gran importancia al evaluar cualquier negocio electrónico desde la perspectiva del cliente. A continuación se verán los casos típicos extremos que ejemplifican este concepto.

    Supongamos que un usuario entra a Internet a una hora pico o de tráfico máximo, su "ISP" esta diseñado para darle en dicha situación una velocidad mínima de 4 kbps, y dicho cibernauta desea descargar un video musical de 3 minutos y 40 segundos digitalizado en mpeg (41,133 kBytes); el tiempo que debe esperar para poder disfrutar la canción es el tiempo de transferencia:

$$\text{Tiempo de Transferencia} = \frac{41{,}133 \text{ kBytes}}{4 \text{ kbps}} = \frac{329{,}064 \text{ kbits}}{4 \text{ kbps}} = 82{,}266 \text{ segundos} = 23 \text{ horas}$$

    El cálculo anterior nos hace ver que se hace un poco menos que imposible que alguien desee comprar un video y esperar 23 horas en bajarlo (viendo la tabla 4 1, el tiempo de transferencia

puede variar de algunas horas hasta varios días). Empeorando la situación el hecho de que algunos ISP's cortan el enlace después de 1 hora o 2 horas de estar conectados (referencias a casos Telmex y Tutopía).

Ahora evaluemos al mismo usuario en la misma situación (hora de máximo tráfico, misma velocidad de transferencia) cuando descarga una canción de 3 minutos 20 segundos digitalizada en MP3 (3140 kBytes):

$$\text{Tiempo de Transferencia} = \frac{3{,}140 \text{ kBytes}}{4 \text{ kbps}} = \frac{25{,}120 \text{ kbits}}{4 \text{ kbps}} = 6{,}280 \text{ segundos} = 1 \text{ hora } 44 \text{ minutos}$$

Se ve una espera mucho más razonable para el cliente, próxima a su tiempo de conexión diaria, y que da el sustento de factibilidad para que la venta de canciones por Internes sea un negocio rentable.

La siguiente tabla muestra los valores extremos que se pueden presentar en el lado del cliente.

Tipo de Información	*Tamaño promedio (1 Byte = 8 bits)*	*Tiempo de transferencia máximo a tráfico máximo (1 kbps)*	*Tiempo de transferencia mínimo a tráfico máximo (4 kbps)*	*Tiempo de transferencia mínimo a tráfico mínimo (42 kbps)*
Página Web (con algunas imágenes pequeñas y un sonido de fondo)	60 kBytes	480 segundos = 8 minutos	120 segundos = 2 minutos	11.4 segundos
Canción digitalizada	4 min = de 40 kBytes a 4 Mbytes según el tipo de formato utilizado	320-32,768 segundos = 5.33-546.13 minutos	80-8192 segundos = 1.33-136.53 minutos	7.6-780.2 segundos
Video musical digitalizado	4 min = 40 Mbytes, aunque también varía según el tipo de formato utilizado	327,680 segundos = 5461 minutos = 91 horas	81,920 segundos = 1365 minutos = 22.75 horas	7801 segundos = 130 minutos =2 horas y 10 min

Tabla 4-1 Comparación de tiempos de transferencia

Para la criptología, aquí esta la puerta a un mercado mucho más extendido al ocultamiento de los secretos gubernamentales ultra-confidenciales; se convierte en una herramienta más popular al ciudadano, al permitir.

1 la protección de bienes de uso y/o consumo común (dinero, música, videos, documentos, informes, planos); y
2 la protección de las relaciones personales y/o empresariales factibles y/o motivadas por la existencia del ciberespacio.

Y en este caso particular, se crea un negocio con un producto menos "pirateable".

4.3 Modos de Operación entre la Tienda Virtual y la Casa Musical

Es importante analizar como se establecerá la relación entre la Tienda Virtual y las Casas Musicales. Por los diferentes procesos que se pueden realizar entre ambos entes, se visualizan los siguientes modos de interacción:

4.3.1 Modelo B2B & B2C

En este caso, el Usuario Final decide comprar una canción, hace su solicitud y la Tienda Virtual envía la misma solicitud a la Casa Musical dueña de la canción seleccionada; ésta valida la venta, lee la canción de su bases de datos, crea la canción personalizándola a las características del Usuario Final y la envía a la Tienda Virtual. Al mismo tiempo, actualiza un cargo en sus bases de datos para que finalizado un período o alcanzado un monto acordado, la Tienda Virtual deberá liquidar su adeudo con dicha firma.

Para la Tienda Virtual este escenario ofrece la ventaja de requerir moderados recursos en el almacenaje, soporte y distribución de la mercancía (pues solo debe manejar catálogos actualizados de las diferentes Casas Musicales), no debe comprar las canciones permanentemente (lo cual implicaría pagar por ellas un gran costo), ya que toda la responsabilidad del manejo de la mercancía y su protección recae en cada Casa Musical.

El riesgo para la Tienda Virtual es el hecho de que solo actúa como un revendedor con poco o nulo valor agregado, lo cual implicaría que puede ser eliminado del la cadena productor-vendedor-consumidor pues cada Casa Musical puede establecer un sitio que hiciera la misma operación y tal vez ofrecer el producto a menor costo.

El riesgo para la Casa Musical es el posible fraude de que la Tienda Virtual aparente vender solo una canción (a precio de usuario final), y de ahí la utilice para revenderla un sinnúmero de veces.

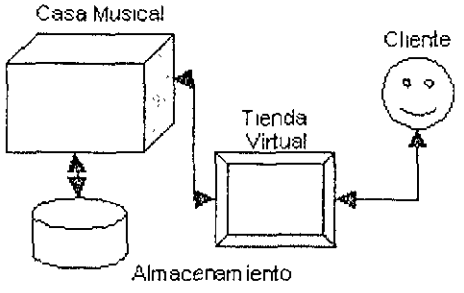


Figura 4-1 Modelo B2B & B2C

4.3.2 Modelo Paquete & B2C

En este segundo caso, la Casa Musical y la Tienda Virtual acuerdan que la primera cede los derechos de un cierto paquete de canciones a cambio de una tarifa establecida entre ambas partes. En este caso, la responsabilidad de salvaguardar la integridad y seguridad del material discográfico es de la Tienda Virtual.

Las desventajas para la Tienda Virtual.

1. el hecho de poseer canciones que tal vez nunca le convengan por ser compradas en paquete (siendo muy probable que dichos paquetes sean armados a criterio de la Casa Musical), y
2. el hecho de poseerlas permanentemente es razón por la cual cada Casa Musical las venderá a un precio elevado (considerando la popularidad del cantante y de la canción en el momento de la venta).

Por consecuencia, la Tienda Virtual requerirá un capital considerable para poder invertirlo en tener un inventario propio aceptable; y no toda canción garantiza el retorno de la inversión.

La oportunidad o ventaja es la libertad de efectuar las ventas como mejor le convenga (subir o bajar precios, crear promociones u ofertas, etcétera); y si la canción y/o el cantante aumentan su popularidad, aumentarán más sus ventas.

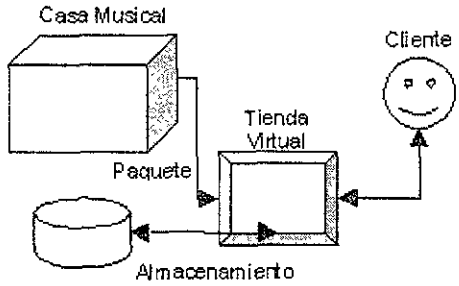


Figura 4-2. Modelo Paquete & B2C

4.3.3 Modelo Regalía & B2C

La operación de este modelo se basa en que cada Casa Musical entrega sus canciones a la Tienda Virtual; y después de un lapso de tiempo o alcanzada una determinada cifra de ventas, la segunda pague las regalías correspondientes a cada firma musical.

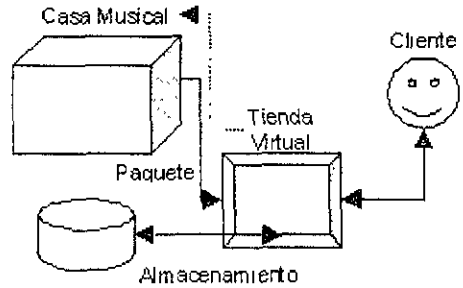


Figura 4-3. Modelo Regalía & B2C

La ventaja para la Tienda Virtual es que no debe invertir gran cantidad de capital, pues en principio no debe invertir en mercancía. Pero la gran disyuntiva para establecer este escenario es el hecho de que se debe plantear todo un sistema de seguridad para asegurar de que la Tienda Virtual pague lo que en verdad vende, a cada Casa Musical; es decir, que deben existir las herramientas para que no pueda negar lo que esta facturando. Esto se puede acentuar por el inconveniente de que de antemano se establece un ambiente de desconfianza de la Casa Musical a la Tienda Virtual. Aunque el diseño del esquema de seguridad necesario para establecer este escenario es posible, el análisis y diseño de las herramientas correspondientes motivan a desarrollar una tesis únicamente enfocada a este problema.

4.3.4 Modelo General

Este es un modelo combinado La idea básica es que la Tienda Virtual compra permanentemente las canciones más populares (según encuestas de radio, TV, revistas) pero maneja los catálogos completos de todas las canciones que tiene cada Casa Musical Cuando el Usuario Final solicita

alguna que no se encuentra en su inventario, la Tienda Virtual se encarga de gestionar la compra de dicha canción directamente con la Casa Musical correspondiente, descargarla y luego generar la canción a vender al Usuario Final.

Este escenario plantea la desventaja para la Tienda Virtual de requerir un capital moderado para adquirir sus canciones más populares, pero con las ventajas del segundo escenario analizado anteriormente. Y para la Casa Musical establece la ventaja de que no debe preocuparse de algún posible fraude como en el primer y tercer escenarios.

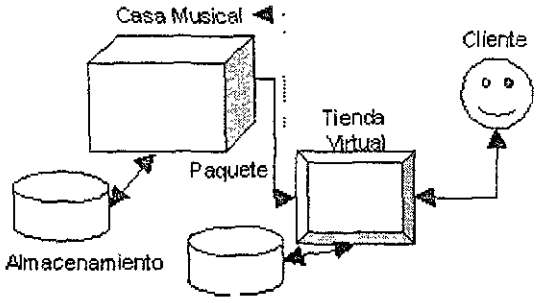


Figura 4-4. Modelo General

Existen muchas otras variaciones respecto al mecanismo de venta, sin embargo, todos ellas pueden ser englobadas dentro de alguna de estas categorías.

4.4 Sistema Modelado

Para la presente tesis se utilizará el Modelo General, a fin de manejar tanto el modo B2B como el B2C. Este escenario puede superar a un sitio de venta propiedad de la Casa Musical al manejar los productos de diferentes Casas Musicales y tener la capacidad de crear CD-ROMs personalizados (anteriormente descrito con más detalle en la sección 4.1"El negocio a desarrollar").

4.4.1 Entes y sus Roles

A continuación se presenta a los principales entes activos (crean, transmiten, reciben, procesan y almacenan información) dentro de este modelo.

Figura 4-5. Representación de los entres participantes en el sistema modelado

4.4.2 Cliente o Usuario Final

El Cliente Final es el usuario principal de la música digitalizada (bien final): la compra, la transfiere, la almacena y la procesa (escucha). Para obtenerla establece diferentes relaciones con los otros entes del modelo, a través de los diferentes servicios de los cuales es usuario:

- Con el Banco: se registra, deposita fondos, permite la transferencia de dinero de sus cuentas a las de otros, puede bloquear su cuenta y pedir historial de actividades.
- Con la Tienda Virtual: se registra, selecciona, compra y transfiere canciones digitalizadas; descarga el CryptoPlayer y facturas digitales; y pide historial de actividades.

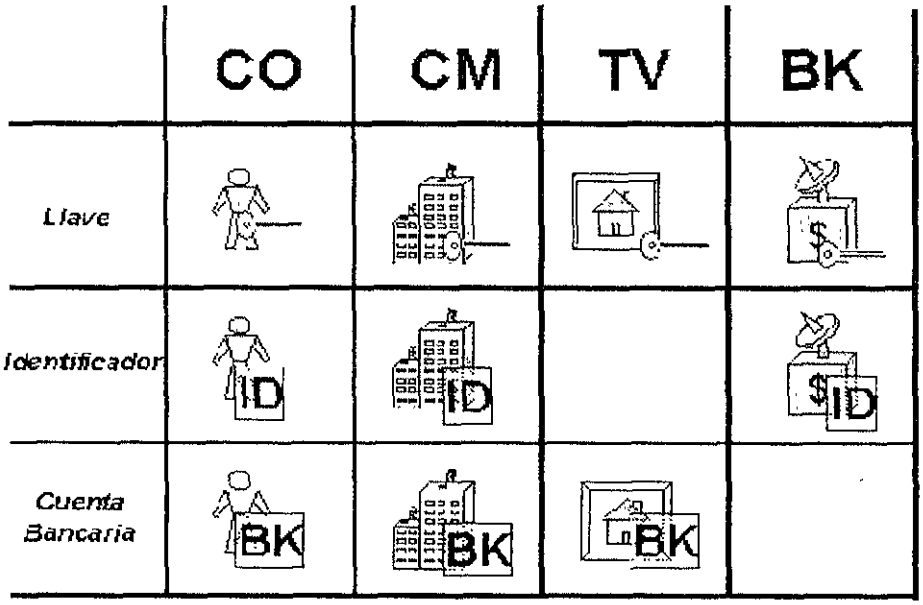


Figura 4-6 Representación de las características de cada ente

4.4.3 Banco

El Banco es el ente que maneja y resguarda el dinero de todos los demás entes en el modelo Las transacciones entre diferentes bancos se hacen en un medio bancario seguro (sistemas cerrados, líneas privadas, etcétera).

Los entes "Cliente Final", "Tienda Virtual" y "Casa Musical" son usuarios de sus servicios:

- Registro de usuario. Esto implica darle un número de cuenta, número de tarjeta y claves para realizar operaciones de banca electrónica y actividades comerciales por Internet.
- Realización de transferencias entre cuentas: Verificar las autorizaciones de transferencia, de compra y de saldo necesarias; para realizar los retiro, abonos y registro de actividades correspondientes.
- Proveer historial de actividades a cada usuario: Dar a cada usuario el registro actual de transacciones realizadas en su cuenta.

4.4.4 Casa Musical

La Casa Musical es el ente que crea la música, pero no la vende directamente al Cliente Final. Por ello necesita establecer relaciones con otros entes:

1. Con el Banco: Para darse de alta y tener una cuenta con la cual pueda realizar transacciones.
2. Con la Tienda Virtual. a quien le vende la canción, por paquete o individual.

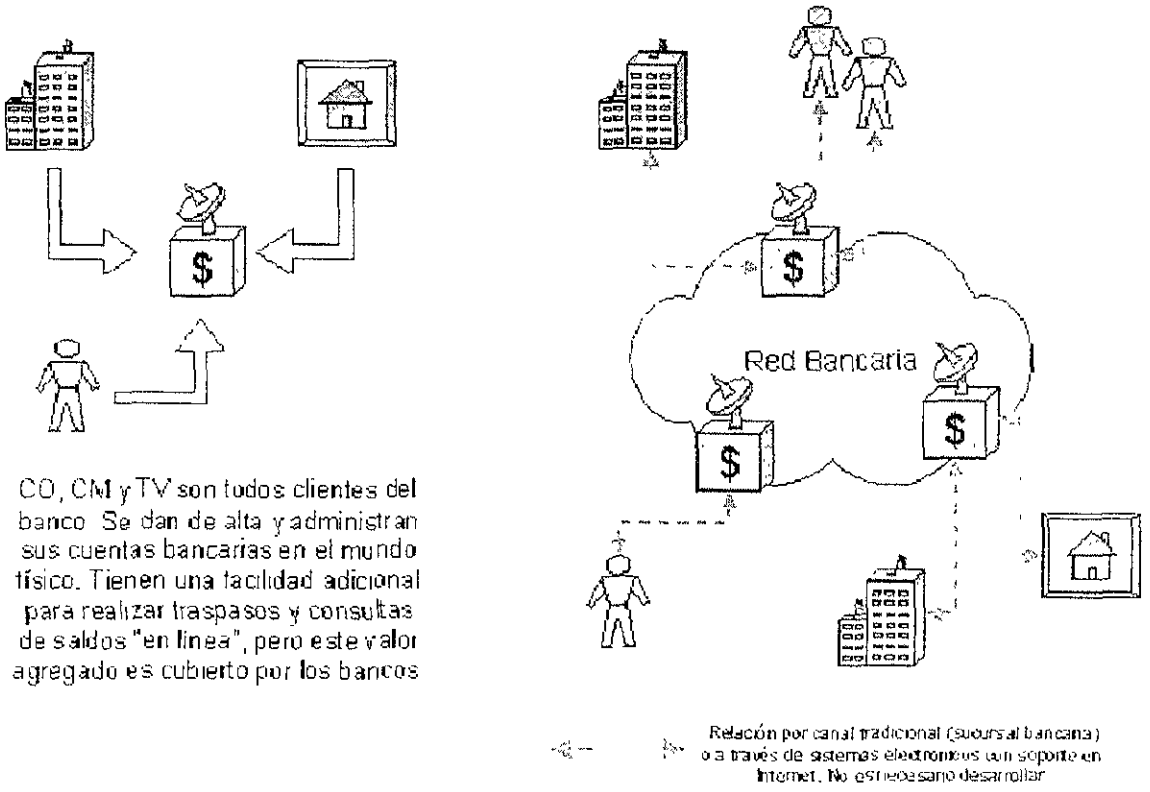


Figura 4-7 Relacion básica entre entes

4.4.5 Tienda Virtual

La Tienda Virtual vende las canciones a cada Cliente Final, personalizándolas de manera que únicamente el Cliente Final que la compro pueda tocar la canción. Establece relaciones:

1. Con el Banco: Se da de alta para tener una cuenta con la cual pueda realizar transacciones.
2. Con la Casa Musical: Quien será su proveedor del material a vender
3. Con el Cliente Final: A quien le venderá el producto.

Como se puede ver en la figura, cuando un comprador ha decido adquirir una canción, y su tarjeta ha sido validada, la tienda virtual se encarga de determinar si la canción vendida se encuentra dentro de su base de datos o si se deberá comunicar con el sistema de almacenamiento de la casa musical. En cualquiera de ambos casos, le dará instrucciones al CryptoMusicMaker para que tome la canción vendida, tome también la llave de almacenamiento, descifre la canción y la vuelva a cifrar con la llave personalizada para el usuario.

Posteriormente, con su llave personalizada y su canción almacenada en el disco duro local, el usuario deberá correr la aplicación CryptoPlayer, la cual se encargará de verificar la identidad del usuario, reproducir la canción y evitar la creación de copias ilegales.

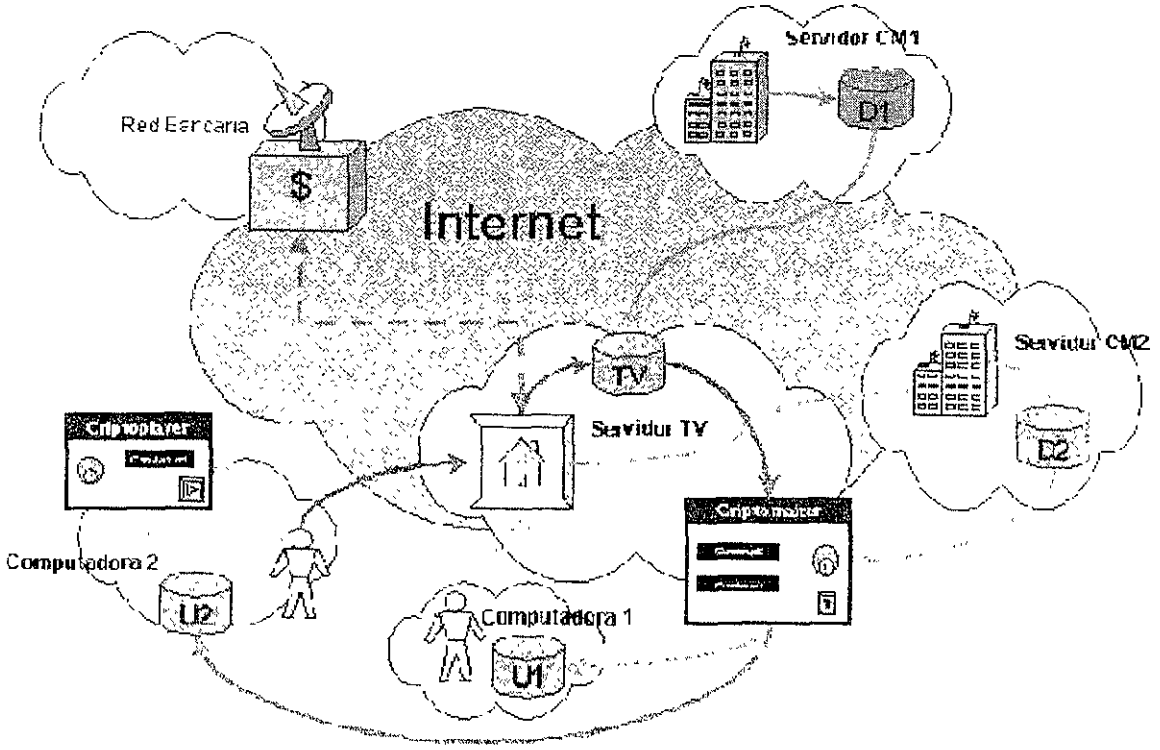


Figura 4-8 Mapa relacional de todo el sistema modelado

4.5 ¿Que se debe proteger?

Con la vista general anterior y lo expuesto en la sección "¿qué se debe proteger en el comercio electrónico?" del capítulo "Comercio Electrónico" de la presente tesis; podemos establecer rápidamente que es lo más importante a proteger en este modelo: el dinero y la música digitalizada.

4.5.1 Dinero

Necesidades de protección:

1. Se le debe proteger porque es un producto intermedio al permitir la compra de otros bienes y servicios. Su protección es indispensable por sus enormes capacidades de ser usado varias veces y de satisfacer deseos humanos. Y es el único bien que se intercambia entre todas las personas físicas y morales de este modelo: Tienda Virtual, Casa Musical, Banco y Usuario Final.
2. Aunque en esta tesis no se propone manejar efectivo digital (un posible substituto al actual efectivo en papel moneda); sí se manejan los bienes informáticos de los actuales sistemas de venta electrónica: los números de tarjetas bancarias (de crédito o débito). Por lo cual se deben proteger dichos bienes intermedios (nos conducen a otro bien que es el dinero) en formato bit (información capaz de ser transmitida en forma electrónica) ya que nos permitirán manejar el dinero en Internet. Estos son:
    a) el número de cuenta bancaria;
    b) el número de la tarjeta asociada a dicha cuenta (tipo débito, crédito, internacional, etc); y
    c) la autorización electrónica relacionada a una transacción (actualmente su uso es poco frecuente en el B2C, aunque más en el B2B).

En la actualidad, existen varias compañías que aceptan o sólo permiten la transferencia de números de tarjetas en "texto en claro". Al paso que aumenta la población de Internet-WWW y se realizan más operaciones comerciales, se está incrementando la resistencia de los usuarios a enviar información sensible (como los datos antes mencionados) sin protección alguna, por las siguientes razones:

1. Riesgos para el comprador individual del B2C (situación no tan alarmante en el B2B, porque en él se utilizan autorizaciones) a que sus números, y consecuentemente su dinero, sean utilizados por extraños con criminales intenciones.
2. Riesgos para los bancos, debido a que deben validar operaciones que en muchos casos pudieran ser realizadas por criminales, con sus consecuencias legales.
3. Riesgos para el vendedor, ya que podría ser incriminado en actos ilegales

Ante esta situación, ¿cómo podemos enviar información sensible, en forma segura, por Internet? Por medio de la criptografía. Las nuevas técnicas y herramientas criptográficas poco a poco se están popularizando, razón por la cual los costos asociados han ido bajando (costos de certificados, llaves, tarjetas inteligentes, etcétera)

Aunque dicha popularización todavía no ha generado la suficiente infraestructura y normalización para manejar efectivo digital o tarjetas digitales, en especial por la enorme dependencia a empresas terceras particulares (ejemplos: DigiCash o CyberCash [5, 189-211] [26]).

4.5.2 Música

Necesidades de protección:

1. Al igual que el dinero, la música digitalizada puede ser utilizada varias veces y satisface el deseo humano de escuchar algo agradable (aunque en gustos se rompen géneros). A este bien se le debe proteger por sus 2 naturalezas:
   a) Es un bien intermedio, ya que al vender la música digitalizada se puede obtener dinero. Y si se revende ilegalmente (piratería), el beneficiario es distinto a los creadores y/o inversionistas del bien original.
   b) Es un bien final, por su consumo público. Lo cual significa que puede ser utilizada por cualquier persona con una computadora multimedia o reproductor musical adecuado; es decir, un mercado potencial de millones de consumidores distribuidos por todo el orbe.
2. Los hechos anteriores obligan a que la información (música) debe protegerse: en primer plano por sí misma; y en segundo plano, al proteger aquellos entes con quienes tiene alguna relación durante su ciclo de vida (a grandes rasgos: creación, almacenamiento, transporte y reproducción).

Por sí misma nos referimos a que debe tener una protección en su estructura por la cual pueda evitar ser "pirateada" por cualquier persona, y por ello nos apoyamos de la criptografía, con el objetivo de particularizar cada canción a las características de cada comprador. Si recurriéramos a que cada Tienda Virtual sólo usará una codificación propietaria diferente al WAV, MIDI, MP3 (concepto de "oscuridad" como lo declara Schneier y distinto a la protección criptográfica); caeríamos en el problema de que analizando dicha codificación (tarea para los interesados en el procesamiento digital de señales) se obtendría la canción; o peor: una herramienta "traductora de códigos" que se difundiría rápidamente por la ciber-comunidad (un clásico ejemplo son los "traductores" de formato WAV a MP3, popularizados por el auge de "Napster").

4.6 Análisis y diseño del sistema seguro

Para una idea de las necesidades de seguridad de un sistema informático, se recomienda leer [5]. La metodología utilizada para el análisis del sistema se puede consultar en [27]; mientras que las nociones importantes para el diseño del mismo se obtuvieron de [28], [29], [30] y [31].

En esta sección mostramos la forma de analizar el modelo a fin de lograr un sistema seguro. Para ello bosquejamos brevemente la metodología usada por fases.

A. Identificación de los entes activos participantes (descritos con anterioridad).
B. Identificación de los bienes a proteger
C. Definición de todo el ciclo de vida del bien a proteger.
D Definición y establecimiento de relaciones de cada uno de los entes y componentes participantes en cada una de las fases del ciclo de vida del bien a proteger.
E. Definición del panorama de ataques y defensas. El cual consiste en:
   - Determinación de los posibles ataques a cada uno de los entes y componentes participantes en cada fase; de acuerdo a las siguientes áreas que permiten un "ataque exitoso":
     1 Acceso por confianza o físico.
     2 La capacidad de diagnosticar el ataque.
     3. Realización del ataque.
   - Determinación de las defensas necesarias para evitar, detectar y detener dichos ataques.

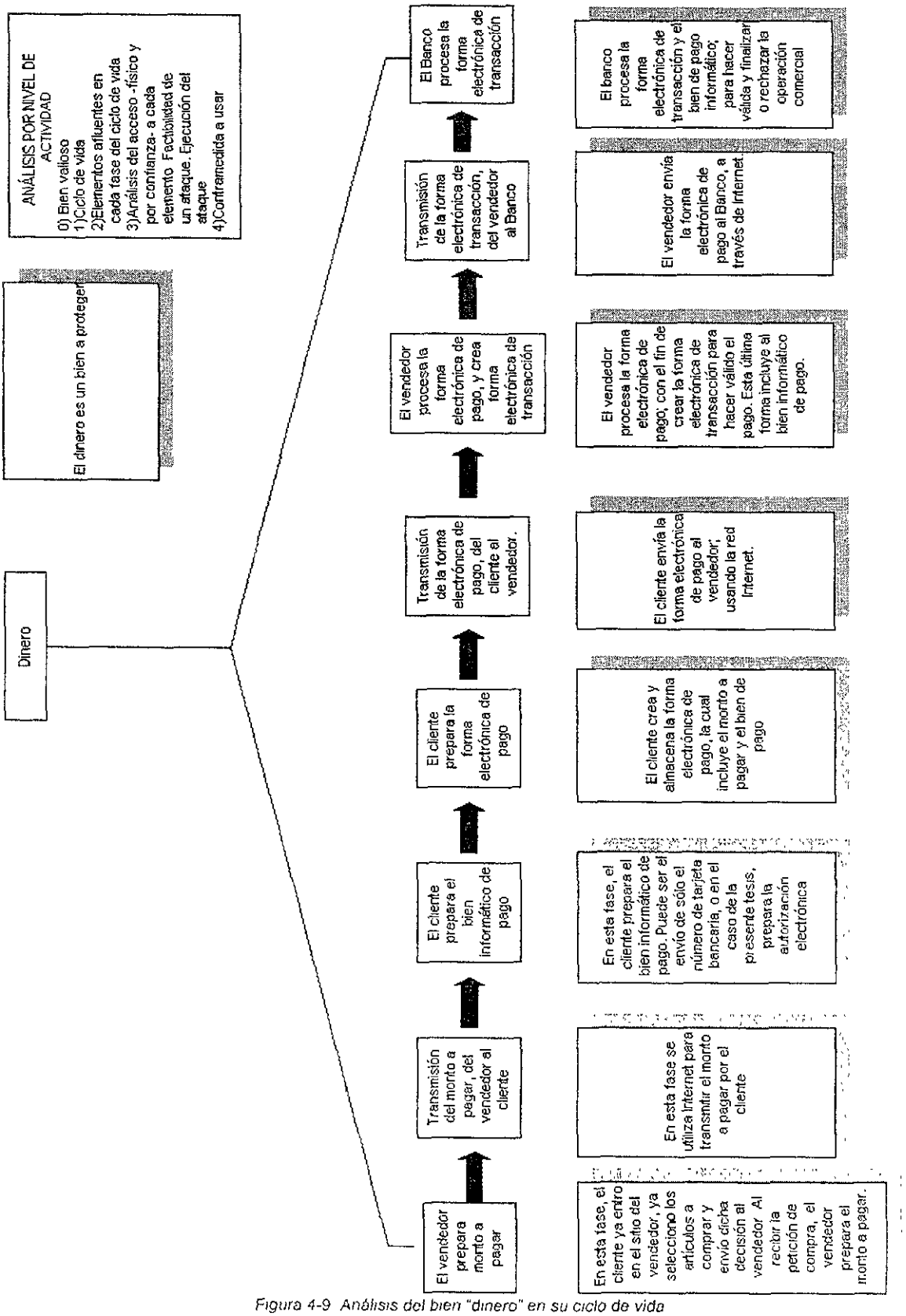


Figura 4-9 Análisis del bien "dinero" en su ciclo de vida

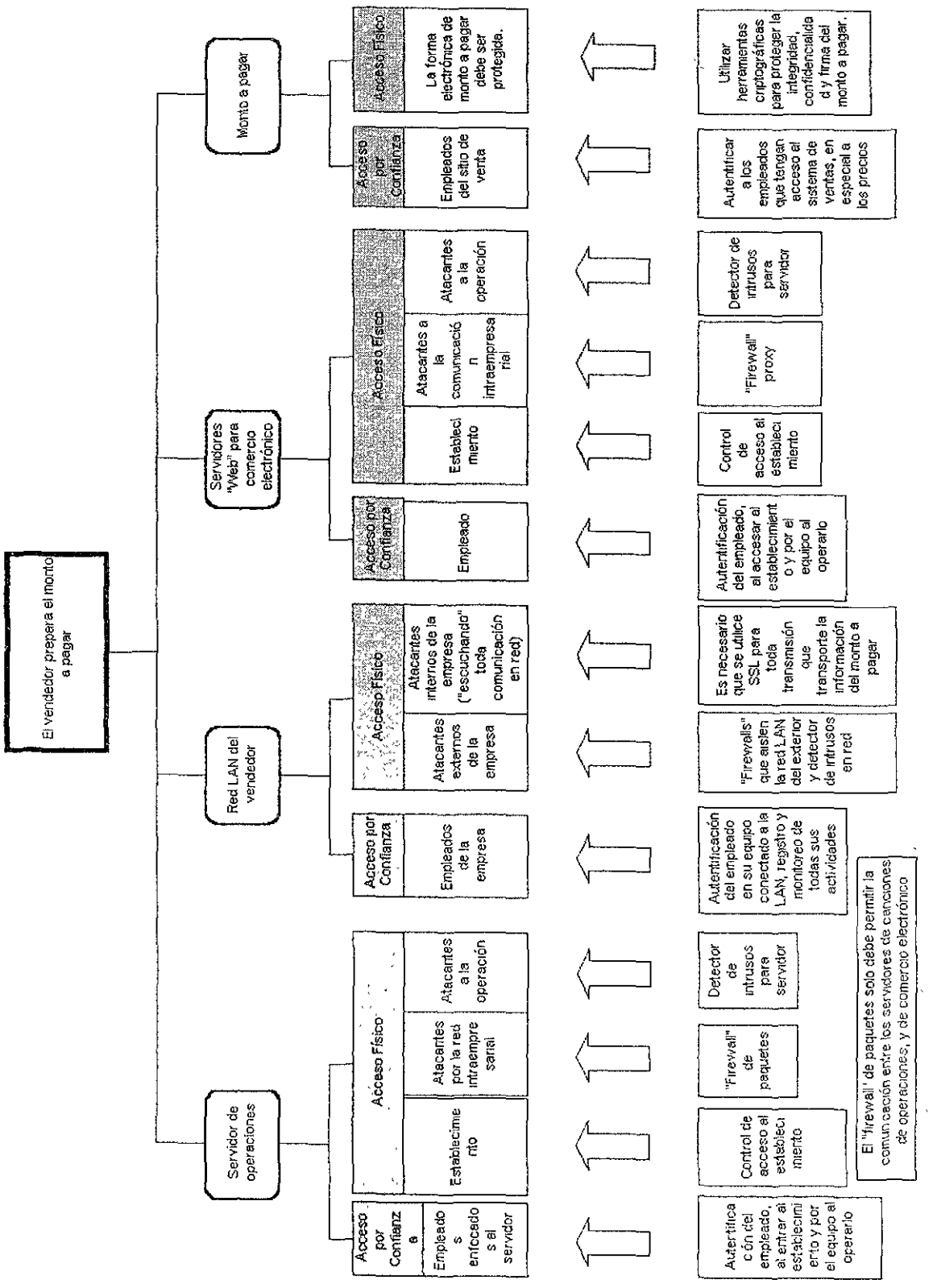


Figura 4-10 Primer panorama de ataques y defensas del bien "dinero"

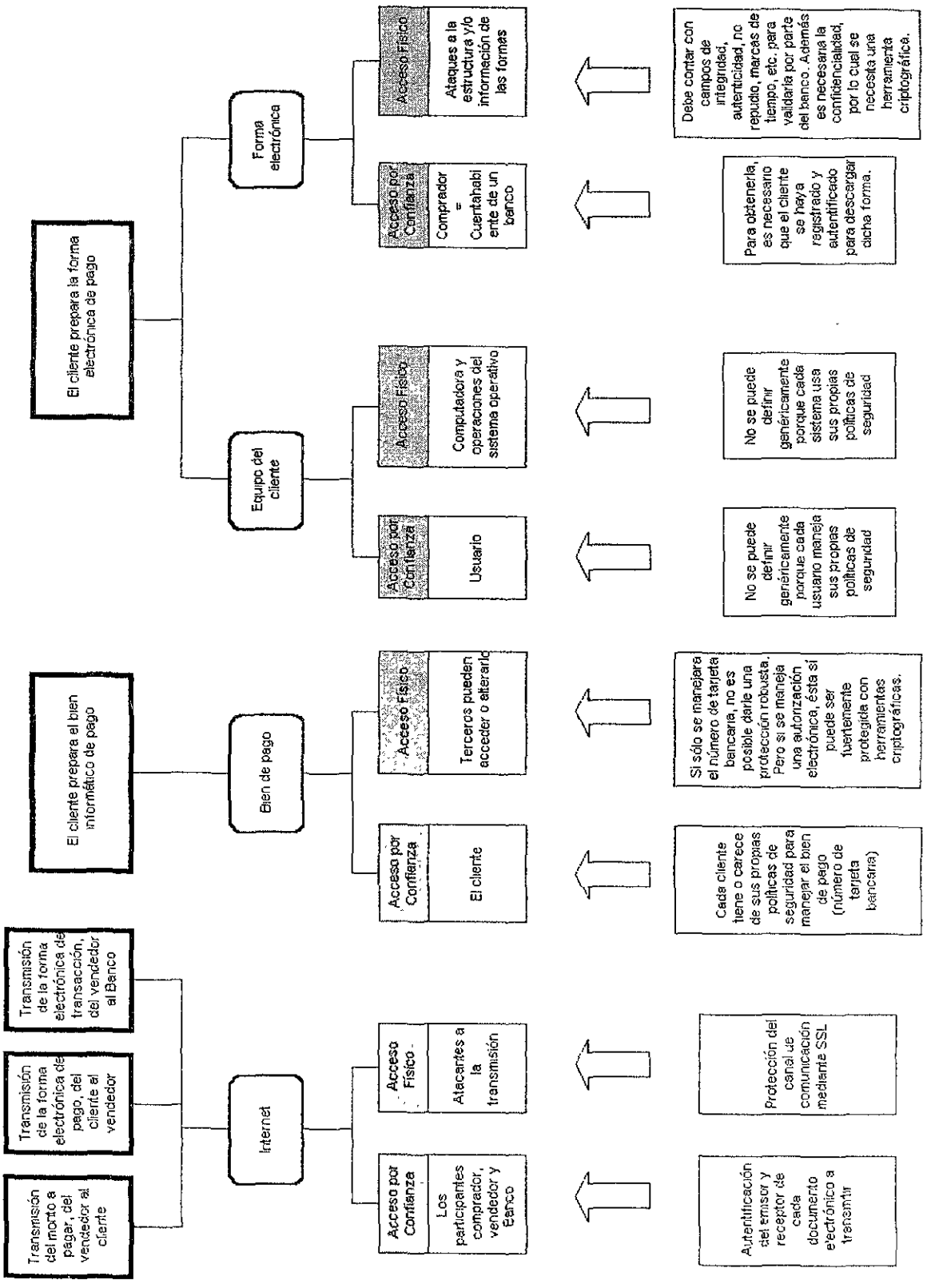


Figura 4-11 Segundo panorama de ataques y defensas del bien "dinero"

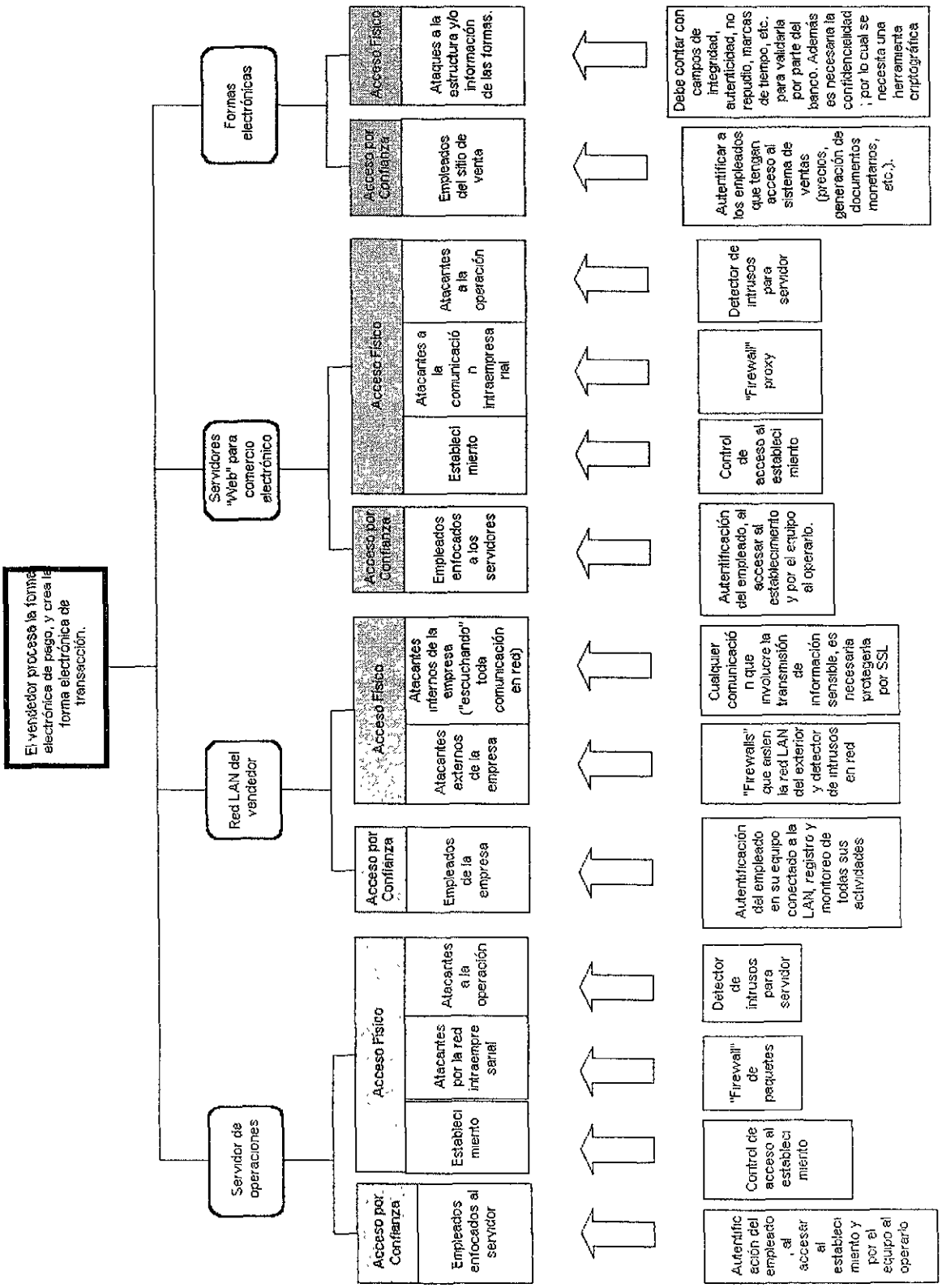


Figura 4-12. Tercer panorama de ataques y defensas del bien "dinero"

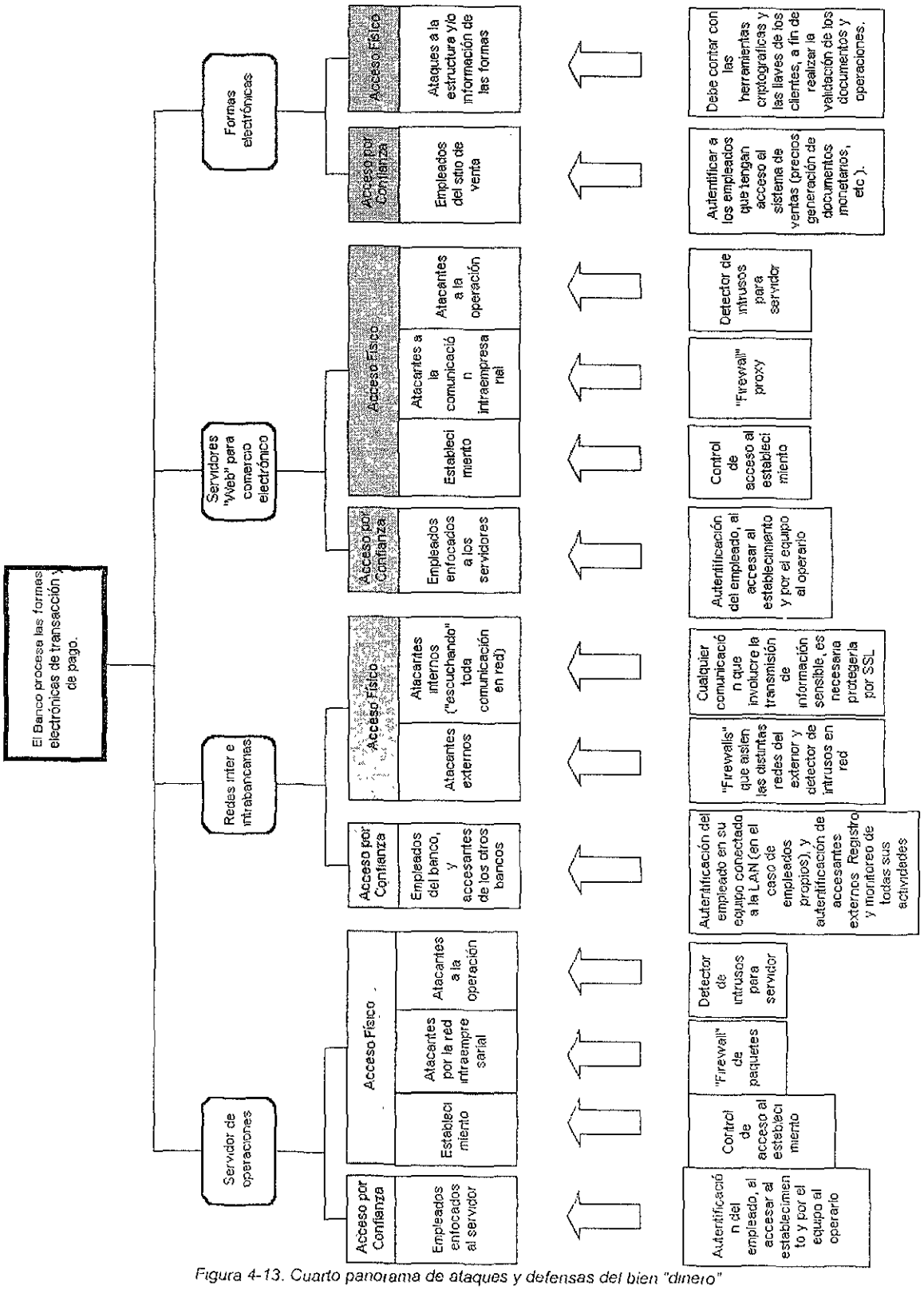


Figura 4-13. Cuarto panorama de ataques y defensas del bien "dinero"

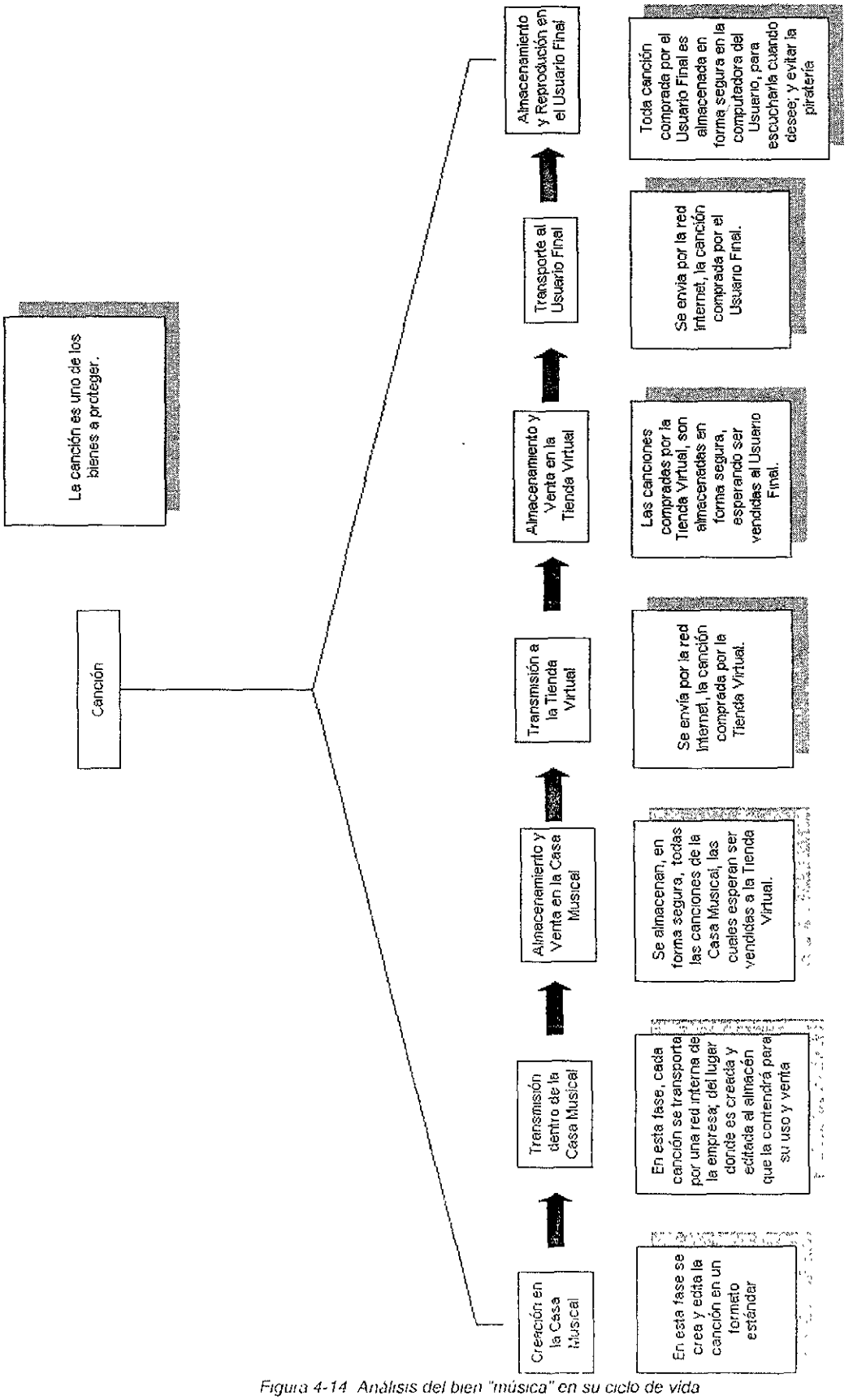


Figura 4-14 Análisis del bien "música" en su ciclo de vida

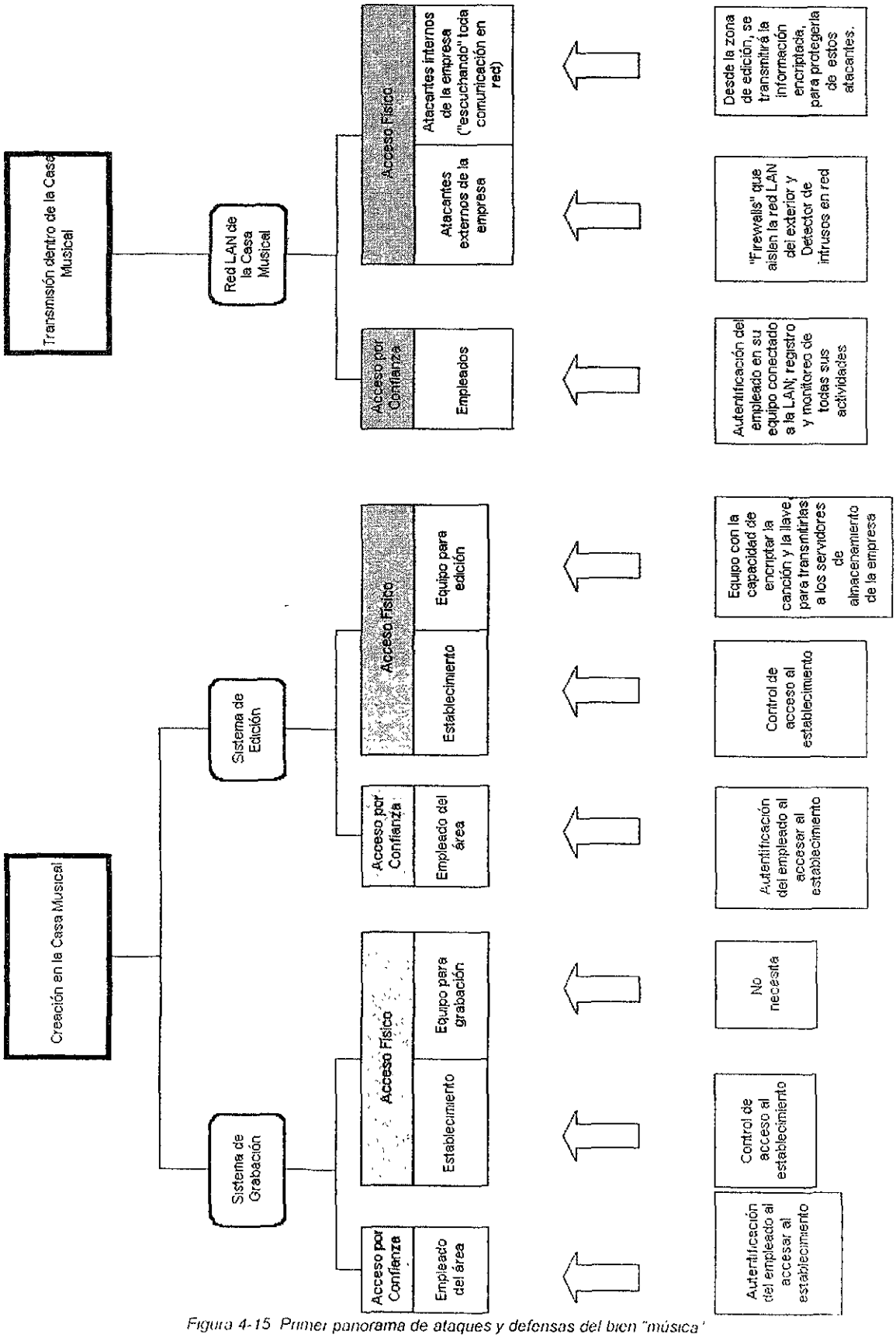


Figura 4-15 Primer panorama de ataques y defensas del bien "música"

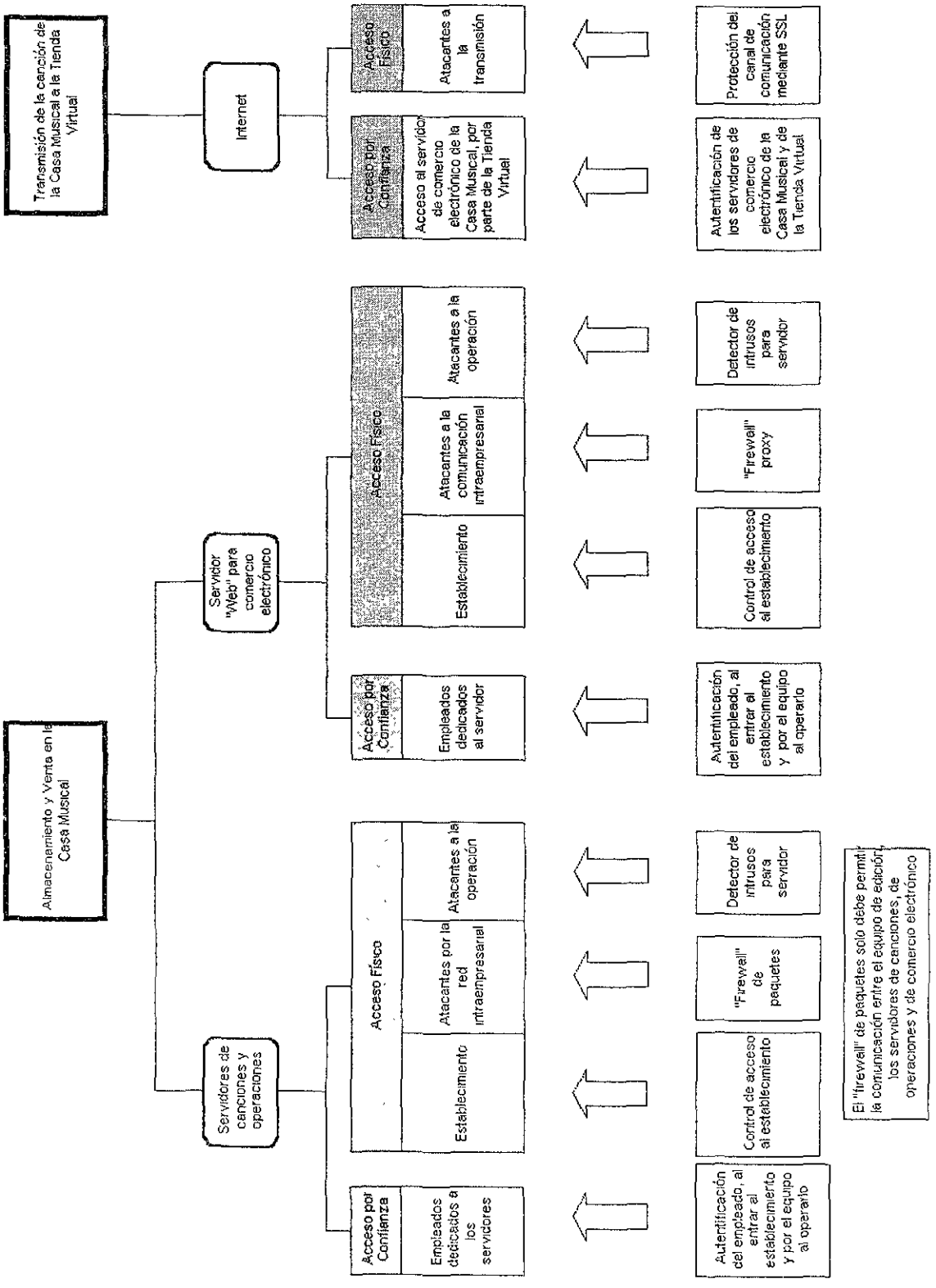


Figura 4-16 Segundo panorama de ataques y defensas del bien "música"

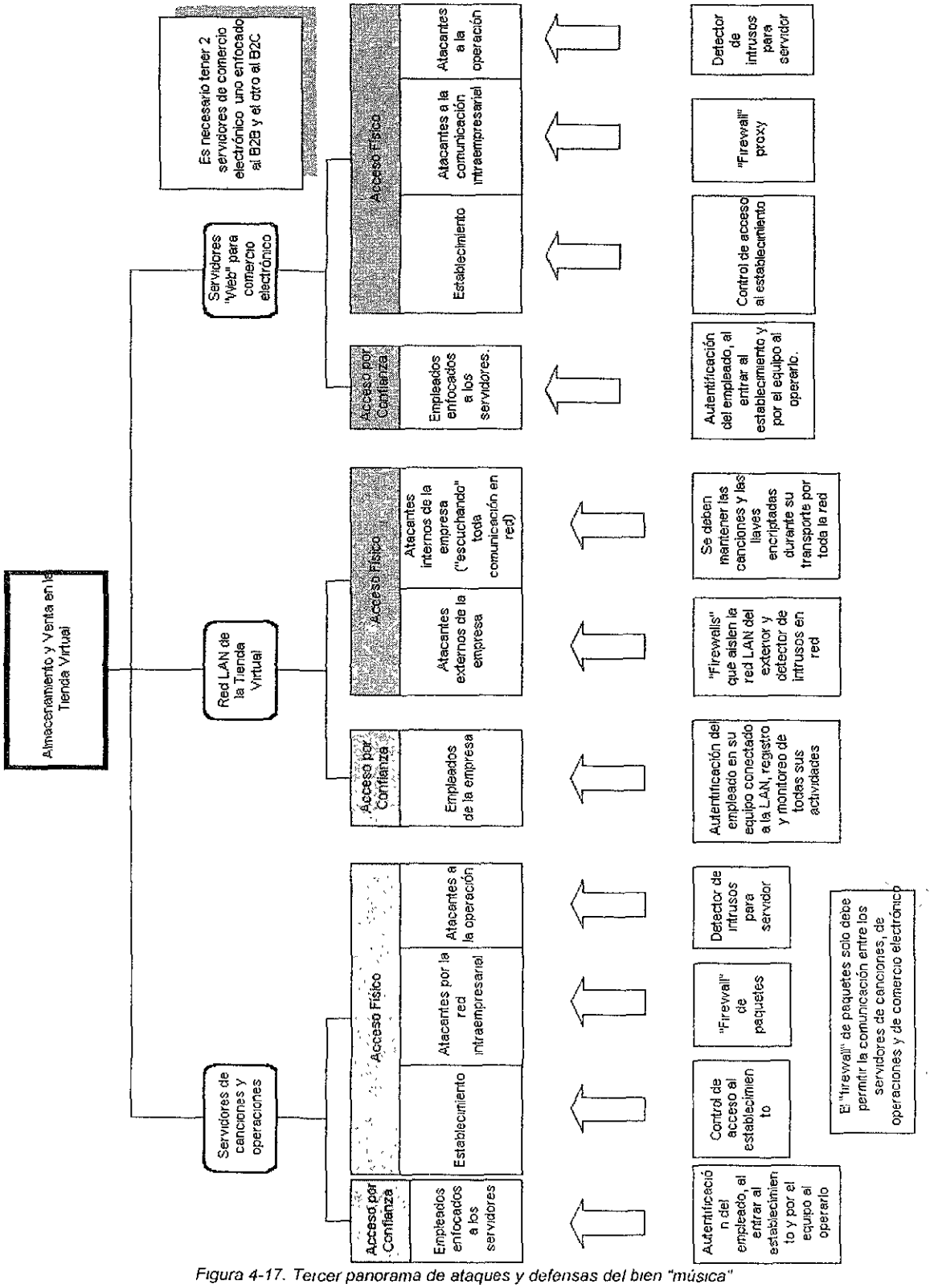


Figura 4-17. Tercer panorama de ataques y defensas del bien "música"

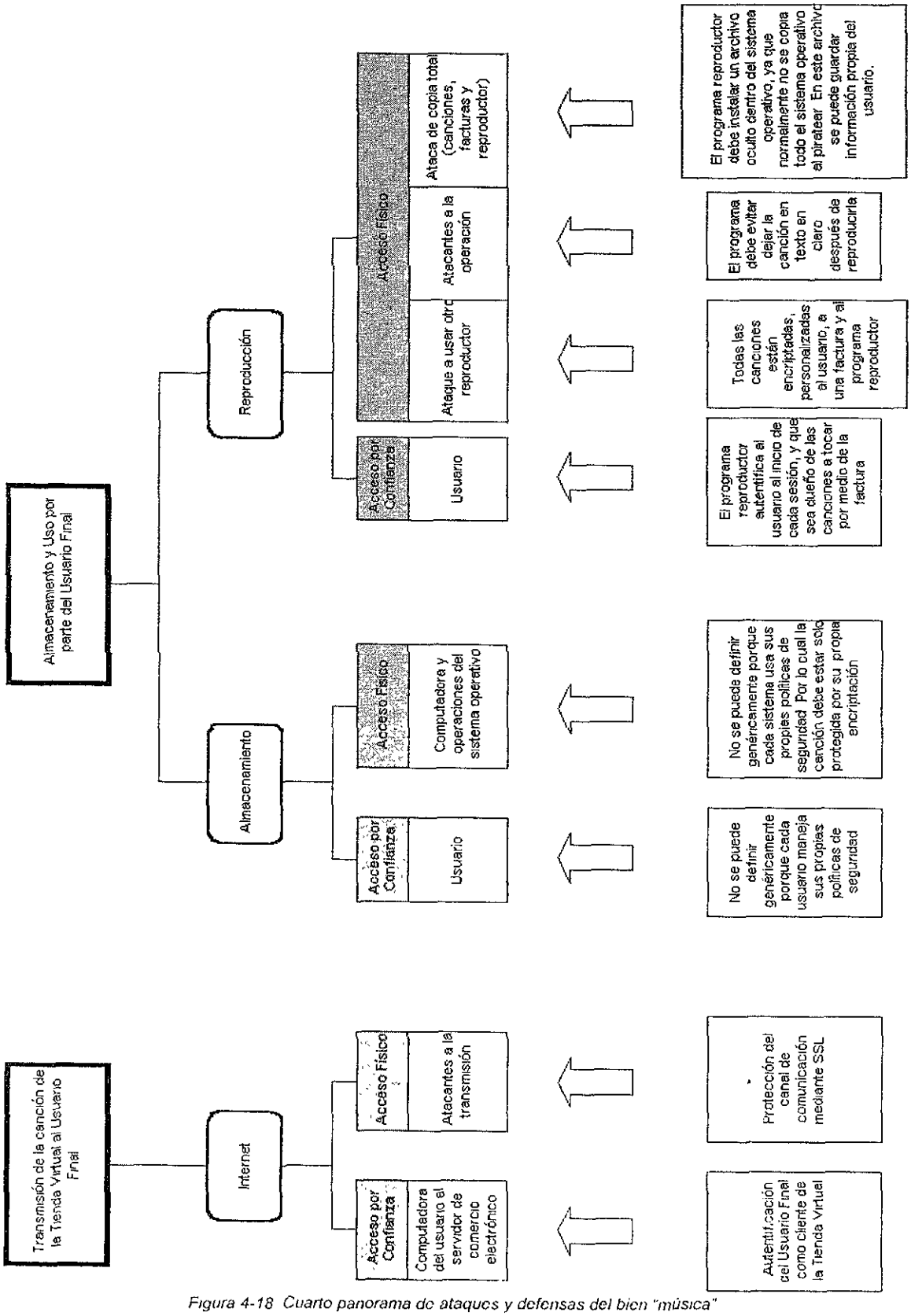


Figura 4-18 Cuarto panorama de ataques y defensas del bien "música"

4.7 Sistema propuesto

A continuación es bosquejado todo el escenario del sistema propuesto; para luego explicar las defensas necesarias del análisis anterior.

4.7.1 Componentes No Criptográficos

Al proteger los entes con los cuales el sistema tiene relación durante su ciclo de vida, nos lleva a enfocarnos a la seguridad informática en sistemas distribuidos. Un ejemplo en el cual se ven los riesgos antes mencionados y por lo cual debemos usar dicho concepto: el hecho de que la Tienda Virtual almacena todas sus operaciones en bases de datos, por lo cual va a existir la posibilidad de que sean atacadas (por personas internas o externas). Si en dichas bases de datos están almacenados en "texto en claro" los números de cuenta o tarjeta de todos los clientes, la envergadura de este problema es grande en comparación a que solo se comprometa el número de cuenta de un solo cliente (talvez interceptado en la transmisión).

La criptografía es un componente fundamental de una solución de seguridad informática para sistemas distribuidos; pero debe trabajar en conjunto con otros componentes no-criptográficos necesarios para integrar la solución acorde a la realidad de un sistema seguro (esquemas de redundancia energética y funcional, "firewalls", seguridad física de establecimientos, computadoras y sistemas operativos seguros, etcétera). Debido al alcance de esta tesis, no se implementarán dichos elementos no-criptográficos, pero sí mostraremos su importancia y actividad dentro del modelo del sistema.

4.7.1.1 "Firewalls"

Dado que la tesis debe abarcar la transmisión de información en redes de datos, éstas posibilitan muchos ataques internos y externos Por ello, el uso de los "firewalls" directamente evita el acceso de atacantes a los recursos informáticos así como la realización de ataques. Pero por las características propias de su funcionamiento, no son la absoluta defensa para todo tipo de ataque por red

4.7.1.2 Sistemas Detectores de Intrusos

Por la misma razón, los sistemas detectores de intrusos localizan, alertan y, si están integrados con los firewalls, frenan a los atacantes cuando quieran accesar, diagnosticar o atacar la infraestructura informática de la empresa.

Se recomienda leer el anexo D de la presente tesis, [23-34-38], [24, 34-37] y [25, 44-46]

4.7.2 Componentes Criptográficos

En esta sección mostramos los elementos criptográficos necesarios para el modelo propuesto.

4.7.2.1 Canal Seguro

Conviene utilizar un "canal de comunicación seguro" el cual, con la finalidad de poder realizar la transferencia de bits en forma segura por la red pública de Internet, incluya los procesos de

1 Petición y confirmación de petición de un canal de comunicación seguro.

2. Establecimiento del canal y realización de la comunicación.
3. Fin de la comunicación y cierre del canal.

4.7.2.2 "CryptoPlayer"

Realiza como acción la ejecución de la canción, para ello necesita:

1. Factura digital de compra.
2. La canción, encriptada de forma que dependa de la factura y la identidad del usuario.
3. Identidad del usuario.

4.7.2.3 "CryptoMusicMaker"

Crea la canción personalizada a cada Cliente Final.
Requiere:

1. La llave de encriptación de la Casa Musical.
2. La canción encriptada por la Casa Musical.
3. Datos del Cliente Final.
4. Factura del Cliente Final.

Da

1. La canción personalizada al Cliente Final

*Importante: la canción o la factura deben llevar en "texto en claro" título, cantante, autor, etc.; es decir, los datos que pudieran ser usados para un ataque por "texto en claro" conocido NO deben de estar encriptados.

4.7.2.4 "Crypto Engine de Autorización"

Protege la "e-form" de autorización a enviar al Banco para la transferencia de fondos de la cuenta de uno de sus cuenta habientes a otras cuentas, así como las formas electrónicas que mandan los cuenta habientes empresariales (Tienda Virtual y Casa Musical) para realizar las operaciones mercantiles.

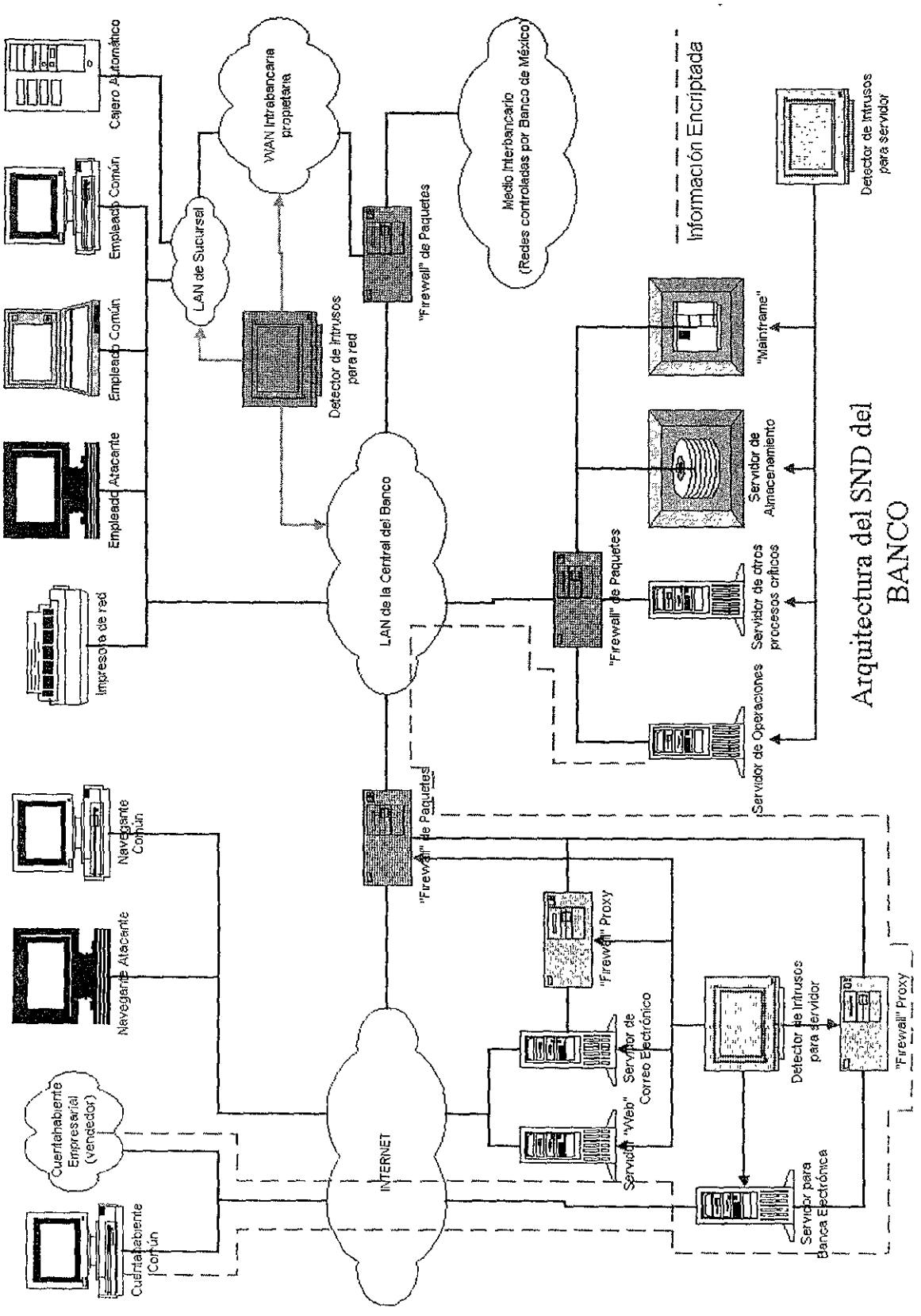


Figura 4-19. Arquitectura del SND para el Banco

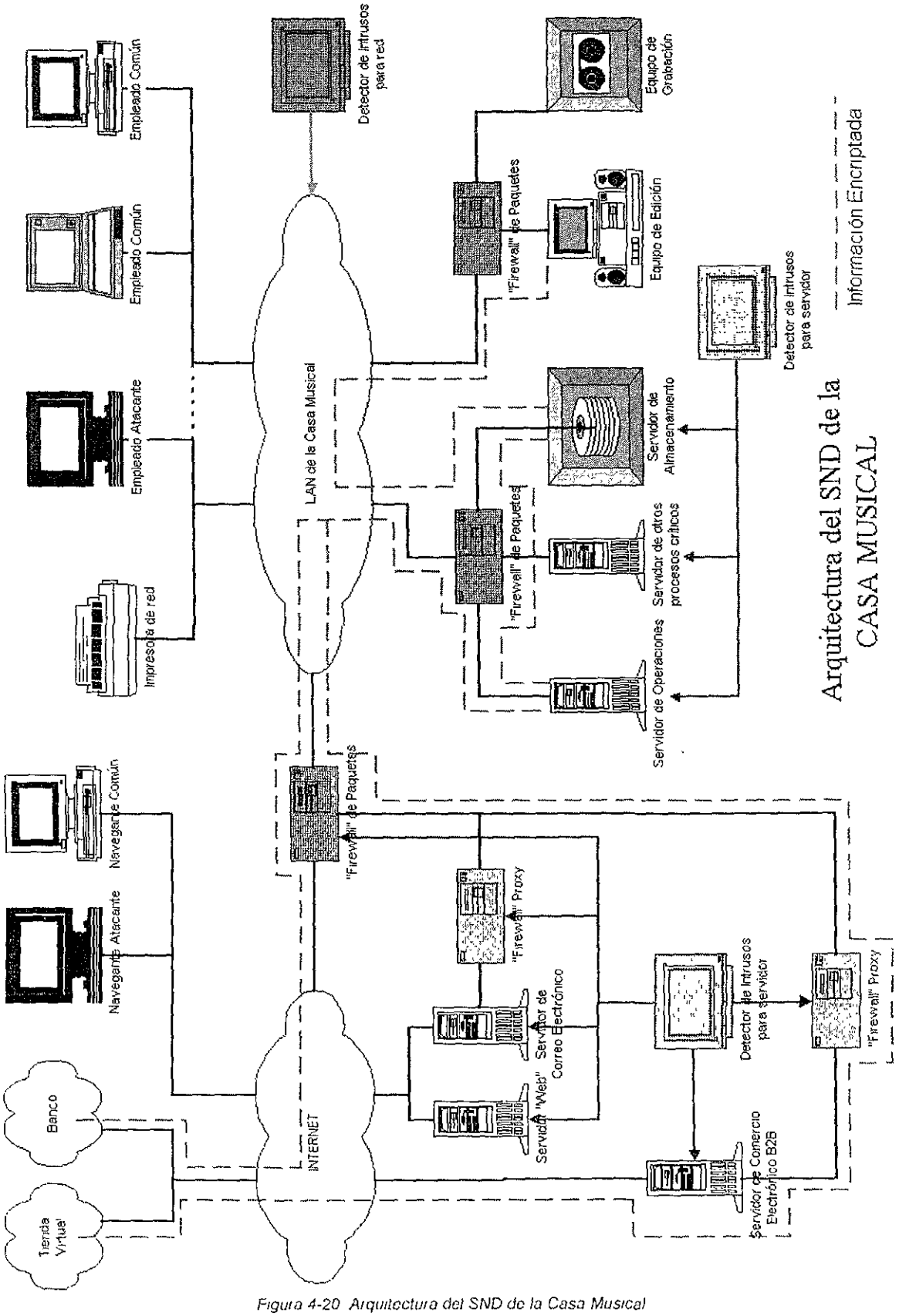


Figura 4-20 Arquitectura del SND de la Casa Musical

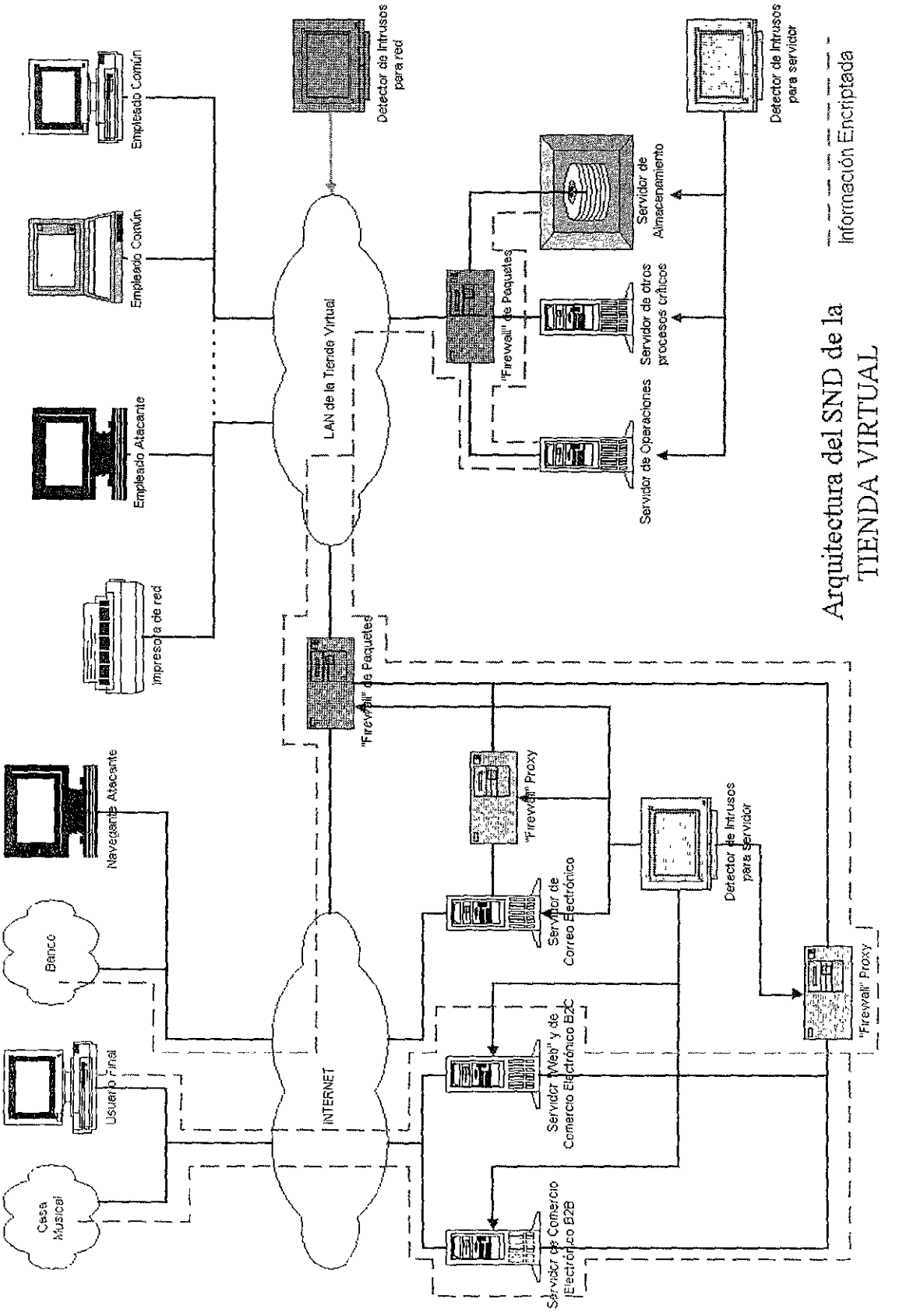


Figura 4-21 Arquitectura del SND de la Tienda Virtual

4.8 Procedimientos

Por último, mostramos las consideraciones y procedimientos que constituyen los protocolos para el manejo de los bienes a proteger.

4.8.1 Manejo de canciones

El Modelo General a usar entre Tienda Virtual y Casas Musicales establece la compra-venta de paquetes de canciones y canciones selectas; ambos pueden ser de carácter temporal (la llave y la canción caducan, para protegerlas en caso de que se hayan comprometido en el almacén de la Tienda Virtual) o permanente. Esto obliga a usar llaves de encriptación temporales o permanentes; "timestamp" (para indicar la fecha de inicio de vigencia) y tiempo de vida de las llaves temporales.

Esta situación también obliga a cada Casa Musical a dar su propio sistema encriptador "CryptoMusicMaker" para que sólo la Tienda Virtual que las haya comprado pueda hacer uso de la misma, además de tener la capacidad de recibir como valores de entrada llaves y datos para particularizar la canción (en un formato estándar) al cliente que se le vendió.

Este esquema implica que cada Casa Musical le da a la Tienda Virtual su "crypto engine", llamado "CryptoMusicMaker", llaves y canción encriptada para crear las canciones a vender al Cliente Final:

- Si la llave, la canción, o el "CryptoMusicMaker" son incorrectos o caducos; no se crea un archivo de salida (canción a dar al Cliente Final).

- El "CryptoMusicMaker" nunca deja una canción en texto en claro en algún registro.

- Las entradas al "CryptoMusicMaker" son:
    1. Canción encriptada.
    2. Llave de Tienda Virtual dada por la Casa Musical.
    3. Fecha del sistema
    4. Llave para encriptar la canción para el Cliente Final; y verificación que no sea una llave prohibida (que de como resultado el texto en claro).
    5 Campos a anexar a la estructura de la canción (los cuales verifica el CryptoPlayer).

- El "CryptoMusicMaker" verifica la integridad, "timestamp", firma de la Casa Musical y vida útil de:
    - Llaves usadas por la Tienda Virtual.
    - Canción

- La salida del "CryptoMusicMaker" es una canción encriptada que solo puede ser tocada por el Cliente Final.

En este modelo se propone que la Tienda Virtual venda canciones digitalizadas personalizadas a las características del cliente, para que él (ella) y únicamente él (ella) pueda reproducirlas. Además se utilizará el concepto del mundo común: el dueño de un bien debe tener un documento que acredita su posesión, por lo cual también será necesario utilizar una factura digital con el fin de que el cliente acredite la posesión de su(s) canción(es).

Las primeras consideraciones a usar son.

- La existencia de información única del cliente, la cual es intrínseca a él y diferente a la de otros clientes. Por lo tanto esta información única debe ser utilizada como un parámetro para "particularizar" la canción.
- El uso de dicha información única del cliente por parte de la Tienda Virtual implica que ésta también la conoce. Dicha información puede ser: la generación de una llave o clave en el momento en el que el usuario se dio de alta en la Tienda Virtual, además de los datos propios que da el usuario durante este proceso.

Para que el cliente escuche la canción debe usar un reproductor llamado "CryptoPlayer", el cual tiene las siguientes características:

- El Cliente Final puede instalarlo en todas "sus" máquinas. El hecho de que se use en varias máquinas implica que la información única del Cliente Final no depende del "hardware" o sistema operativo, por lo tanto se puede usar como información única los datos que dio cuando se dio de alta en la Tienda Virtual y la clave que ésta le haya asignado. Además el "CryptoPlayer" solo puede estar instalado para reconocer a un solo usuario.
- El "CryptoPlayer" conoce y usa la información única del Cliente Final para poder reproducir dichas canciones que el compra. Dicha información debe estar guardada en algún registro, encriptado, por lo cual no pueda ser visto por alguien ajeno al propio programa.
- Por seguridad, el "CryptoPlayer" debe se inicializado con un "password" al inicio de cada sesión.
- El "CryptoPlayer" usa una base de datos para almacenar las canciones que compra el usuario y las facturas correspondientes a cada canción.

Esto significa que si el Usuario Final desea escuchar una canción, debe tener los siguientes elementos para que funcione el "CryptoPlayer" (verifique y desencripte correctamente):

- El "password" para iniciar la sesión del "CryptoPlayer".
- El datos de usuario dados en la instalación (nombre completo, RFC, etc.), los cuales deben corresponder a los establecidos en la factura (usuario legítimo).
- La clave que se le asigno al darse de alta como cliente de la Tienda Virtual.
- La canción encriptada, la cual debe corresponder a la establecida en la factura (canción legítima) en cuanto a nombre y tamaño.
- La factura de dicha canción, con la misma relación de información y datos, tanto de la canción como del usuario (el usuario es legalmente dueño de la canción).
    - Además, el "CryptoPlayer" deberá verificar la integridad, la firma y el "timestamp", tanto en la canción(es) como en la factura.

Se puede diseñar el "crypto engine" para que todo el mensaje cifrado sea una combinación de los 3 elementos anteriores, y luego usar la llave extra proporcionada por la Tienda Virtual O bien, la llave se forma solo con los 3 elementos anteriores.

Resumiendo lo anterior, la Tienda Virtual también tiene una naturaleza dual por el tipo de comercio electrónico a establecer según sus participantes:

- Al vender sus canciones a los usuarios finales, requiere que su operación sea B2C (Business to Customer, negocio a consumidor).
- Al comprar las canciones a las Casas Musicales, requiere que su operación sea B2B (Business to Business, negocio a negocio) en un grado poco desarrollado.

Concluyendo con esto, se ejemplifica un negocio en el cual se conjugan los 2 tipos de comercio electrónico más comunes: el B2B y el B2C, unidos por un ente común: la Tienda Virtual

4.8.2 Manejo del dinero y Autorización Electrónica

Se asume que el representante legal de la Tienda Virtual y de la Casa Musical, así como el Cliente Final, se dan de alta como usuarios de sus respectivos Bancos FISICAMENTE (lo cual significa que no existen altas al Banco por medios electrónicos). Esto es con el fin de que la autentificación de los entes dueños de una cuenta, sea realizada por medio de documentos oficiales (ya que en la actualidad definen el nivel máximo de autentificación social). Esta actividad se realiza en las sucursales de cada banco, y es cuando se les asigna a cada uno el Número de Cuenta, el Número de Tarjeta asociada a dicha cuenta y su clave para descargar las herramientas electrónicas necesarias para operaciones electrónicas.

Una vez que cada ente ya es cuentahabiente del Banco, descargará las formas electrónicas y herramientas criptográficas necesarias para poder realizar sus operaciones comerciales por Internet. Para dicha descarga, así como para usar los servicios de banca electrónica (consulta de saldo, transferencia de fondos entre diferentes cuentas, pago de servicios domiciliados, etc.); cada cuentahabiente (particular o representante legal) primero deberá entrar al sistema y autentificarse con su clave.

Para las operaciones comerciales por Internet, en la actualidad el "pago a terceros con cuentas de diferentes bancos" no esta establecido; aunque esta en estudio su implementación. Por el momento, se utiliza el pago interbancario (más indirecto y no en línea conforme a las políticas de la red SECOBAN) como una opción a esta situación. Para los propósitos de esta tesis, manejaremos un posible esquema de "pago a terceros con cuentas de diferentes bancos" en el cual se maneja una forma electrónica que funcionará como "autorización encriptada". Otras formas de pago se pueden ver en [5, 189-211] y [26].

El Banco crea sus "e-forms" para "autorizaciones de transferencia" y "peticiones de transferencia entre cuentas", y los algoritmos criptográficos para proteger dichos documentos (algoritmos implementados como un "crypto engine", y pueden ser distintos para cada banco); los cuales pueden ser descargados por cada uno de sus clientes registrados.

Una "autorización de transferencia" de dinero entre diferentes cuentas, es análoga a la firma de conformidad para validar un pagaré. Este documento consta de:

- Número de cuenta emisora (comprador)
- Número de cuenta receptora (vendedor)
- Monto autorizado por ambas partes
- "Timestamp" del comprador
- Firma digital del comprador

Al comprar un usuario del Banco por Internet-WWW, debe de dar su autorización que será canalizada por el negocio cibernético. Dicha autorización es encriptada con el "crypto engine" del banco poseedor de la cuenta del usuario, con el fin de que este documento solo sea visible para el comprador y para el Banco; y así evitar atentados por parte del vendedor.

Para realizar la operación de compra-venta, el negocio debe canalizar la "autorización de transferencia" que le otorga el cliente como parte de la "petición de transferencia entre cuentas", la cual encripta la Tienda Virtual con el "crypto engine" de su banco. Toda "petición de transferencia entre cuentas" debe enviarse al Banco que posee la cuenta receptora (donde esta la cuenta de la Tienda Virtual), para que éste certifique y asegure que la identidad del beneficiario (cuenta receptora = vendedor o atacante) declarado en la "petición", sea la misma que realiza la operación. Si esto no se cumple, el Banco rechaza la petición.

Si todo esta correcto, este Banco envía una "petición de transacción" en la cual adjunta la "petición de transferencia entre cuentas" en texto en claro, más el "certificado de identificación del beneficiario" al Banco poseedor de la cuenta emisora, por el medio interbancario.

El segundo Banco es quien:

1. Desencripta la "autorización de Transferencia".
2. Verifica las firmas, "timestamp", integridad, monto autorizado y cuentas emisora y receptora de la "autorización de transferencia".
3. Coteja la información anterior con la de la "petición de transferencia entre cuentas" proporcionada.

Si TODO esta bien, los dos Bancos realizan la transferencia entre cuentas, le asignan un número de serie, la registran en sus respectivas bases de datos, y se genera un "acuse de transacción" para los bancos. El primer Banco envía "acuse de transferencia" al vendedor o emisor de la "petición de transferencia entre cuentas".

Si ALGO FALLA, se rechaza la "petición de transacción" y el segundo Banco le envía al primero el "rechazo de transacción", y éste envía su "rechazo de transferencia" al emisor de la petición. Además se pueden realizar otras acciones al analizar la falla:

- Si lo único que falla son las fechas:
    1. El reloj de la computadora del dueño de la cuenta emisora y consecuentemente, el "timestamp" de la autorización esta mal.
    2. El dueño de la cuenta receptora (tercero o vendedor) esta mandando una autorización antigua.
- Si no corresponden las cuentas receptoras de la autorización y la petición:
    3. El atacante quiere hacerse pasar por la cuenta beneficiada de la autorización.
- Si el Banco poseedor de la cuenta emisora desencripta basura de la "autorización":
    4. Falla o no esta actualizado el "crypto engine" del dueño de la cuenta emisora.
    5. Existe un atacante haciendo pruebas o quiere personificar al dueño de la cuenta emisora.
- Si lo que no corresponden son los montos en la "autorización" y en la "petición":
    6. El vendedor (cuenta receptora) trata de cargar más de lo pactado.
    7. El comprador (cuenta emisora) trata de pagar menos de lo pactado.
- Si fallan la firma y/o la integridad de la autorización:
    8. Existen fallas en la comunicación comprador-vendedor, pues se daño la autorización.
    9. El atacante modificó la autorización.

4.8.3 Servicio a autómatas o a personas

Por servicio a autómatas nos referimos a los sitios en Internet que están corriendo procesos para atender otros procesos remotos con fines específicos. Para el presente trabajo, los autómatas son los procesos que preparan una "petición de transferencia" en la Tienda Virtual; para luego enviarla a otro autómata en el banco, el cual esta escuchando un puerto específico en un servidor, por el cual procesará la "petición de transferencia" como anteriormente se describió.

Por servicio a personas nos referimos a los sitios en Internet que ofrecen una interfaz gráfica para interactuar con los cibernautas: un sitio "Web" común y corriente.

La Tienda Virtual y la Casa Musical interactúan con el Banco de 2 formas:

1. Como autómata: para realizar peticiones de transferencia y la actualización automática de "e-forms".
2. Como persona: el administrador de cada negocio puede bloquear la cuenta de la empresa o consultar el historial de actividades.

Mientras que la relación de la Tienda Virtual a la Casa Musical es:

1. Como autómata: al realizar actualizaciones de llaves, canciones, "CryptoMusicMaker" y catálogos; así como en la compra de canciones seleccionadas por el Cliente Final.
2. Como persona: al realizar la compra de canciones por paquetes o seleccionadas por el administrador del negocio; y la consulta al historial de actividades.

En cambio, la relación de la Casa Musical con la Tienda Virtual es:

1. Como persona: porque sólo envía ofertas, comentarios y consulta al catálogo.

Esta dualidad de "personalidad" de los usuarios del Banco y la Casa Musical obliga a definir 2 propuestas del funcionamiento de los sitios correspondientes a estos 2 entes:

- Solo se tiene un sitio con una sola interfaz común a ambos entes (autómata y persona). Para diferenciarlos se tiene un "time out" en la espera de petición (hecha por los autómatas); pero este enfoque obliga a analizar todo paquete que entra y son operaciones con tiempos de retardo acumulativos.
- Se tienen dos sitios, uno es la interfaz a los usuarios autómatas y el otro a los usuarios personas.

Por último, el Cliente Final solo se puede actuar como persona tanto con la Tienda Virtual como con el Banco. Esto se debe a su naturaleza de consumidor individual.

4.8.4 En Resumen

La ventaja del modelo B2B2C propuesto en esta tesis es la facilidad de establecer relaciones seguras entre dos entes cualesquiera, en las cuales ellos utilizan una "aplicación o sistema criptico complejo propietario" para realizar sus operaciones dentro del comercio electrónico, y puede ser una alternativa a utilizar soluciones propietarias de una sola compañía o corriente (como el EDI).

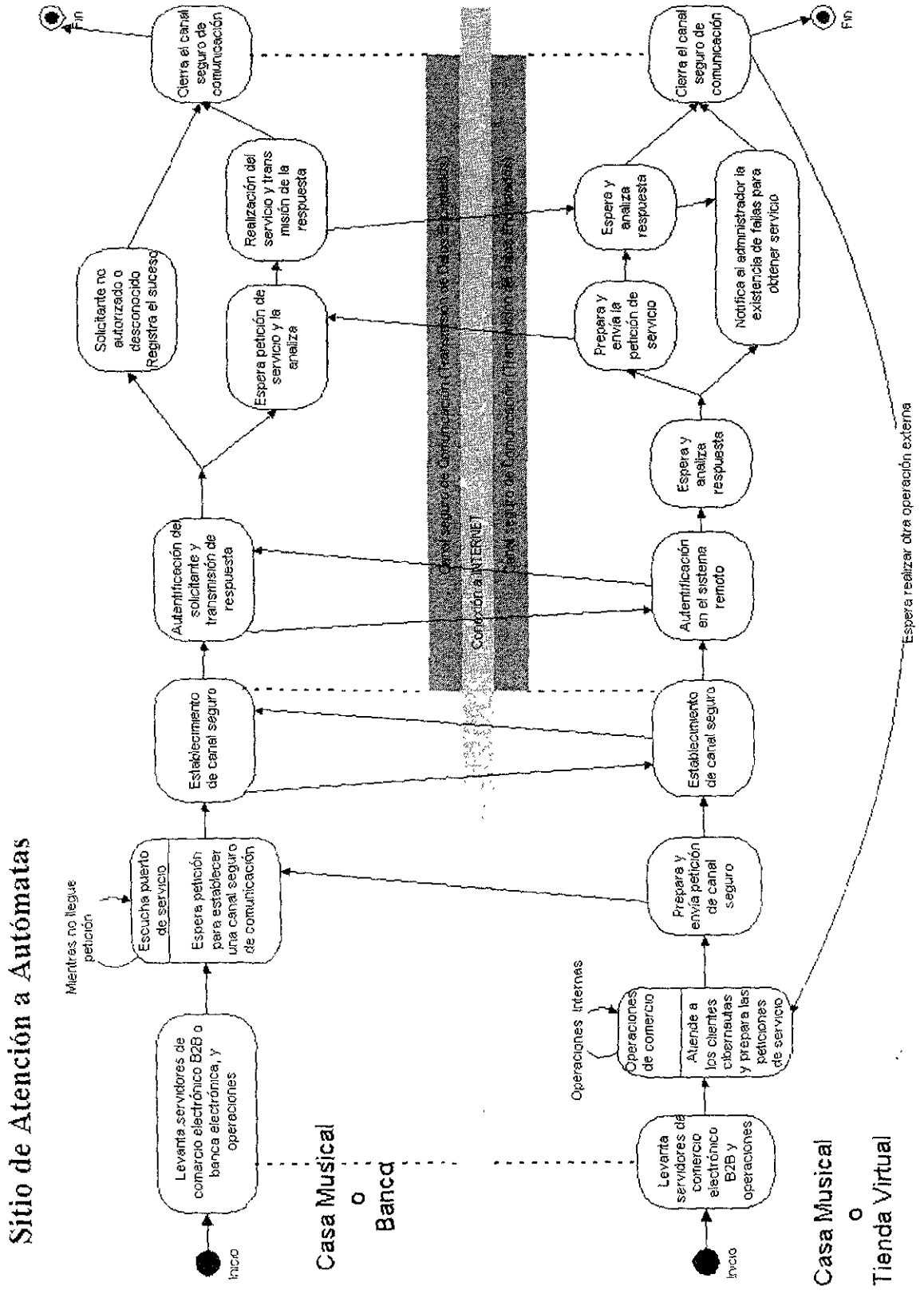


Figura 4-22 Diagrama de estados del funcionamiento del sitio de atención a automatas

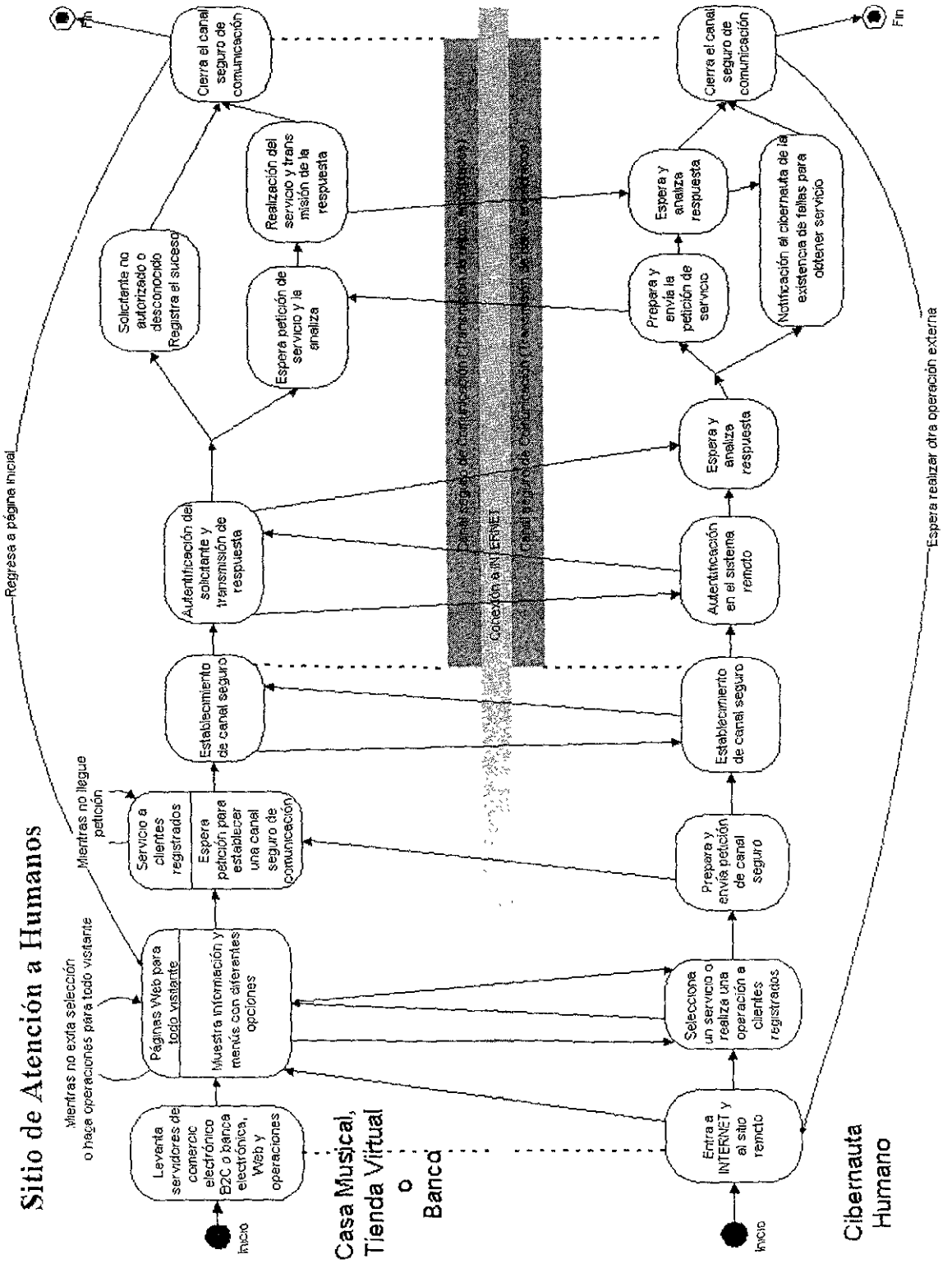


Figura 4-23 Diagrama de estado del funcionamiento del sitio de atencion a humanos

5 Documentación del Sitio Web Desarrollado y Aspectos de Programación

En esta sección se describe, en términos generales, la estructura y objetivos de las páginas Web que conforman el sitio de comercio electrónico utilizado para simular un portal de comercio electrónico en Internet. Se comienza por hacer una revisión de las tecnologías y lenguajes de programación empleados; posteriormente se describe la estructura lógica más común de acuerdo a la cual se organizan los sitios de comercio electrónico. De acuerdo a esta estructura, se establece la forma y jerarquía bajo la que se organizaran las páginas HTML de nuestro simulador, sus relaciones, vínculos y las acciones que se producirán al pasar de una a otra; y finalmente, se muestran fragmentos de código fuente y su interpretación.

5.1 Resumen de Tecnologías y Lenguajes de Programación Empleados

5.1.1 PWS ("Personal Web Server")

"Microsoft Personal Web Server" es un servidor Web de escritorio que permite publicar páginas HTML y compartir documentos en una red corporativa desde equipos de escritorio Además, PWS puede ser usado como plataforma de desarrollo para crear y probar sitios Web antes de ser cargados en el servidor de su ISP.

¿Qué es un servidor Web?
Mientras que un servidor Web pone documentos de todo tipo a disposición de los visitantes de Internet, PWS pone los documentos a disposición de un explorador de Web de la intranet corporativa.

PWS constituye una gran plataforma para que pruebe su sitio antes de alojarlo en el servidor de la compañía o en un proveedor de servicios Internet; pues permite comprobar los vínculos, formularios, secuencias de comandos y aplicaciones para asegurarse de que su apariencia y funcionamiento sean los correctos[35].

5.1.2 MIIS ("Microsoft Internet Information Server")

Es un servidor de Web de Microsoft originalmente diseñado para correr en la plataforma de Windows NT, actualmente se incluye como un paquete de Windows NT 4 o superiores, Windows 2000 y se puede utilizar a través de la utilería PWS en Windows 9x. Dado que este servidor está ajustado estrechamente a Windows NT, su administración es relativamente sencilla; sin embargo, esto lo limita a no poder ser un servidor de Web Universal, tal como el servidor de Web desarrollado por Netscape

5.1.3 ISAPI ("Internet Server Applications Program Interface")

Interfaz de programación de aplicaciones de servidor Internet. Una interfaz de programación de aplicación que reside en un equipo servidor para el inicio de los servicios de "software", ajustados para el sistema operativo Microsoft Windows NT. Es una API para desarrollar extensiones para Microsoft Internet Information Server y otros servidores HTTP compatibles con la interfaz ISAPI[35].

5.1.4 ASP ("Active Server Pages")

ASP proporciona un método eficiente y sencillo para crear sitios Web con páginas dinámicas y acceso a bases de datos. Para que un usuario realice una petición de páginas Web, deberá proporcionar en su explorador una dirección que indique un archivo con extensión ".asp".

Cuando se trabaja con IIS y Active Server Pages, el servidor de Web analiza las peticiones de páginas que recibe. Si se encuentra con una solicitud de una página con extensión " asp" en lugar de ".htm", entonces se apoya en la aplicación ISAPI que sirve de soporte de ejecución de las páginas ASP.

La aplicación ISAPI de ASP reconoce las líneas HTML, de las instrucciones que dan la funcionalidad dinámica a las páginas activas. Cuando determina el lenguaje en el que se encuentran los programas escriturados ("scripts"), da paso al motor de ejecución de "scripts" adecuado (JavaScript, VisualBasic Script, etc) Los motores de ejecución de scripts se encargan de realizar el análisis sintáctico y la compilación de las instrucciones ejecutables. Existe una memoria caché de páginas recientemente procesadas que permite aumentar las prestaciones de ASP, evitando repetir los procesos de separación de instrucciones, análisis sintáctico y compilación de las páginas más utilizadas.

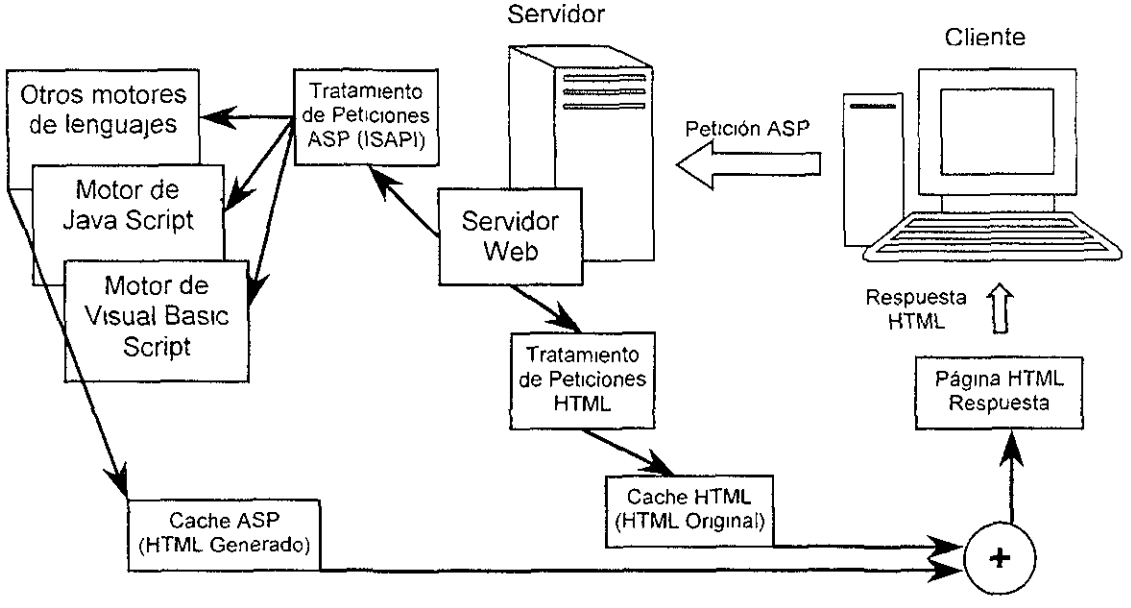


Figura 5-1. Funcionamiento General de ASP

Una vez resueltas las fases anteriores, se procede a ejecutar las instrucciones. Los motores de ejecución de scripts a menudo se encuentran con objetos ActiveX exteriores con los que tienen

que interactuar. Un ejemplo muy importante de esta situación se centra en el acceso a bases de datos a través de ADO (ActiveX Data Objects), basados en tecnología COM (Component Object Model).

El usuario recibe como respuesta un archivo ".htm", que se ha formado uniendo las instrucciones HTML originales de la página ".asp" con las instrucciones HTML que se han generado tras la ejecución de los scripts. Para más información, consulte [3, 283-385]

5.1.5 JavaScript

JavaScript es un lenguaje de alto nivel, basado en objetos, diseñado para permitir a los programadores Web la generación de documentos HTML interactivos de un modo sencillo. Ofrece las características básicas de un lenguaje orientado a objetos sin las complejas realizaciones que acompañan a otros lenguajes como Java y C++. No permite la definición de clases ni la utilización de herencia

El vocabulario de JavaScript, relativamente pequeño, es fácil de comprender y nos da un amplio número de posibilidades, antes no disponibles. JavaScript nos proporciona un conjunto de herramientas compactas propias que realzan las interacciones entre los usuarios y las páginas HTML. Estas herramientas nos permiten responder a las pulsaciones del ratón, a las entradas de los formularios, a la navegación de la página y a otros eventos.

Las respuestas a las acciones de los usuarios pueden ser invocadas sin necesidad de realizar transmisiones por la red. Esta es la mayor ventaja de JavaScript respecto a otras soluciones como ASP o CGI ("Common Gateway Interface"): las interacciones del usuario al ser procesadas en la computadora del propio usuario evitan la sobrecarga de tráfico en Internet Con ASP o CGI, las interacciones con el usuario deben ser procesadas en el equipo servidor y, por lo tanto, transmitidas por la red.

Como la mayoría de los lenguajes de "script", JavaScript es interpretado en tiempo de ejecución por el navegador antes de que se realice. La desventaja de los lenguajes interpretados es el tiempo que se tarda en ejecutar el código, porque el navegador compila las instrucciones antes de ejecutarlas. Sin embargo, la ventaja es que son mucho más fáciles de utilizar.

Los programas JavaScript se insertan en las páginas HTML: si el navegador es compatible con JavaScript interpretará el código y lo ejecutará Por tanto, su ejecución depende de la capacidad que tenga el navegador para interpretar el código JavaScript. Para más información, consulte [6].

5.1.6 Java

Java es un lenguaje de programación orientado a objetos desarrollado por Sun Microsystems. Fundamentado en C++, Java se diseño para ser pequeño sencillo y portátil, a través de plataformas y sistemas operativos, tanto en nivel de código fuente como binario, lo que significa que los programas Java (applets y aplicaciones) pueden ejecutarse en cualquier computadora que tenga instalada una máquina virtual de Java.

Como se verá más adelante, se utilizó una librería de Java llamada "Cryptix" para el cifrado y decodificación de los archivos de música así como para la aplicación cliente del usuario.

5.1.7 HTML y D-HTML ("Hipertext Markup Language" y "Dynamic HTML")

HTML es el código estándar para la creación de páginas Web. Recientemente, sin embargo, han aparecido una serie nueva de etiquetas y propiedades para las etiquetas anteriormente definidas

que permiten una mayor interacción y una mejor interfase de usuario. Para más información, consulte [2]

5.2 Proceso Básico de Compra en Internet

El mecanismo mediante el cual un usuario de Internet puede comprar un producto con su tarjeta de crédito varia de tienda virtual en tienda; sin embargo, se pueden identifican los siguientes pasos básicos:

a. El usuario selecciona el producto o servicio a adquirir (se añade a una "cesta de compras").
b Se le indica al sistema que se desea comprar el producto. En este caso, el usuario recibirá en la pantalla de su ordenador o dispositivo de acceso una orden de pedido que deberá incluir: Relación de los productos a adquirir, precio unitario y total. Gastos de envío, tramites e impuestos.
c En este punto, el comprador deberá introducir sus datos de identificación y destino necesarios para elaborar la factura y realizar el envío.
d. A çontinuación se seleccionará el medio de pago. Si utiliza la tarjeta, es conveniente asegurarse que está en una página Web segura
e. El comercio recibirá la orden de pago y solicitará autorización al banco del consumidor a través de la red bancaria.
f. Si el pago es aceptado el comercio enviará una orden de confirmación del éxito de la compra. Se recomienda guardar una copia de esta información, pues constituye un comprobante de que el pago ha sido efectuado.
g Finalmente el comercio entregará los productos solicitados, concluyendo de este modo el proceso de compra

No.	Descripción
1	En esta página se muestra un menú al resto de las secciones del portal, un recuadro para que los usuarios registrados se den de alta y las "Ofertas de la Semana".
2	Página en la que el usuario puede darse de alta, solicitar su registro al sistema o pedir su "password" en caso de que lo haya olvidado. Además, en esta página se indica el correo electrónico de atención a clientes.
3	Se da una explicación detallada de la forma en la que se deberán realizar las compras, así como el mecanismo mediante el cual se reproducen las canciones en la computadora del usuario.
4	En esta página se despliegan las canciones (productos o mercancía a la venta) almacenadas en nuestra base de datos. En esta página se dan los detalles elementales de la canción.
5	Esta página despliega aquellos productos seleccionados por el usuario. Al inicio se encuentra vacío. El proceso de "llenado" se realiza a través de una "cookie".
6	Preguntas más frecuentes. En esta sección se dan tips y consejos para el uso de tarjetas de crédito en Internet, y se responden algunos cuestionamientos relativos al "software"
7	En esta página los usuarios que no están registrados en la base de datos de usuarios pueden crearse una cuenta nueva a través de la cual realizarán sus compras.
8	Cuando un usuario selecciona una canción, esta se almacena temporalmente en una "cookie", misma que sirve para desplegar el contenido completo del registro almacenado en la base de datos. Si el usuario decide comprar esta canción, primero tendrá que agregar los datos de la "cookie" temporal a la "cookie" que guarda los registros del carrito.
9	La página de compra pedirá el número de tarjeta de crédito. A continuación hará la verificación de que se trata de un número válido y posteriormente captura el número de folio de la trasferencia.
10	Por último, nuestro portal tendrá una página en la que, primero, se desencriptarán los archivos "mkr" (provenientes de la Casa Musical) y se encriptarán con la llave propia del usuario. Después se generará la factura y por último, se enviará todo este paquete al usuario
11	Página de error, en caso de que ocurra algún incidente durante la transferencia.

5.5 Modo de Operación

El funcionamiento del sistema de seguridad, al que llamamos "CryptoPlayer", se basa en la existencia de dos componentes de "software": uno del lado del servidor ("CryptoMusicMaker") y otro más del lado del cliente ("CryptoPlayer").

"CryptoMusicMaker" es un sistema de almacenamiento, distribución y venta de música digitalizada, cuyo objetivo es poner a disposición del público una gran cantidad de títulos y temas musicales, permitiendo que sean los usuarios quienes personalicen su propia audioteca y únicamente compren aquellas melodías que sean de su interés personal.

Las razones por las que se escogió el mercado de audio digital fueron básicamente:

- porque no se necesita un gran ancho de banda para transmitir audio digitalizado.
- porque existe hoy en día un mercado potencial maduro para el audio digitalizado (ejemplo Napster).
- porque el audio digital es un bien informático, lo cual implica que para su venta y distribución no es necesario un soporte físico; por lo tanto, para mantener su valor, se requiere de un mecanismo que lo defienda contra intrusos y no debe permitirse su copia ilegal (cifrado).

El procedimiento mediante el cual un cliente cualquiera puede hacer uso del sistema es el siguiente:

a. Darse de alta en el sistema.
b Se le proporcionará un "password".
c. A continuación deberá descargar "CryptoPlayer".
d. Durante la instalación del reproductor, éste solicitará el "password" que le fue proporcionado en el punto dos.
e. Ir al Catálogo
f Agregarlo productos Carrito de Compras
g Comprar melodías
h. Proporcionar número de tarjeta de crédito
i. Si la operación se lleva a cabo con éxito, deberá descargar en su computadora el(los) tema(s) musical(es) de su carrito junto con su factura digital

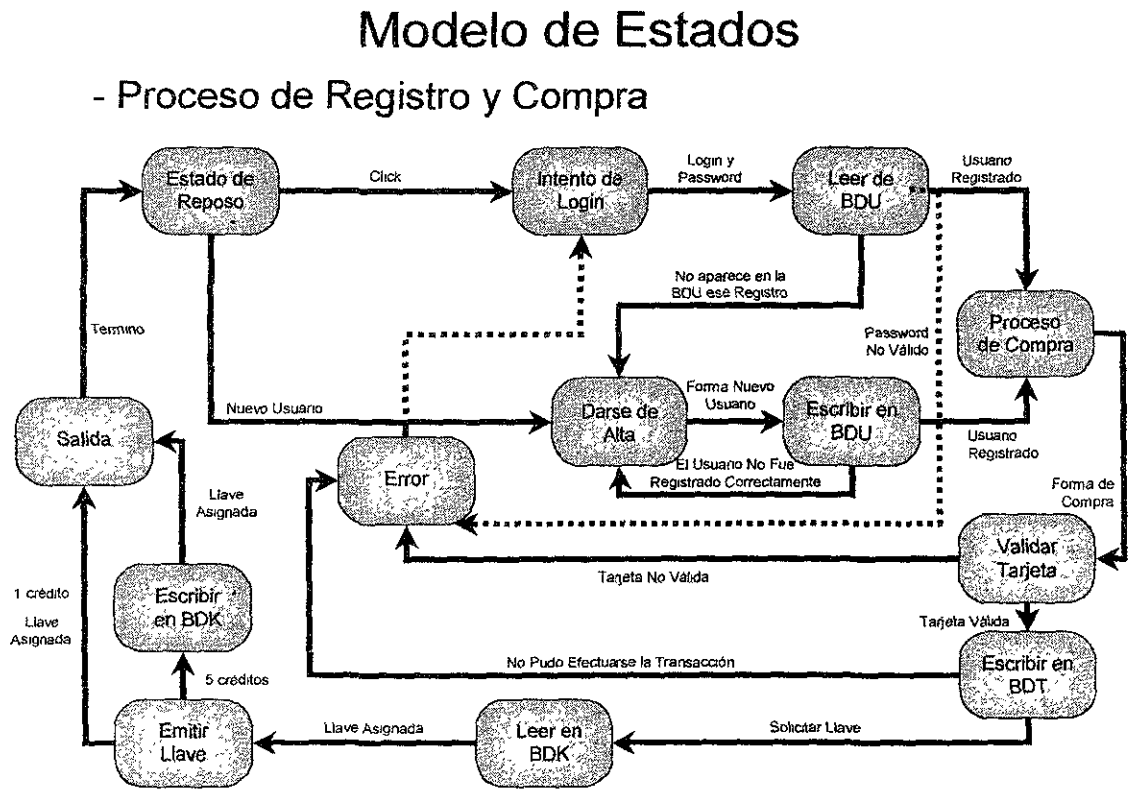


Figura 5-5: Modelo de Estados del Portal Comercial

5.6 Modelo de Estados

De acuerdo a este modelo, un navegante de Internet, al llegar a nuestro sitio Web comercial, podrá ver el catálogo de canciones que se ofertan en el portal, escoger aquellas que sean de su agrado y depositarlas en el carrito de compras Podrá ver también las páginas de FAQ y podrá enterarse de la forma en la que opera el sitio web en su totalidad antes de efectuar cualquier compra Esto es muy importante ya que, como se vio en el capítulo 2, el comprador de Internet basa sus decisiones en el conocimiento. Entre más conozca del portal comercial, sus políticas de ventas y el procedimiento de compra, más dispuesto estará de convertirse en nuestro cliente.

Pasado el punto de exploración del portal, el usuario deberá estar listo para realizar una compra. Si es la primer vez que nos visita, primero tendrá que pasar por un procedimiento mediante el cual se auto-creará un cuenta personal. Este punto es importante ya que permite conocer mejor a los clientes, tener una base de datos de los mismos, sus gustos y preferencias, hábitos de consumo y nos permite mantener contacto regularmente con ellos.

Después de este punto, el usuario deberá proporcionar sus datos de facturación y el número de su tarjeta de crédito. Se generará entonces una petición electrónica misma que será validada (junto con la tarjeta de crédito) y, si todo sale bien, se transferirán al disco duro del usuario tanto los archivos de las canciones (cifrados con su llave personal) que haya comprado, como las llaves respectivas.

5.7 Análisis de Código

Por razones obvias, no se puede describir todo el código presente en las páginas Web ya que ello representaría una cantidad enorme de información (mucha de ella repetitiva). Por esta razón, se tomarán solamente algunos fragmentos representativos que nos podrán dar idea de la funcionalidad de cada lenguaje de programación. Trataremos de comenzar desde lo más básico incrementando poco a poco el nivel de complejidad.

Se recomienda revisar la bibliografía mostrada al final de esta sección si se tienen dudas respecto a la sintaxis, las propiedades o características de los objetos, así como si se desea profundizar en alguno de los temas aquí señalados.

5.7.1 DHTML

Anteriormente, cuando una organización creaba un portal Web, debía asegurarse que todas las ligas apuntaran correctamente, que los colores de letras fondos o imágenes (por ejemplo, el logotipo de la empresa) correspondieran y estuvieran en el sitio adecuado. El problema de seguir este esquema radica en que, si se deseaba hacer un cambio en todas las páginas Web, dicho cambio debía reproducirse tantas veces como páginas hubiera en el portal.

La incorporación del HTML Dinámico permite ahorrar trabajo de administración y actualización al utilizar hojas de estilo (CSS); así por ejemplo, si tenemos el siguiente código dentro de una página web:

<style>@import URL("Estilo_Form.css");</style>

y al mismo tiempo contamos con un archivo llamado "*Estilo_Form.css*", cuyo contenido es el que se muestra a continuación:

Estilo_Form.css

```
body {color:'#000000'; Font-family:arial; text-align:justify;}
h1 {color:'#000000'; text-align:center; font-size:18;
font-family:Arial; font-style:italic; font-weight.bold}
h2 {color:'#FF0000'; text-align:justify; font-size·13; font-style:Arial}
h3 {color:'#FF5500', text-align·justify; font-size:13; font-style:Arial}
```

Al incorporar esta etiqueta dentro de la cabecera de nuestras páginas HTML, estaríamos forzando a que todas las páginas tenga un color de fondo **negro** y tengan un tipo de letra por defecto **Arial** con alineación **justificada** (etiqueta <body>).

De igual modo, si dentro de nuestra página Web etiquetamos un párrafo con <h1>, por ejemplo, indicaríamos que dicho párrafo tendría un color de letra **negro**, su alineación estaría **centrada**, el tamaño y fuente sería **18** y **Arial** respectivamente, y tendría activa la propiedad de **remarcado**. Y así sucesivamente

Como puede verse, la utilización de hojas de estilo ahorra tiempo cuando se desea homogeneizar la presentación de las páginas estableciendo un formato predefinido. De igual forma, cuando se desea cambiar el aspecto de todas o algunas de las páginas web, solamente será necesario modificar el archivo ".css".

5.7.2 JavaScript

JavaScript está basado en una jerarquía de objetos predefinidos que se asumen constantes en todos los navegadores para Internet Además, JavaScript es muy útil cuando se desean controlar

eventos dirigidos por acciones del usuario o cuando se desean realizar operaciones sencillas en las que no es necesario que la página Web se tenga que volver a comunicar con el Servidor.

Se recomienda dirigirse a la bibliografía para entender con mayor detalle la jerarquía de objetos de JavaScript y los procedimientos necesarios para invocar los eventos; sin embargo, para comprender los tres ejemplos que se dan a continuación veamos la gráfica siguiente:

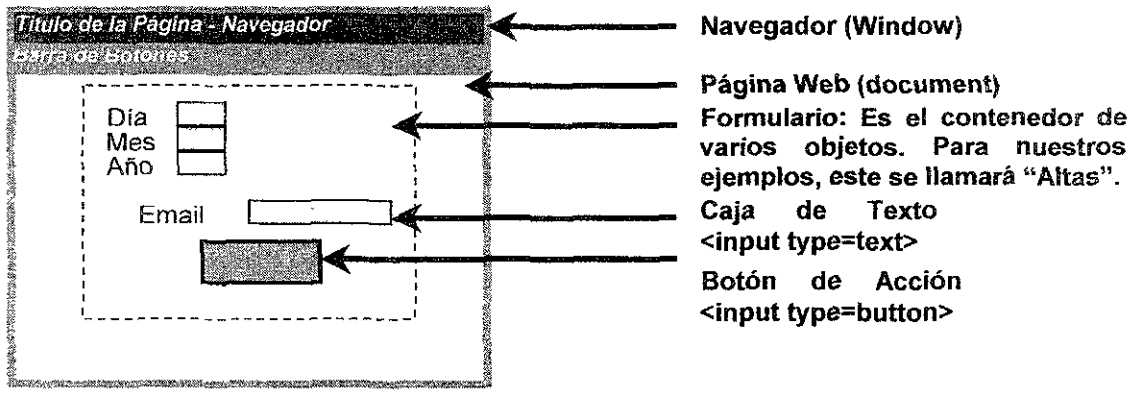


Figura 5-6: Ejemplo de una Página Web

a) Operaciones con objetos del navegador. Una de las tareas más sencillas que puede realizar un código JavaScript es la modificación y/o lectura de las propiedades de un objeto

```
function ponFecha()
{
        var vDia=document.Altas.Dia.value;
        var vMes=document.Altas.Mes.value,
        var vAño=document.Altas.Año.value;

        document.Altas.Fecha.value=vDia + "/" + vMes + "/" + vAño;
}
```

La función mostrada aquí, toma los valores de tres cajas de texto contenidas dentro de un formulario llamado "Altas". Con estos valores forma una sola cadena concatenando las tres cadenas de texto e intercalando diagonales entre valores Por último, la cadena final es asignada a otra caja de texto del mismo formulario

b) Verificación de Formularios. Otra de las actividades en las que constantemente se recure a los scripts de JavaScript es en la verificación de los campos de formularios.

```
function VerificaCampos()              {
        if(document.Altas Email value=="")
{
window alert("No se introdujo la dirección de e-mail");
}
else
{
window.alert("¡¡¡Gracias!!!"),
        Alta(document.Altas.Email.value),
                }
}
```

En este ejemplo se ve que al invocarse la función VerificaCampos(), se busca la casilla de E-mail y se verifica su valor. Si la casilla está en blanco, el script envía un mensaje de error para solicitar que el usuario corrija la falta. En el caso de que exista el valor, lo agradece y envía este valor como parámetro a otra función que es la encargada de dar de alta la dirección de correo electrónico.

c) Eventos. Por último, el manejo de eventos es de las funciones más sencillas pero al mismo tiempo de las más potentes a la hora de trabajar con páginas HTML

<input name="Enviar" value="Enviar" type=button OnClick=VerificaCampos()>

En este ejemplo se puede ver que se ha incorporado dentro de la página web una etiqueta de entrada tipo botón. Este botón tiene un nombre y un valor, pero al realizarse la acción de pulsarlo (OnClick), hace un llamado a la función VerificaCampos(), vista con anterioridad.

5.7.3 ASP

Mientras que la definición de JavaScript se establece mediante las etiquetas <script language="JavaScript">, para ASP debe usarse la etiqueta:

<%@ language=jscript %>

En general, el lenguaje ASP entiende todas sus instrucciones siempre que estén dentro de una etiqueta cuya forma genérica es: <% --código-- %>.

Aunque ASP hace uso de los recursos del servidor para la generación de páginas HTML (lo que aumenta el tráfico del lado del servidor), tiene como puntos a su favor el ser un lenguaje de fácil aprendizaje y de relativa sencillez en cuanto a su puesta en operación.

Para el caso de nuestro portal Web, se le utilizó tanto para el manejo de bases de datos como para el manejo y administración de "cookies".

A) Bases de Datos en ASP

Para poder utilizar bases de datos a través de ASP, es necesario dar de alta la librería:

<!-- #INCLUDE File="ADOJAVAS.inc" -->

La cual contiene una gran cantidad de valores constantes que son necesarios al trabajar con bases de datos

Un ejemplo simple del manejo de bases de datos con ASP se muestra a continuación

```
<%

Ob_Conector = new ActiveXObject("ADODB.Connection")
// Se importa un Objeto ActiveX que establecerá la conexión con el ODBC

Ob_RS = new ActiveXObject("ADODB.RecordSet")
// Se crea un nuevo Objeto ActiveX que almacenará los resultados

Ob_Conector.Open("BD_Canciones")
// Se abre la conexión con el ODBC

Ob_RS.Open("Canciones", Ob_Conector, adOpenStatic, adCmdTable)
```

```
//Se indica de que tabla se obtendrán los datos y la manera en la que estos serán obtenidos y actualizados.

Ob_RS.Filter = "IdProducto=" + Request.Form("CurrentSelec") + ""
//Criterios de filtrado e instrucciones SQL
%>

<% while (!Ob_RS.Eof) { %>
<!—Aquí se colocaría el código que se desea extraer de la base de datos à
<%
Ob_RS.MoveNext().
}
Ob_RS.Close()
Ob_Conector Close() %>
// Se cierra la conexión y el listado de resultados.
```

B) "Cookies"

Por su parte, llamamos "cookies" a pequeños almacenes de información (generalmente archivos tipo texto) que almacenan, administran, crean y borran los navegadores de Internet y que nos permiten guardar información referente al usuario, sus gustos, preferencias, las páginas que ha visitado, etc.

La forma mediante la cual asignamos o extraemos información de una "cookie" es mediante las instrucciones "Response" y "Request" respectivamente, siendo su sintaxis genérica la siguiente:

[Response/Request] Cookies(cookie)[(clave)].atributo]=valor;

Y la manera de eliminar una "cookie" es mediante la instrucción:

Response.Cookies(cookie).Expires="01/01/1980";

Donde la fecha de expiración ya ha pasado.

5.8 Librería Cryptix

Cryptix es un esfuerzo internacional cuyo objetivo es producir una serie de librerías y código fuente criptográfico abiertos y robustos. Este producto es de acceso libre y puede ser utilizado tanto en implementaciones comerciales como no comerciales. Actualmente esta siendo usado por desarrolladores de todo el mundo. Su código fuente se basa en el lenguaje de programación Java.

5.8.1 Cryptix JCE

De acuerdo a la página oficial de Java en SUN, la Extensión Criptográfica de Java (JCE) provee un marco de trabajo e implementaciones para encriptado, generación de llaves, convenciones para el uso de llaves, y algoritmos para la autentificación de mensajes. Soporta además encriptado simétrico, asimétrico, de bloque y de flujo. Esta extensión también da soporte para la creación de "flujos seguros" y objetos firmados

Sin embargo, la página oficial de Java no provee a los desarrolladores internacionales de la implementación del JCE, esto debido a que las políticas de exportación de los Estados Unidos impiden la salida de material criptográfico clasificado fuera de sus fronteras. Cryptix JCE comenzó

a desarrollarse para resolver este problema. Cryptix JCE es un conjunto de algoritmos y programas que se ajustan al estándar general esbozado por el API del JCE 1.2 oficial publicado por SUN. Cryptix JCE espera ser compatible 100% con la implementación de SUN y por supuesto, está disponible a nivel internacional de forma libre.

5.8.2 Características

Actualmente Cryptix JCE es soportado por las versiones 1.1, 1 2 and 1.3 del JDK de SUN.

5.8.3 Cifradores

Cryptix tiene a su disposición los siguientes algoritmos de cifrado:

Blowfish	CAST5	DES
IDEA	MARS	RC2
RC4	RC6	Rijndael
Serpent	SKIPJACK	Square
TripleDES	Twofish	

Soporta además la convención de llaves propuesta por Diffie-Hellman

Modos de Trabajo		
CBC	CFB-(con tamaños e bloque de 8, 16, 24, ..., bytes)	ECB
OFB (con distintos tamaños de bloque)		openpgpCFB

Funciones Resumen		
MD2	MD4	MD5
RIPEMD-128	RIPEMD-160	SHA-0
SHA-1	SHA-256/384/512	Tiger

Códigos de Autentificación		
HMAC-MD2	HMAC-MD4	HMAC-MD5
HMAC-RIPEMD-128	HMAC-RIPEMD-160	HMAC-SHA-0
HMAC-SHA-1	HMAC-Tiger	

Firmas Digitales		
RawDSA	RSASSA-PKCS1	RSASSA-PSS

Cifradores Asimétricos: RSA / PKCS#1

5.9 Ejemplos desarrollados

Los ejemplos que se muestran a continuación son páginas "web" desarrolladas para probar las implementaciones de los cifradores antes de su uso en el portal comercial desarrollado. La idea al desarrollar estas páginas, fue la de analizar la forma en la que operan los "applets" ya creados, y analizar la forma en la que están definidos sus constructores y métodos del lenguaje Java, para de esta forma, efectuar las modificaciones necesarias en ellos de acuerdo a las características fundamentales de nuestro problema y, además, para servir como material didáctico en posteriores cursos o como una base para tesis más avanzadas que intenten desarrollar este mismo tema.

5.9.1 Cifrador de Cesar

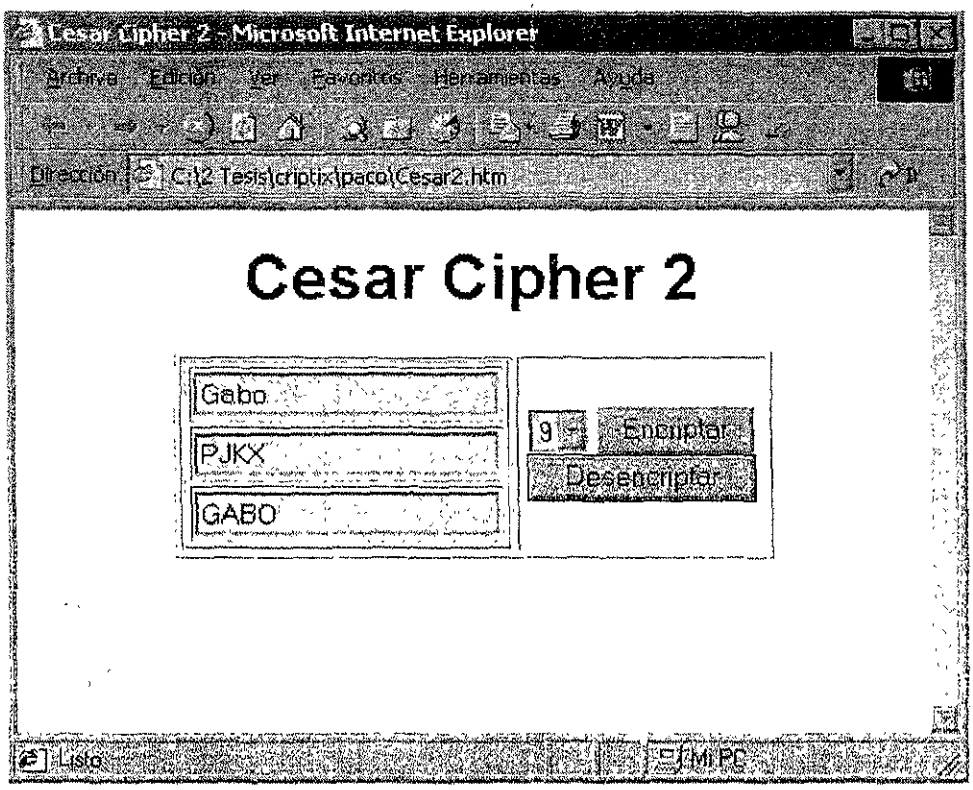


Figura 5-7: Cifrador de Cesar

El primer algoritmo que desarrollamos fue el Cifrador de Cesar. Como se puede apreciar en la figura 5-7, tenemos tres cajas de texto, de las cuales, en la primera el usuario introduce cualquier texto, al pulsar el botón de "Encriptar", aparece en la segunda caja el texto cifrado según el número especificado en la caja de selección. Hay que recordar que el cifrador de Cesar es uno de los métodos más sencillos (y antiguo) de encriptación Su forma de operar es básicamente sustituyendo cada letra por la letra correspondiente "n" caracteres por delante (o por detrás) en el alfabeto Para el ejemplo, al cifrar la palabra "gabo" la primera letra ***g*** se permuta por ***p*** debido a que esta última esta 9 posiciones por delante en el alfabeto

Posteriormente, al pulsar el botón de "Desencriptar" aparece en la tercera caja de texto el mismo texto pero aplicando la operación inversa (desencriptado).

5.9.2 Páginas con funciones Resumen

Para nuestro segundo ejemplo, mostrado en la figura 5-8, hicimos algo similar. En este caso, el usuario escoge una cadena de texto de las que se muestran en la tabla de ejemplos inicial. Introduce esta cadena en la primera caja de texto y el "applet" se encarga de buscar la función resumen de dicha cadena. En este caso, podemos escoger entre algoritmos SHA-1 y MD5.

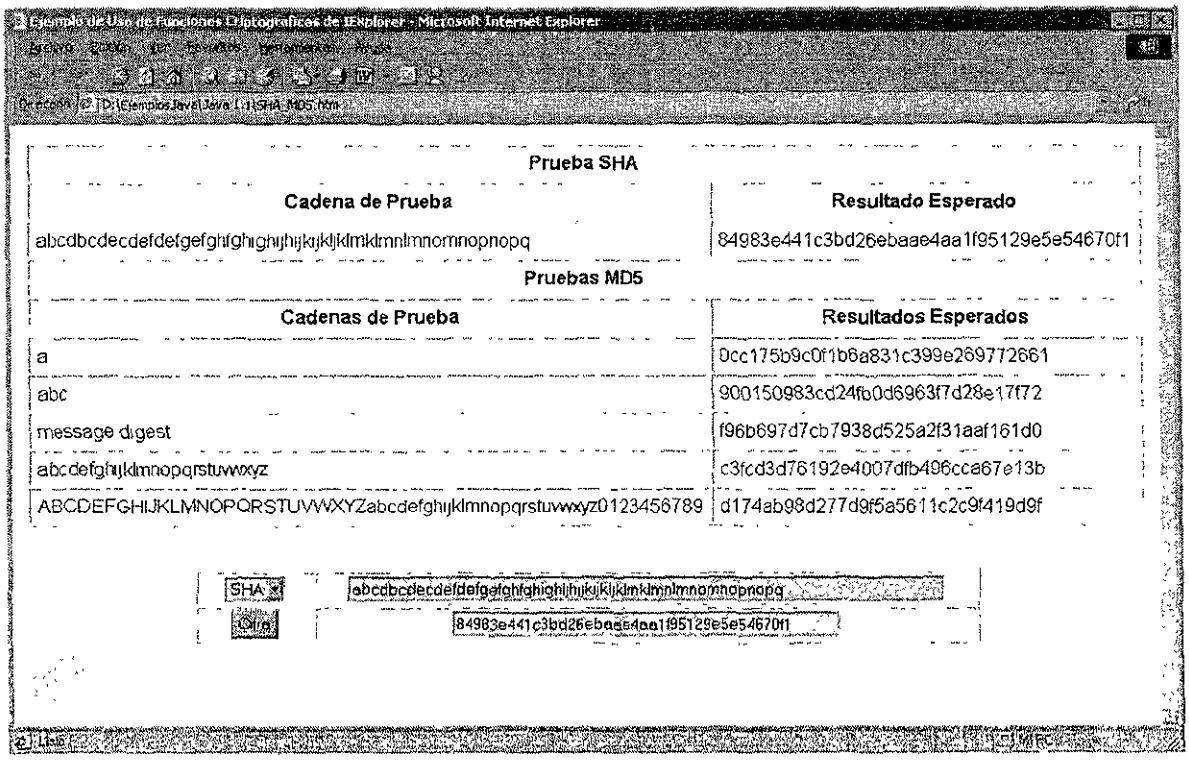


Figura 5-8: Funciones Resumen

Cabe hacer notar aquí que, como se muestra en el anexo A de nuestra tesis, la arquitectura básica de seguridad de Java posee dos elementos esenciales la Arquitectura Esencial de Seguridad de Java y la Arquitectura Criptográfica de Java (JCA) Dentro de la segunda, están definidas las clases que precisamente nos permiten obtener la función resumen de cadenas de texto de cualquier longitud. Estas clases fueron utilizadas para la implementación de este ejemplo

5.9.3 Páginas Encriptadoras

El último ejemplo mostrado en esta sección es una página "web" a través de la cual podemos encriptar archivos con extensión "***.txt***" utilizando ya sea, un algoritmo de cifrado DES, Blowfish o Rijndael. Véase la sección "CryptoMusicMaker" del siguiente capítulo "Resultados", en la cual se explica a detalle este ejemplo

6 Resultados

Esta sección presenta los resultados más importantes correspondientes a las etapas y actividades críticas realizadas durante el desarrollo del trabajo de tesis.

6.1 Java para el comercio electrónico

6.1.1 Razones por las cuales se utilizo Java

Dado que el producto inmediato de la tesis es una aplicación demostrativa por medio de la cual el usuario puede palpar el uso de la criptografía en el comercio electrónico, la primera decisión importante fue decidir que lenguaje de programación utilizar tanto para las interfaces y programas, como para los algoritmos criptográficos necesarios.

Después de un análisis de los posibles lenguajes a usar, Java fue seleccionado por sus siguientes características:

1. La existencia de librerías con funciones de encriptación para este lenguaje.
2. Capacidad para reproducir algunos tipos de formatos de audio, con características mejoradas a partir del JDK1.3 de Sun; las cuales utilizamos en el presente proyecto.
3. Operabilidad multiplataforma (para los sistemas operativos más populares), lo cual permite expandir el posible público usuario de la aplicación demostrativa. Y también dicha característica lo ha convertido en uno de los pilares fundamentales para el desarrollo de aplicaciones para Internet.
4. Es un lenguaje orientado a objetos, lo cual facilita la implementación del modelo que se realiza.

Un hecho, de gran trascendencia en el presente trabajo, aconteció al descargar la última versión del paquete de desarrollo del lenguaje del sitio web de Sun (el jdk1.3 a principios del año 2001): las librerías con las funciones criptográficas (agrupadas en el JCE) no están integradas a dicho paquete porque sólo pueden ser utilizadas dentro USA (ya que la criptografía es considerada un arma por las leyes de dicho gobierno). Estas disposiciones no sólo afectan a este lenguaje ni solo a esta compañía, sino que afecta a toda su industria enfocada a la seguridad informática

Para el proyecto, esta situación motivo a investigar posibles alternativas; encontrándose "JCE alternativos" desarrollados por grupos interesados en utilizar la protección de la criptografía con las capacidades de Java. Es un hecho que todas las "JCE alternativas" carecen de una documentación para utilizarlas, y en muchos casos, de ejemplos, instrucciones y herramientas para instalarlas y probarlas. La sección 6 2 del presente capítulo profundiza más en este tema. Sin embargo, un resultado concluyente de la investigación es la detección de un enorme potencial de desarrollo en este campo (en "software", "hardware" e integración); por la ausencia de los estadounidenses en el mercado global de aplicaciones criptográficas.

6.1.2 Sitio de Comercio Electrónico y diferencias de Java

La siguiente etapa consistió en diseñar el sitio de comercio electrónico. Se inicio con utilizar una misma computadora como sitio de comercio electrónico y cliente, para lo cual se instaló el

"Personal Web Server" para Windows 9x. Una vez en funcionamiento, se inicio el diseño de las páginas de la Tienda Virtual, y después se inicio el desarrollo de las bases de datos y la transferencia de la información entre ellas y las páginas del sitio, para dar al usuario mayor interactividad cuando haga sus transacciones con el sitio.

Como se detalla a profundidad en el capítulo anterior, fueron utilizadas las siguientes herramientas: Access, ASP, Java, JavaScript y HTML dinámico; para construir un sitio más interactivo en la información manejada. Casi todas las herramientas anteriores son tecnología propietaria de Microsoft. Y algunas de las ventajas de este esquema fue la gratuidad de las herramientas, así como un desarrollo rápido por la fácil integración de las mismas (por proceder de la misma compañía); pero hizo que resaltaran las diferencias del lenguaje Java de Microsoft y el estándar de Sun.

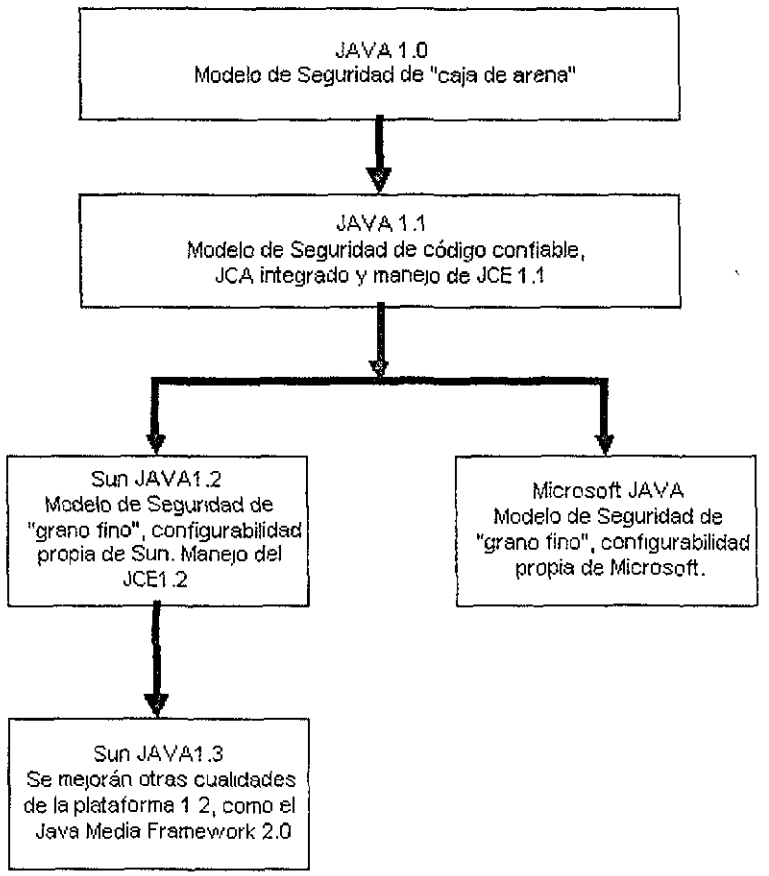


Figura 6-1. Evolución de Java y diferencias entre las implementaciones de Sun y Microsoft

Al utilizar el navegador "Navigator" de Netscape, el cual sigue un modelo más parecido al diseñado por Sun; se tenían fallas y errores al accesar al sitio web diseñado. En cambio, al usar el "Explorer" de Microsoft, no se presento ninguna situación anómala. Un hecho explotable como ventaja si se considera que el 95% de los cibernautas utilizan el "Explorer" de Microsoft (estadística de IDC); y lo cual aventajaría a un sitio web de comercio electrónico enfocado a un mercado masivo.

El análisis de las dos implementaciones del lenguaje nos llevo a concluir que conceptualmente son iguales: las versiones más actuales manejan modelos de seguridad de "grano fino"; es decir, que

pueden configurar y particularizar las medidas de protección a cada aplicación o applet que el usuario utilice. Pero la forma en que se implementa dicho modelo (llamadas a función, manejo de políticas, manejo de llaves y nombres de métodos) varían drásticamente del esquema diseñado por Sun al utilizado por Microsoft.

El resultado más inmediato y útil fue encontrar que ambas compañías mantienen en común la compatibilidad con la plataforma Java 1.1, en la cual se incluyó el JCA y se manejó el JCE. Este hecho nos llevo a deducir que para diseñar aplicaciones o applets que requieran manejar las 2 plataformas, se debe de utilizar como eje de trabajo las clases definidas en la plataforma 1.1 o manejar clases de compatibilidad (lo cual se realizó en este proyecto con un "parche").

A futuro se vislumbra que con el continuo desarrollo y especialización de cada vertiente se hará más difícil una mayor generalización de las aplicaciones, por lo cual se ve la enorme necesidad de normalizar el lenguaje antes de que se presentes situaciones críticas.

6.2 Algoritmos y llaves criptográficos para el comercio electrónico

En esta sección relacionamos los algoritmos y la longitud de las llaves criptográficas con las necesidades del modelo de comercio electrónico que hemos desarrollado en la presente tesis.

Primero se muestran las características de fortaleza de los algoritmos y llaves, luego un análisis de los bienes informáticos a proteger; para después relacionarlos y extraer el conjunto de llaves y algoritmos a usar.

6.2.1 Fortaleza de llaves y algoritmos

La evaluación de la fortaleza de los algoritmos y llaves criptográficos es un área reciente y en constante evolución Se han creado diversos criterios para evaluar unos y otros, pero es poco el desarrollo analítico aplicado, menor la divulgación de los resultados y no existe todavía una normalización para compararlos. De cualquier forma, se utilizan los resultados más demostrativos de los análisis y trabajos realizados por diferentes personas e instituciones, al criptoanalizar los algoritmos y llaves por medio de un ataque por fuerza bruta.

En general, el ataque a cada familia de cifradores y llaves se estima en función de 2 parámetros: la capacidad de cómputo requerida para efectuar el ataque y la cantidad de dinero disponible por el atacante.

La capacidad de cómputo generalmente se evalúa en mips-año: ejecutar un millón de instrucciones por segundo durante un año, lo cual significa ejecutar $3*10^{13}$ instrucciones En el mundo real, una PC con un procesador Pentium a 100 MHz tiene una capacidad de cómputo de 50 mips-año.

6.2.1.1 Equivalencia de llaves

A lo largo de esta sección se mostrará información relacionada a las llaves para algoritmos simétricos y asimétricos; razón por la cual es conveniente observar la siguiente tabla [18, Tabla7.8], en la cual se observa la equivalencia de la longitud de las llaves simétricas y asimétricas:

Longitud (en bits) de llave simétrica	Longitud (en bits) de llave asimétrica
56	384

64	512
80	768
112	1792
128	2304

Tabla 6-1. Equivalencia de llaves simétricas y asimétricas

Debido a que mucha información del análisis de llaves esta sólo enfocada a simétricas o asimétricas; la tabla anterior permite encontrar la equivalencia de un dato específico, de un sistema a otro.

Además, esta tabla también nos permite establecer el equilibrio de protección de las llaves de los algoritmos simétricos y asimétricos, en caso de que se diseñe y utilice un sistema híbrido (donde los asimétricos normalmente transportan las llaves simétricas y las simétricas protegen el almacenamiento de las asimétricas). La fortaleza de la llave de transporte debe ser por lo menos igual a la fortaleza de la llave transportada, y la llave de almacenamiento de las llaves de transporte debe tener una fortaleza superior a dichas llaves.

6.2.1.2 Llaves y algoritmos asimétricos

Dado que los algoritmos de cifrado asimétrico se basan en operaciones con grandes números (factorización, multiplicación, exponenciación, logaritmos, etcétera); el principal ataque por fuerza bruta a dichos algoritmos es por medio de la factorización de grandes números. Aunque este tipo de factorización es difícil, desafortunadamente para los matemáticos y diseñadores de algoritmos, cada año se vuelve más rápida.

Usando el método de *filtro de campo numérico especial*, (la técnica de factorización más rápida por el momento) tenemos los siguientes resultados [18, Tabla 7.5]:

Longitud del número en bits	Mips-año requeridos para factorizar el número
512	<200
768	100,000
1024	$3*10^7$
1280	$3*10^9$
1536	$2*10^{11}$
2048	$4*10^{14}$

Tabla 6-2 Tiempo de factorización de números grandes usando el método de filtro de campo numérico especial

Y en función del presupuesto del atacante (el cual se clasifica en 3 grandes grupos) la longitud de las llaves asimétricas recomendadas son [18, Tabla 7.6]:

Año	Atacante Individual	Atacante Corporativo	Atacante Gubernamental
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Tabla 6-3 Longitud de llaves asimétricas para defenderse de diferentes atacantes

Asumiendo que un atacante individual puede tener una capacidad de computo de 10,000 mips-año; un atacante corporativo, $1*10^7$ mips-año; y un atacante gubernamental, $1*10^9$ mips-año.

6.2.1.3 Llaves simétricas

El ataque por fuerza bruta a estas llaves es la búsqueda en forma exhaustiva de la llave utilizada en el correspondiente espacio de llaves.

La ley de Moore establece que el poder de computo se duplica cada 18 meses, tiene por consecuencia directa que los costos de un equipo se reducen en un factor de 10 cada 5 años. Es decir, que un equipo que costaba $1 millón en 1995, costó $100,000 en el 2000. Al aplicar esta ley a la [18, Tabla 7.1], se relaciona la longitud de la llave con la inversión necesaria para romperla por medio de un ataque de fuerza bruta, evaluando para los años 1995, 2000 y 2010.

Inversión 1995	Inversión 2000	Inversión 2010	40 bits	56 bits	64 bits	80 bits	112 bits	128 bits
$100 K	$10 K	$100	2 s	35 h	1 a	70,000 a	10^{14} a	10^{19} a
$1 M	$100 K	$1 K	0.2 s	3.5 h	37 d	7,000 a	10^{13} a	10^{18} a
$10 M	$1 M	$10 K	0.02 s	21 m	4 d	700 a	10^{12} a	10^{17} a
$100 M	$10 M	$100 K	2 ms	2 m	9 h	70 a	10^{11} a	10^{16} a
$1 G	$100 M	$1 M	0.2 ms	13 s	1 h	7 a	10^{10} a	10^{15} a
$10 G	$1 G	$10 M	0.02 ms	1 s	5.4 m	245 d	10^{9} a	10^{14} a
$100 G	$10 G	$100 M	2 µs	0.1 s	32 s	24 d	10^{8} a	10^{13} a
$1 T	$100 G	$1 G	0.2 µs	0.01 s	3 s	2.4 d	10^{7} a	10^{12} a
$10 T	$1 T	$10 G	0.02 µs	1 ms	0.3 s	6 h	10^{6} a	10^{11} a

Nomenclatura: s = segundos, m = minutos, h = horas, d = días, a = años

Tabla 6-4 Relación de la inversión necesaria para romper llaves simétricas

Asumiendo, según el ensayo "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commmercial Security", que un atacante individual puede invertir hasta $10,000; un atacante corporativo de $10,000 – $300,000,000 (según si la empresa es chica, mediana o grande); y un atacante gubernamental (como una agencia de inteligencia) de $300,000,000 en adelante.

6.2.1.4 Algoritmos simétricos

Aunque no existe una forma de evaluar la robustez de cada algoritmo (como ha implementado los principios de confusión y difusión) ni cual es su eficiencia en el manejo de la longitud de la llave; sí se puede evaluar cada cifrador en base a 2 parámetros:

1. La velocidad de encriptación (refleja indirectamente la confusión y difusión realizadas sobre el texto en claro; se recomienda leer [32] para ver con más detalle el criptoanálisis cuando se han implementado pocas o muchas etapas de confusión y difusión).
2. El desarrollo criptoanalítico enfocado en cada algoritmo particular.

Para el primer punto tenemos la siguiente tabla en la cual se muestran las velocidades de encriptación de algunos cifradores de bloques en un 486SX a 33 MHz [18, Tabla 14.3].

Algoritmo	Velocidad (KiloBytes/segundo)	Algoritmo	Velocidad (KiloBytes/segundo)
Blowfish (12 rounds)	182	MD4	186

Blowfish (16 rounds)	135	MD5	135
Blowfish (20 rounds)	110	SHA	23
DES	35	NewDES	233
FEAL-8	300	REDOC II	1
FEAL-16	161	REDOC III	78
FEAL-32	91	RC5-32/8	127
GOST	53	RC5-32/12	86
IDEA	70	RC5-32/16	65
Khufu	221	SAFER (6 rounds)	81
Lucifer	52	TripleDES	12

Tabla 6-5. Velocidades de encriptación de algunos algoritmos

Para el segundo punto, por la literatura [18] podemos ver que DES y sus variaciones (DES2X, TripleDES, etc.) han sido sometidos a un enorme trabajo criptoanalítico; lo cual obliga a no utilizar dicha familia de cifradores en aplicaciones de comercio electrónico actuales y futuras.

6.2.2 Determinación de la longitud de llave requerida

Como se ha mencionado con anterioridad, nuestros 2 bienes informáticos más importantes son la canción digitilazada y el dinero (número de tarjeta). Es necesario analizar su características para determinar las necesidades criptográficas a cubrir

Para determinar la longitud de la llave requerida por cada bien, se deben considerar 3 parámetros:

1. el **tiempo de vida del bien**;
2. el **valor monetario del bien;**
3. el **tipo de atacante** a enfrentar, en especial por su capacidad económica.

Estas tres variables permiten determinar la longitud mínima de la llave (simétrica o asimétrica) que deberá ser usada para proteger dicho bien; ya que el tiempo necesario para romper la llave debe ser mayor que el tiempo de vida útil, y el costo de implementar el ataque debe ser mayor al valor del bien y al presupuesto del atacante.

6.2.2.1 Canción

Analizando la canción digitalizada, existen dos tiempos de vida importantes:

1. El **tiempo de novedad**, cuando la canción es nueva y es lanzada al mercado Se presenta en todas las canciones, sin importar género ni público. Este período puede ir de unas semanas hasta 2 años.
2. El **tiempo de popularización** por parte del público, cuando es asimilada como parte de la cultura musical de un grupo humano ("las mañanitas", "happy birthday", etcetera) Este período puede llegar a pasar los 100 años; y son pocas las canciones que alcanzan este nivel

Y los atacantes pueden ser de dos categorías:

1. **Atacante individual** o un grupo de atacantes individuales; con recursos moderados pero con un enorme interés de poder usar el dinero de otros.
2. **Atacante corporativo**, incluyéndose a las organizaciones criminales; lo cual nos lleva a considerar que pueden dedicar cuantiosos recursos para criptoanalizar el número de tarjeta.

Por lo cual se concluye que la llave a utilizar para proteger el número de tarjeta debe tener una longitud que permita una protección de 60 años, un ataque cuyo costo supere los US$300,000, y soporte un atacante corporativo con recursos cuantiosos.

Utilizando las tablas mostradas, se recomienda una llave simétrica de un mínimo de 112 bits de longitud (aunque se recomienda una de 128 bits) o una llave asimétrica de un mínimo de 2304 bits de longitud; y no usar ningún cifrador de la familia DES. Dado que el número de tarjeta y la forma electrónica en sí son un conjunto de información relativamente pequeño, se pueden usar cifradores asimétricos.

6.2.3 Determinación de los algoritmos a usar

Dado que se van a utilizar aplicaciones y applets Java para implementar el modelo, se van a utilizar librerías JCE para realizar las operaciones criptográficas.

Se descartó el JCE de Sun (versiones 1.2 beta, 1.2 EA y 1.2 EA2), porque no pueden ser descargadas desde lugares fuera de USA. Al momento de hacer esta evaluación, existía solo el JCE de Bouncy Castle versión jdk1.3-105; el cual se descartó por sus múltiples fallas (para principios de julio del 2001 salió la versión jdk1.3-106 con las correcciones necesarias). Lo cual nos llevo a evaluar el JCE de Cryptix en sus dos versiones: 3.2.0 y JCE.

Utilizando los resultados de la longitud de llaves requeridas por cada bien informático, se presentan las siguientes tablas para delimitar el subconjunto de algoritmos candidatos a ser usados.

6.2.3.1 Cifradores simétricos de Cryptix

Algoritmo	*Tipo de llave*	*Longitud (en bits) usada por omisión o recomendada*	*Rango de longitud (bits)*	*Incremento gradual en el rango (bits)*	*Cryptix 3.2.0*	*Cryptix JCE*	*Candidato a utilizarlo en el modelo*
Blowfish	Variable	128	40-448	8	X	X	Sí
CAST5	Variable	128	40-128	8	X	X	Sí
DES	Fija	56 (redondeada a 64 por paridad)	Un solo valor	0	X	X	No

DESX	Conjunto (16 octetos en total)	1 llave de 56 bits tipo DES 1 llave de 64 bits tipo XOR	Un solo valor	0	X		No
DES2X	Conjunto (32 octetos en total)	1 llave de 56 bits tipo DES 3 llaves de 64 bits tipo XOR	Un solo valor	0	X		No
DES_EDE3	Conjunto (24 octetos en total)	3 llaves de 56 bits tipo DES	Un solo valor	0	X		No
TripleDES	Fija	168 (redondeada a 192 por paridad)	Un solo valor	0		X	No
HMAC	Variable	128	Cualquier valor diferente de 0	No especificado		X	Sí
IDEA	Fija	128	Un solo valor	0	X	X	Sí
Loki91	Fija	64	Un solo valor	0	X		No
MARS	Variable	256	128-256	64	X	X	Sí
RC2	Fija	128	Un solo valor	0	X	X	Sí
RC4	Variable	128	40-1024	8	X	X	Sí
RC6	Variable	256	128-256	64		X	Sí
Rijndael	Variable	256	128-256	64	X	X	Sí
SAFER	Variable	128	64-128	64	X		Si
Skipjack	Fija	80	Un solo valor	0		X	No

SPEED	Variable	128	48-256	16	X		Sí
Serpent	Variable	256	128-256	64		X	Sí
Square	Fija	128	Un solo valor	0	X	X	Sí
Twofish	Variable	256	128-256	64		X	Sí

Tabla 6-6. Algoritmos simétricos disponibles en el JCE Cryptix

6.2.3.2 Cifradores asimétricos disponibles en Cryptix3.2.0

Algoritmo	*Tipo de llave*	*Longitud (en bits) usada por omisión o recomendada*	*Rango de longitud (bits)*	*Incremento gradual en el rango (bits)*	*Candidato a utilizarlo en el modelo*
ElGamal *FALLA	Variable	No especificado	384-1024, obtenido en pruebas	128, obtenido en pruebas	No
RSA	Variable	No especificado	384-768, obtenido en pruebas	128, obtenido en pruebas	No

Tabla 6-7. Algoritmos asimétricos disponibles en el JCE Cryptix v3.2.0

6.2.3.3 Cifradores asimétricos disponibles en CryptixJCE

Algoritmo	*Tipo de llave*	*Longitud (en bits) usada por omisión o recomendada*	*Rango de longitud (bits)*	*Incremento gradual en el rango (bits)*	*Candidato a utilizarlo en el modelo*
DiffieHellman	Variable	16384	384-16384	8	Sí
ElGamal	Variable	1536	384-16384	8	Sí
RSA	Variable	16384	384-16384	8	Sí

Tabla 6-8. Algoritmos asimétricos disponibles en el JCE Cryptix vJCE

6.2.3.4 Análisis

Por los resultados anteriores, se puede observar que no conviene utilizar Cryptix 3.2.0 en el caso de que se deseen utilizar algoritmos asimétricos, ya que sólo RSA funciona sin problemas y el rango de la longitud de las llaves es insuficiente para nuestra aplicación.

En cuanto al algoritmo de cifrador simétrico a usar, tenemos buenos candidatos (todos presentes en la versión JCE y algunos en la 3.2.0):

- MARS
- RC6
- Rijndael
- Serpent
- Twofish
- Blowfish

Donde los primeros 5 concursaron para ser el algoritmo a usar como AES (Advanced Encryption Standard, siendo el ganador Rijndael).

Para nuestro modelo, se decidió utilizar Blowfish como cifrador simétrico (dado que es un cifrador rápido, en Counterpane se lista todas las personas y organismos que lo usan (bastantes), es libre y no existe mucho trabajo criptoanalítico sobre él); y ElGamal como cifrador asimétrico (pues no existe tanto trabajo criptoanalítico en comparación a RSA). Sin embargo en el código del "CryptoMusicMaker", descrito en 6.5, también se considera usar Rijndael ya que fue el algoritmo seleccionado por AES. En general, el manejo de algoritmos en el JCA y JCE de Java se simplifica a utilizar el nombre del algoritmo deseado en las funciones "crypto engines" creadoras de llaves y encriptadores / desencriptadores.

Por último, se utiliza SHA-1 (disponible en las dos versiones de Cryptix) para las funciones de integridad de la información. Esto se debe a que SHA da un resumen de 160 bits, lo cual es más sensible a cambios en comparación a los 128 bits que ofrece MD5.

6.3 Uso de herramientas no criptográficas

A partir del análisis de las necesidades de protección de la información y durante el diseño del modelo de comercio electrónico, se vio que la criptografía es una parte esencial de un sistema seguro, pero no es el único componente necesario para proteger la información. Debido a la enorme capacidad de interconectividad de Internet, característica base para todas las actividades del ciberespacio, es también un punto de entrada beneficioso a los atacantes informáticos.

El análisis nos reveló, en el capítulo 4, que el diseño de un sistema seguro para el comercio electrónico debe implementar algoritmos y protocolos criptográficos integrados a:

1. herramientas no criptográficas como muros corta-fuegos (firewalls) y detectores de intrusos,
2. políticas de seguridad a seguir por los diseñadores y todos los usuarios del sistema.

Aunque el alcance de la tesis no comprende implementar estas herramientas y políticas no criptográficas para tener un sistema seguro, sí fueron consideradas, estudiadas y utilizadas dentro del modelo teórico básico presentado

6.4 Sitio "Web" desarrollado

Para realizar pruebas y entender todo lo que implica el entrar al comercio electrónico, se diseño un pequeño sitio "Web" con tecnología Microsoft: Windows9x, PWS, Access (para las bases de datos), DHTML y ASP para traer y presentar los datos en forma rápida e interactiva; así como también se utilizo Java y Java Script para ciertas funciones e interfaces. Todo el capítulo 5 está dedicado a analizar detalladamente el uso de dichas tecnologías.

Sin embargo, nos percatamos de que es necesario mucho tiempo y desarrollo para poder implementar todos los flujos informáticos y procesos digitales necesarios, que conlleven a tener un sitio totalmente funcional de nivel III (véase la figura 2.1 y toda la sección 2.6 del presente documento). Logramos plantear el modelo teórico del sitio, así como los proceso básicos que deben implementarse; así también el simulador programado tiene una funcionalidad básica que permite ver y analizar el comportamiento básico del sitio y las actividades que un comprador cibernético podría hacer en él.

En la figura 6-2 mostramos la página donde el usuario puede ver y seleccionar las canciones que desee comprar.

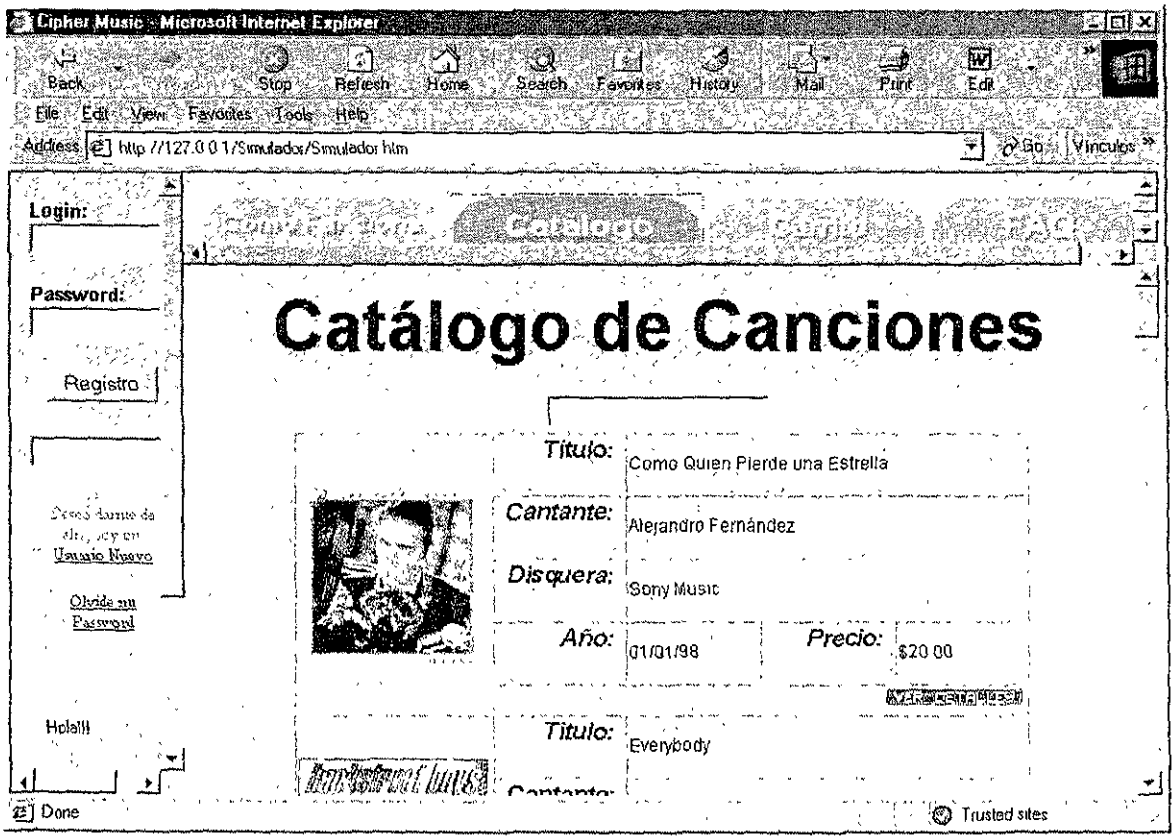
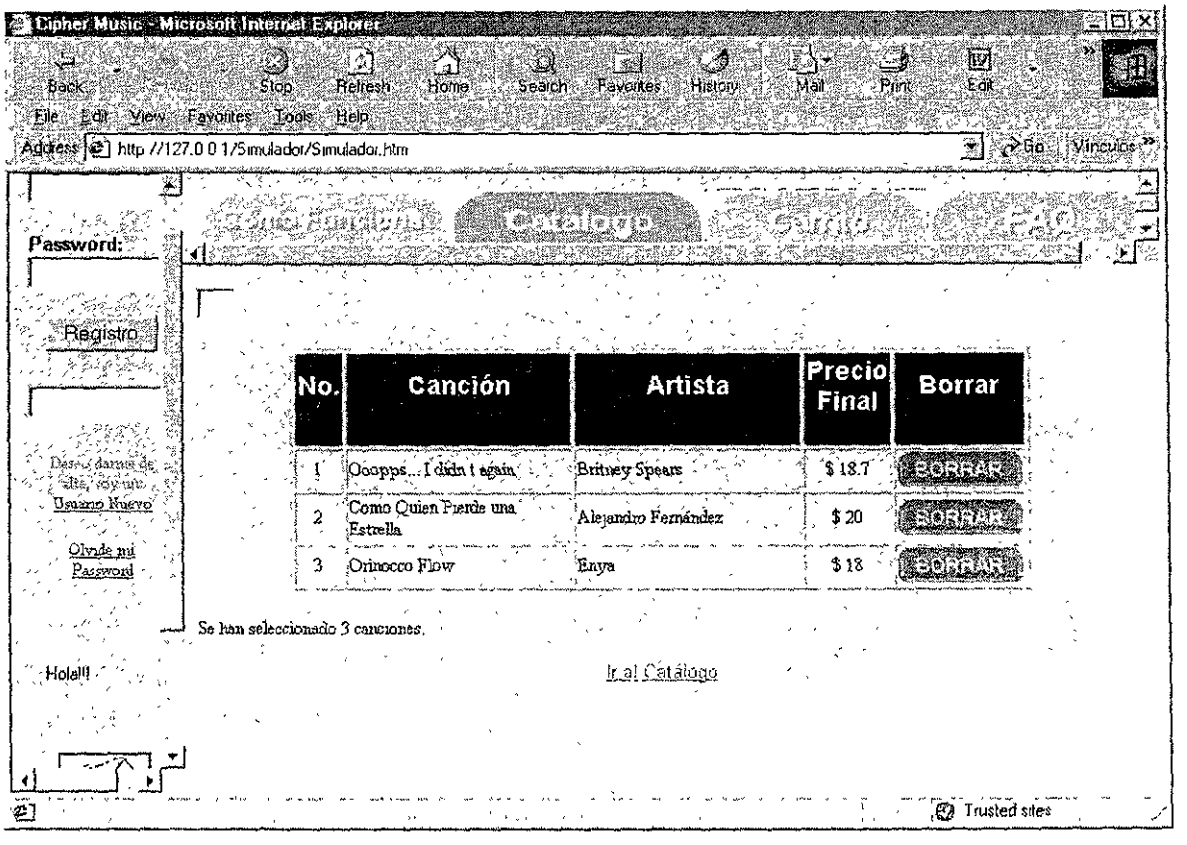


Figura 6-2 Pagina que muestra el catálogo de la Tienda Virtual.

Está página muestra un ejemplo de cómo puede ser la Tienda Virtual, donde el cibernauta entra, se registra, escoge las canciones que le interesan y puede ver con el boton "Ver Detalles" toda la información del bien que desea adquirir antes de comprarlo.

Así también, se construyó la página donde el usuario puede ver su "carrito de compras";en la cual se enlistan todas las canciones seleccionadas por el cliente cibernético y tiene la opción de "quitarlas" antes de enviar su pedido a la Tienda Virtual (Figura 6-3).

Esta página es un buen ejemplo de la necesidad de "interactividad" entre el sitio "Web" y el cibernauta; pues si sólo manejáramos páginas estáticas (equivalente a un sitio que trabajaría a Nivel I, según la clasificación de la sección 2.6 de este documento) se estaría desperdiciando todo el potencial del nuevo medio computadoras-Internet-WWW.



No.	Canción	Artista	Precio Final	Borrar
1	Ooopps...I did n t again	Britney Spears	$ 18.7	BORRAR
2	Como Quien Pierde una Estrella	Alejandro Fernández	$ 20	BORRAR
3	Orinocco Flow	Enya	$ 18	BORRAR

Figura 6-3 Página del "carrito de compras" de la Tienda Virtual

6.5 "CryptoMusicMaker"

Como se mencionaba anteriormente, no se programaron todos los procesos digitales ni se crearon todos los flujos informáticos necesarios para llegar a tener un sitio "Web" con calidad de Nivel III y funcional. Sin embargo, se programaron algunas de las aplicaciones "Web" necesarias y demostrativas de los conceptos que hemos manejado a lo largo de la tesis

El manejar herramientas criptográficas dentro de páginas "Web", a diferencia de aplicaciones para sistemas locales, nos llevó a evaluar muy diversas alternativas (ya que no existe documentación ni ejemplos al respecto) Observando los ejemplos presentados al final del capítulo 5, el 'Cifrador de

Cesar' representa la concepción de crear todo el esquema criptográfico a partir de cero. Tuvimos que programar todo el funcionamiento con Java y JavaScript, y tal vez sea una buena solución pero tiene el inconveniente de ser lenta (sobre todo al implementar un algoritmo robusto como Blowfish, AES, RSA, etc.). Por ello empezamos a recurrir a las herramientas y arquitectura criptográfica ya desarrollada del lenguaje Java, donde el último ejemplo del capítulo 5 muestra el manejo de las herramientas de "hash" (resumen) para mensajes que uno escriba en un campo de la página.

Finalmente, después de mucho análisis y pruebas, se logró ejecutar dentro de un "applet" las librerías de encriptación del JCE de Cryptix. Esto era necesario para crear el ejemplo de la concepción básica del "CryptoMusicMaker", donde una página "web" es usada para encriptar archivos con extensión "***.txt***" utilizando ya sea, un algoritmo de cifrado DES, Blowfish o Rijndael La página HTML se muestra en la siguiente figura:

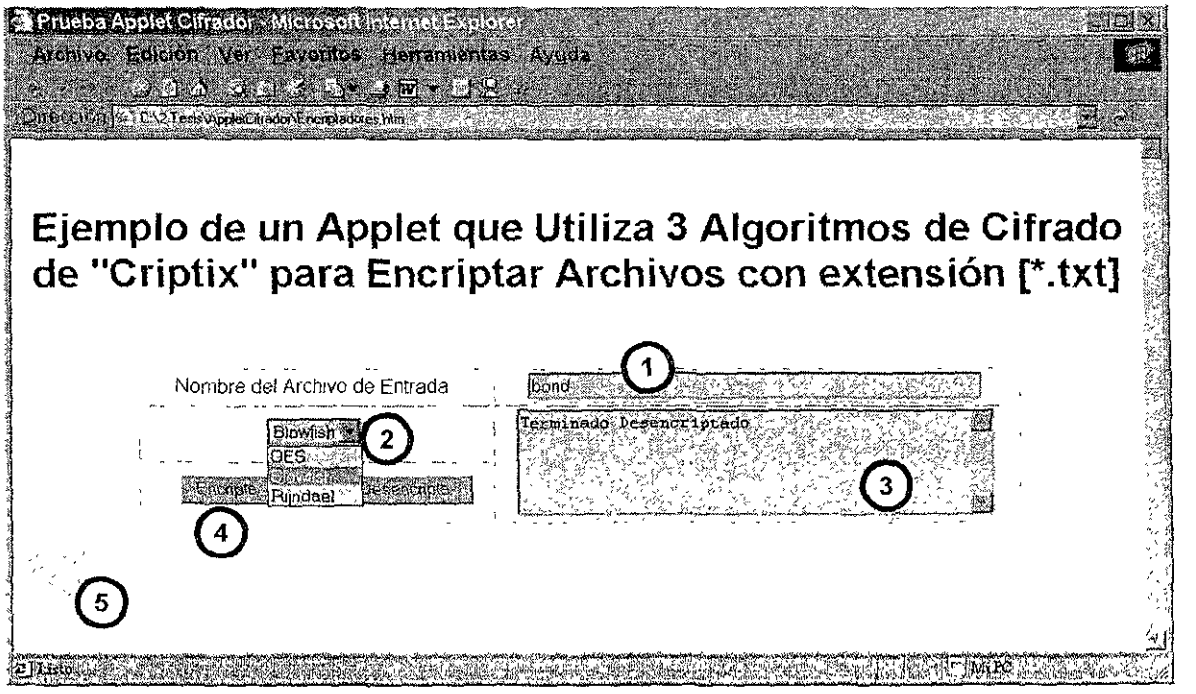


*Figura 6-4. Encriptador de Archivos * TXT*

De acuerdo a la figura 6-4, podemos ver que el funcionamiento de la página es tal y como sigue.

A) Primero, en la caja de texto de entrada (1), se escribe el nombre del archivo que se desea encriptar (sin extensión), sabiendo que este deberá tener extensión ***.txt*** , en realidad, no es necesario que los archivos a encriptar sean de tipo texto, puede usarse cualquier archivo y únicamente será necesario cambiar su nombre o extensión.

B) A continuación se escoge el algoritmo mediante el cual se desea encriptar usando la caja de selección (2).

C) Los botones de "Encripta" y "Desencripta" (4) son disparadores de los métodos de Encriptado y Desencriptado del "applet" (5).

D) Debe hacerse notar que, al finalizar las tareas, el usuario observaría en la ventana de respuestas (3) una serie de mensajes cortos en los que se le informaría de la conclusión de cada una de las tareas Dado que estos mensajes son en algunos casos limitados,

también puede programarse la consola de Java para enviar mensajes de control e informes del progreso del encriptado-desencriptado tal y como se muestra en la figura 6-5.

Aún cuando en este documento no se muestra el código de este ejemplo, las librerías de "Cryptix" permiten configurar también el modo de operación de los algoritmos de encriptación (dado que estamos trabajando con encriptadores de bloque), la longitud en bits de la llave y el relleno o complemento ("padding").

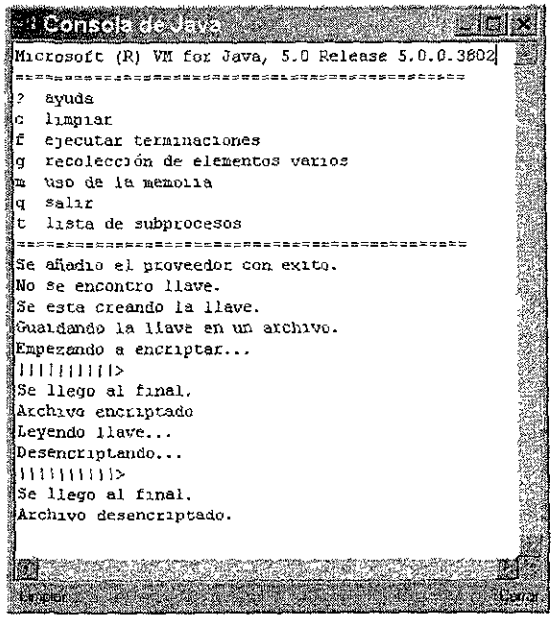
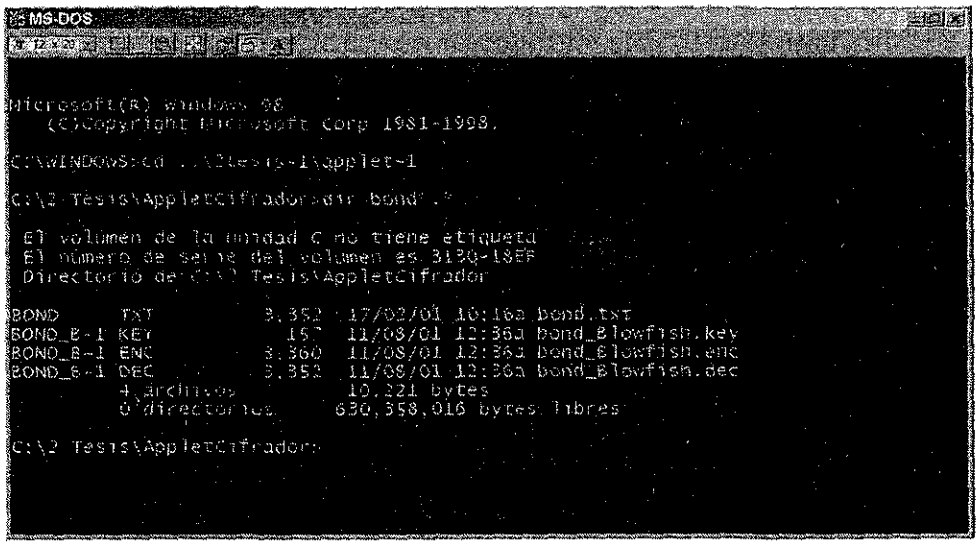


Figura 6-5. Consola de Java con los resultados del encriptado-desencriptado

Puede verse en esta imagen que el primer proceso que debe efectuar el programa es cargar el proveedor de encriptado ("Criptix") para que, a través de él, pueda hacer uso de los algoritmos de encriptado (DES, Blowfish, Rijndael), y el resto de las herramientas criptográficas que maneja este paquete. Ya con el proveedor listo, se verifica la existencia de la llave adecuada. En el caso de que no exista la llave, esta se genera y almacena en el disco duro.

El siguiente paso es precisamente el encriptado (o desencriptado). El resultado final, tal y como se muestra en la figura 6-6, será tanto el archivo original (con extensión ***.txt***), más tres archivos adicionales. El primero de ellos tiene extensión ***.key*** y se refiere a la llave usada por el algoritmo, el archivo encriptado tendrá extensión ***.enc*** , debe hacerse notar que, dado que se efectúa un relleno (padding) el tamaño de este archivo es, por lo regular, algunos bytes mayor que el archivo original. El último archivo se identifica por la extensión ***.dec*** y es el archivo desencriptado.

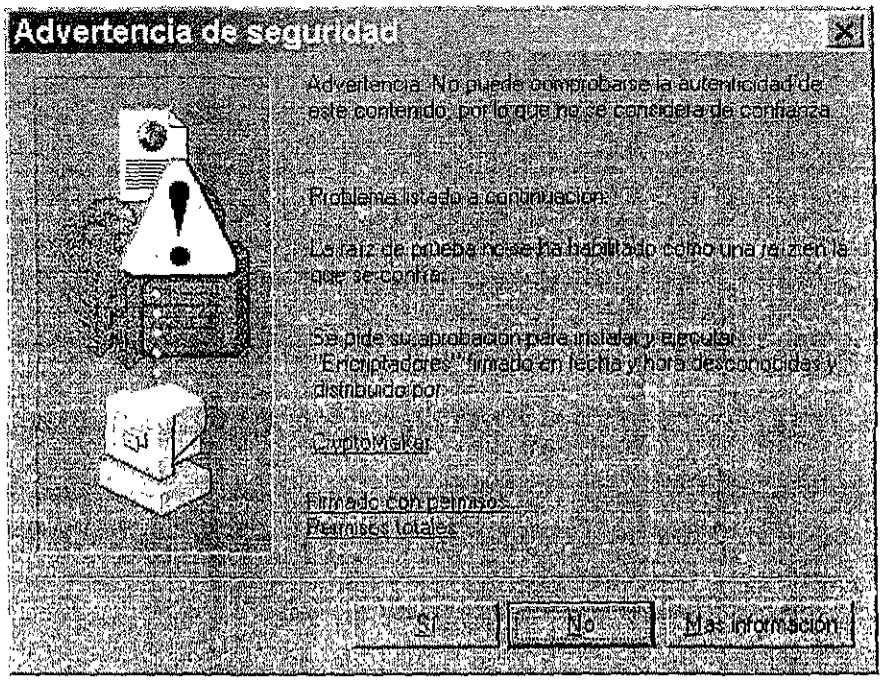
Algo que debe quedar muy claro es que, para efectuar esta simulación, el "applet" debe tener la capacidad de leer y escribir archivos en el disco duro de la máquina local Para dotar al "applet" de los permisos necesarios para efectuar estas operaciones, primero es necesario generar un certificado digital y "firmar" electrónicamente el código que formará parte de nuestro programa Desafortunadamente no existe mucha literatura respecto a la forma en la que deben efectuarse estas operaciones, sin embargo, recomendamos la página de Internet marcada con la referencia [38] de nuestra bibliografía, así como la ayuda en línea del SDK de Java creado por Microsoft [53]



6-6 Terminal de MS-DOS Pueden verse los archivos creados con sus extensiones y tamaño en bytes

Además, el costo de los certificados digitales no es bajo; razón por la cual decidimos autocrear nuestros propios certificados con los cuales trabajamos durante la etapa de desarrollo (el JDK de Microsoft así como el de Sun tienen herramientas propias para crear este tipo de certificados "no legales")

Cuando un usuario cargue la página HTML por primera vez, aparecerá la advertencia mostrada en la figura 6-7



6-7 Certificado Digital

Este mensaje indica que el "applet" que se ejecutará en la página esta diseñado para efectuar operaciones que "pueden ser consideradas peligrosas"; tal como escribir en el disco duro. Por esta razón, si cualquier usuario ve una advertencia similar a ésta al navegar por Internet, deberá estar seguro de que, quien escribió un "applet" con estas características, es un programador de confianza, pues de otra forma, su información puede verse comprometida.

Para entender mejor cuales acciones son consideradas por Java como "peligrosas" es recomendable leer el anexo A "Modelo de Seguridad de Java".

Cuando los sitios en Internet cuentan con este tipo de certificador pero dichos certificados han sido emitidos por entidades comerciales de confianza (tales como Verisign o e-Trust), el certificado se instala en el navegador del cliente de forma transparente. Esto se debe a que, al ser entidades de confianza han establecido de antemano acuerdos y licencias con los productores de "software" (Microsoft, Netscape, etc), de forma tal que los certificados que estas empresas emiten están listos para aplicaciones de comercio electrónico.

6.6 "Crypto Player"

La última aplicación desarrollada fue el "Crypto Player": una aplicación para ejecución en sistemas locales, donde utilizando las capacidades multimedia de la arquitectura Java2, se pudiera ejemplificar el uso de la criptografía para proteger bienes informáticos vendidos a través del comercio electrónico y sujetos a ser atacados por la piratería

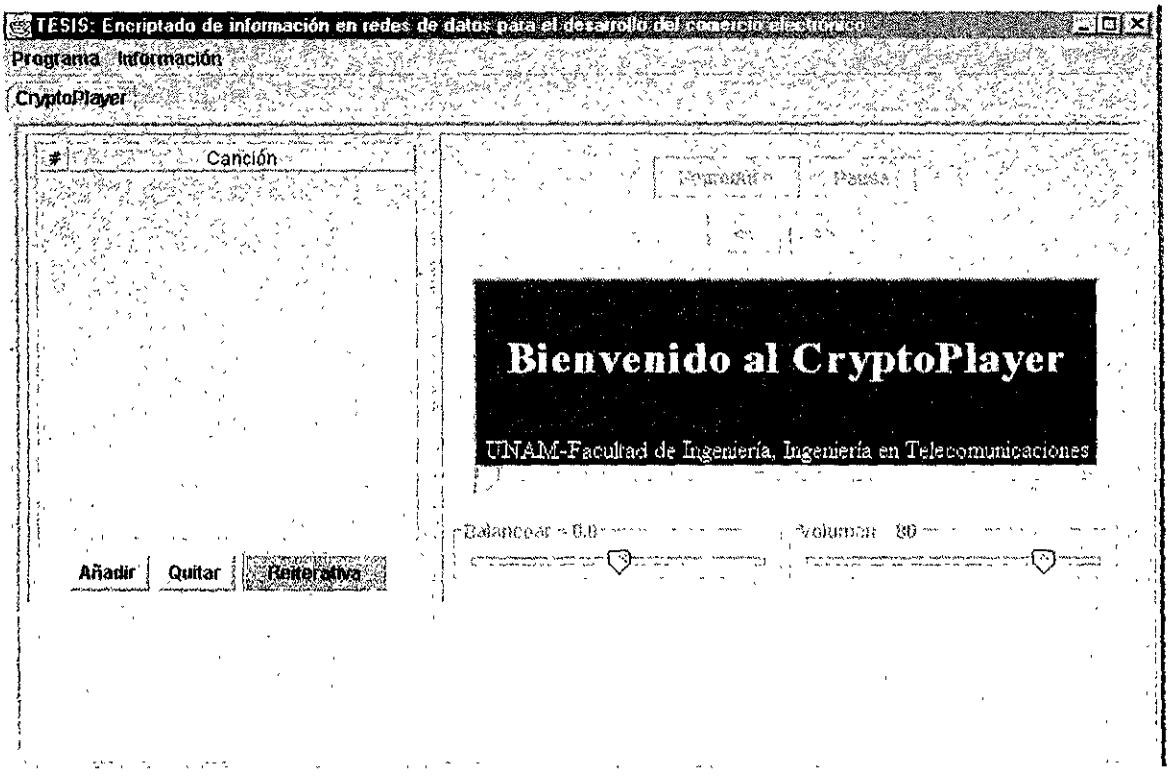


Figura 6-8 Pantalla de bienvenida del "Crypto Player"

Esta aplicación se basa en el ejemplo "JavaSound" provisto en el JDK1 3 edición Estándar de Sun. Únicamente exploramos la parte criptográfica para mostrar como un bien informático protegido criptográficamente solo puede ser utilizado por las herramientas permitidas (véase figura 6-10).

Aunque como mostramos en el modelo teórico propuesto en el capítulo 4, para que dicha aplicación sea comercialmente aceptable, debe manejar "passwords" así como particularizarse al sistema local en el cual se ejecuta. Pero el desarrollo de los procesos de personalización, instalación, particularización a los recursos detectados del usuario, el ocultamiento de información vital en diversos lugares del sistema y la protección propia del "software" contra la piratería; son elementos que salen fuera del alcance del presente trabajo (pueden conformar muy bien otro tema de investigación).

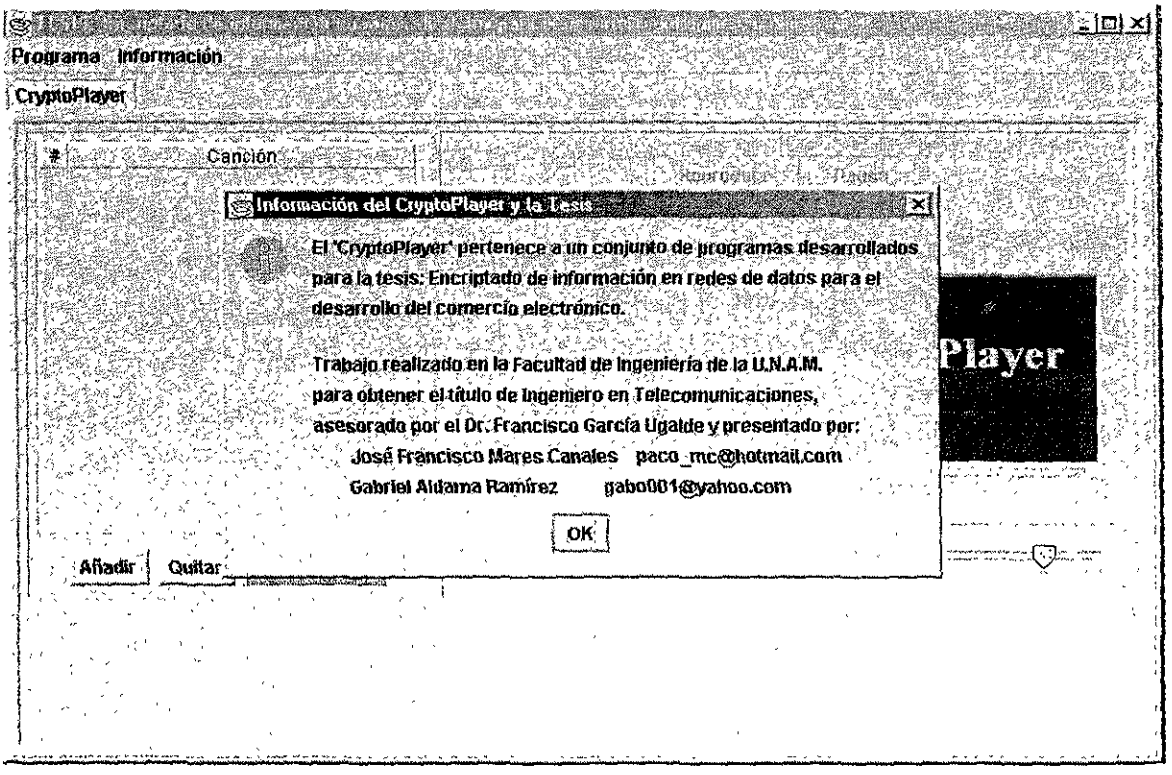


Figura 6-9. Pantalla de información del "Crypto Player"

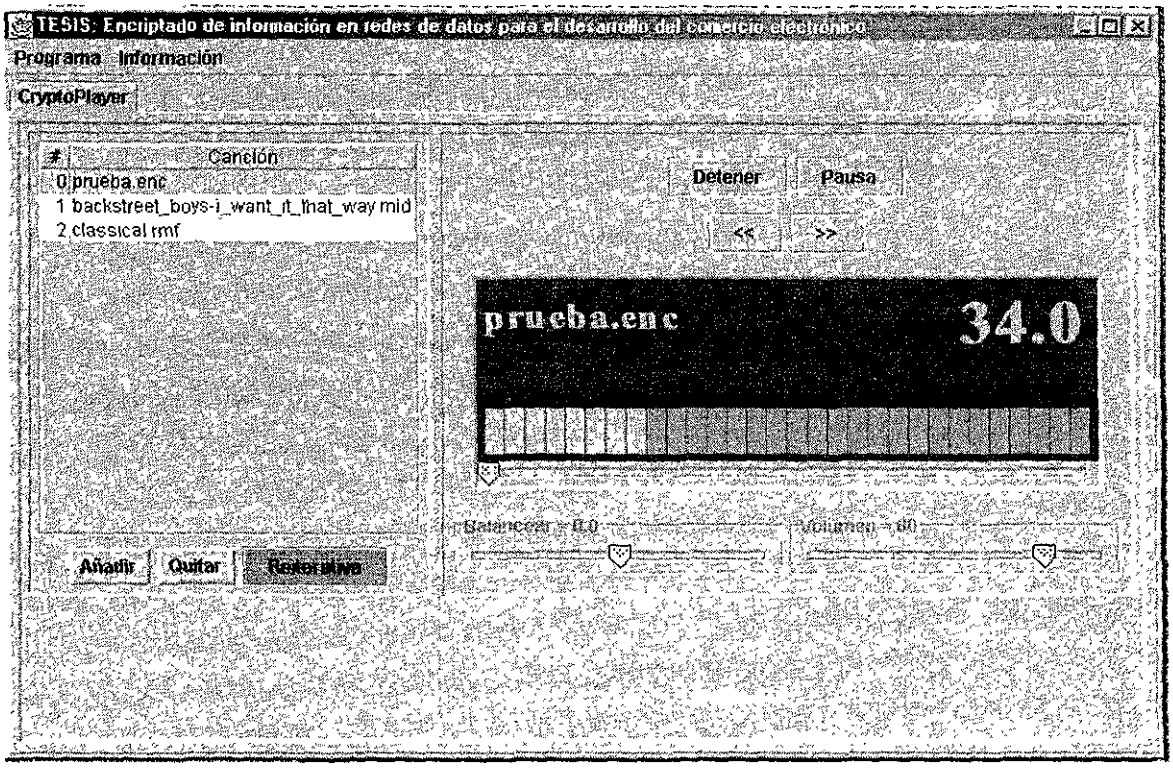


Figura 6-10. Ejemplo de reproducción del "Crypto Player"

Conclusiones

La criptografía se está convirtiendo en una parte esencial de los sistemas de comunicaciones e información de hoy. Ayuda a proveer responsabilidad, imparcialidad, precisión y confidencialidad. A través de ella se pueden prevenir fraudes en el comercio electrónico, validar las transacciones financieras, identificar a nuestro interlocutor o mantener nuestro anonimato. En el futuro, conforme el ámbito de las computadoras y las redes de datos se generalice, la criptografía será más y más vital.

Cada forma de comercio que se ha inventado está sujeta a algún tipo de fraude: el dinero puede ser falsificado, los cheques alterados, pueden robarse números de tarjetas de crédito, etc. Sin embargo, estos sistemas son exitosos debido a que sus beneficios y conveniencias sobrepasan las pérdidas. Los sistemas de seguridad no son perfectos, pero usualmente son suficientes para nuestras necesidades. Un buen sistema criptográfico mantiene un balance entre lo que es posible y lo que es aceptable.

Los esquemas de comercio electrónico presentan alguna forma de falsificación, tergiversación, negación de servicio, o cualquier otro tipo de trampa. De hecho, la computación ha hecho que el riesgo aumente, al permitir ataques antes imposibles. La información, y en especial las malas noticias, se mueven demasiado rápido: una debilidad en seguridad que sea descrita en Internet puede ser aprovechada por miles antes de que se encuentre una solución. Ya es un principio que los sistemas de hoy deben anticiparse a los ataques futuros.

Pero ¿cómo se puede aplicar ese principio? Esta tesis presenta una posibilidad, un mapa de un nuevo territorio en el cual se conjuntan la criptografía y el comercio electrónico. Su creación requirió el estudio y análisis de diversos temas: la información en formato bit, el comercio electrónico, la criptografía, el diseño de páginas y servicios de Internet, y el uso de metodologías y lenguajes de programación para diseñar sistemas informáticos seguros.

Al plantear los objetivos específicos de esta tesis, mostrados en la introducción, logramos acotar el problema. Analizando los resultados obtenidos, podemos afirmar que sí logramos definir el esquema teórico básico para la puesta en operación de un servicio de comercio electrónico seguro (capítulo 4), e incluso diseñar un simulador del sitio "Web" que permite probar el funcionamiento de la compra-venta de canciones encriptadas por Internet (capítulo 5). De igual forma se programó una aplicación que desencripta la canción comprada para reproducirla (capítulo 6). Sin embargo, reconocemos que tanto el sitio "Web" como la aplicación no tienen toda la funcionalidad y automaticidad que hubiéramos deseado (algunas operaciones deben realizarse en forma manual), ya que su utilidad es de carácter demostrativo, y sirvió para validar lo planteado en esta tesis.

El segundo objetivo de la tesis, establecer el marco de referencia en el cual se puedan relacionar las necesidades de seguridad existentes en el comercio electrónico y con los instrumentos para cubrirlas, también fue alcanzado por las siguientes acciones:

- Se sintetizaron criterios para detectar y evaluar los bienes informáticos a proteger, la clasificación de productos finales o productos intermedios mostrada en la sección 2.9.

- Se logró aplicar una metodología (desarrollada por la NSA, Counterpane y DARPA) para diseñar el modelo propuesto como un sistema informático seguro; comenzando su planeación a partir del ciclo de vida de los principales bienes informáticos a proteger. El resultado de este análisis mostró, en las figuras 4-9 a 4-21, que la protección de la información se debe realizar en dos niveles: en el tecnológico, asegurando todas las fases del ciclo de vida, todas las capas del modelo OSI y todos los procesos en los cuales

interactúa; y en el humano, creando las políticas de seguridad y asignando la capacitación y responsabilidades necesarias para asegurar que los usuarios utilicen correctamente un sistema informático seguro.

- Se consiguió establecer una relación entre el tamaño de llave criptográfica a utilizar y el producto informático a proteger en base a parámetros: el tiempo mínimo necesario que debe estar protegido el bien informático, la capacidad de cómputo y la capacidad financiera necesarias para montar un ataque por fuerza bruta según el adversario viable a enfrentar. De igual forma se pudo definir que algoritmo criptográfico a utilizar para cada bien al comparar el trabajo criptoanalítico y velocidad de procesamiento de cada "crypto engine" implementado en el JCE de Cryptix (véase capítulo "Resultados").

- Por último se logró utilizar las herramientas criptográficas del lenguaje Java para poder diseñar las aplicaciones necesarias en las cuales se aplicaron los conocimientos obtenidos con el fin de lograr los objetivos anteriores.

En resumen, al alcanzar el marco de referencia se pudo establecer los componentes básicos de una metodología para el diseño de sistemas informáticos seguros para el comercio electrónico, la cual establece la siguiente guía de preguntas:

1 *¿Qué se va a proteger?* Detectar los bienes informáticos a proteger.

2 *¿Donde se les debe proteger?* Al analizar el ciclo de vida del bien, y de los elementos con los cuales tiene contacto, se detectan los posibles atacantes y los ataques que puede sufrir en las diversas etapas por las cuales debe evolucionar.

3 *¿Con qué se le va a proteger?* Evaluar donde es necesario proteger al bien informático con herramientas criptográficas y donde con herramientas no criptográficas.

4 *¿Contra quien y por cuanto tiempo se debe proteger?* En el caso de usar herramientas criptográficas, y dado que ya se conocen los atacantes; se determinan los algoritmos y la longitud de las llaves necesarias para la protección del bien según las capacidades del agresor y el tiempo mínimo que debe ser asegurado el bien.

Es importante destacar, como señalamos en el capitulo de introducción, que desde el inicio de la presente tesis no se pensó en llegar a uno o varios productos de nivel comercial. Existen factores, detectados en la etapa de investigación documental y comprobados en la etapa de desarrollo, que dificultan la implementación del comercio electrónico·

- La falta de consenso, normalización y documentación; tanto en herramientas, interfaces, y navegadores como en el uso y administración de formas electrónicas.

- La existencia de herramientas y sistemas propietarios que en muchos casos solo tienen compatibilidad con productos de su casa comercial, costo elevado, fallas no detectadas y escasa documentación.

- La vigencia de legislaciones e infraestructuras inadecuadas, que limitan el uso y comercialización de herramientas criptográficas o restringen todas las actividades y bienes posibles en el nuevo medio computadoras-Internet-WWW y el comercio electrónico.

- La existencia de lagunas conceptuales en la aplicación tanto de la criptografía así como del comercio electrónico

Aún con todos los factores adversos detallados arriba, se cumplió con el compromiso propuesto en la tesis, al administrar los recursos disponibles (los conocimientos y experiencia del director de

tesis así como el de los dos alumnos que dedicamos tiempo completo al proyecto, ahorros y becas de Probetel, algunas computadoras personales y una conexión de alta velocidad de Internet) y al usar "software" de uso y distribución gratuita (los JDK de Sun y Microsoft, los JCE libres de Cryptix y Bouncy Castle, el uso de Linux y el PWS de Microsoft para máquinas Windows 9x, así como el acceso a las bibliotecas y foros digitales de las comunidades de "hackers" y "crackers").

También consideramos que la visión general y conceptos sintetizados en el presente documento forman un mapa de lo que es el nuevo territorio en el cual se debe proteger la información usada para comprar, recrear, sociabilizar, conocer, comunicar ideas, etc. en el nuevo medio. Mapa que puede servir como base para crear un proyecto de mayor envergadura, constituido por varios proyectos de tesis en los cuales se requerirán ingenieros en telecomunicaciones, computación y electrónica así como interactuar con especialistas de leyes, mercadotecnia, publicidad y comunicación social; al establecer un punto de partida para futuros trabajos (mapas más detallados) sobre las siguientes áreas y temas:

Encriptación:

- Como se menciona en el capítulo 3, la legislación de EE.UU. ha limitado a las empresas de dicho país a exportar sus productos criptográficos; y en general, la expresión del conocimiento e información en ésta área. Razón por la cual existe un gran vacío que reclama metodologías de aplicación así como productos en "software" y "hardware" para una sociedad que esta asimilando rápidamente la información en bits en su vida diaria. Detectamos que es muy importante empezar a desarrollar metodologías de aplicación de la criptografía (esta tesis es muestra de una de ellas) así como del criptoanálisis, las cuales nos conducirán a metodologías para desarrollar "software" y / o "hardware" criptográfico seguro, y en general, aplicaciones e infraestructuras informáticas seguras.

La necesidad de estas metodologías irá creciendo, porque un producto puede manejar un buen algoritmo criptográfico con una gran llave; pero cualquier falla de la implementación compromete la seguridad del sistema. Los compradores y usuarios de dichos productos requieren saber como detectar dichas fallas, y en el peor de los casos, las "puertas traseras" que puedan existir en productos como los de Crypto AG[1].

Además, en la actualidad, muchos sistemas son diseñados tomando a la criptografía tan sólo como "un componente más", cuando esta visión es incorrecta. Para que un sistema criptográfico funcione, es necesario ponerlo en operación como un sistema completo e integrado. Cada año, miles de millones de dólares son desperdiciados en productos inseguros, que presentan serias deficiencias o huecos que no han sido corregidos. Más aún, cuando estos malos productos son ampliamente utilizados, se vuelven un blanco fácil para los criminales. Empeorando esta situación

[1] Crypto AG llegó a ser una de las empresas privadas de criptografía más importantes del mundo. Su negocio es la venta de máquinas que protejan las comunicaciones de políticos, diplomáticos, empresas y de cualquiera que desee mantener su información a salvo de las orejas de husmeadores como la National Security Agency (NSA) de EE.UU. El autor de su éxito es Boris Hagelin, un sueco nacido en Rusia que fabricó equipos de codificación para los militares norteamericanos durante la Segunda Guerra Mundial. La gratitud del Tío Sam se expresó en grandes sumas de dinero que él invirtió en su negocio en Suiza Durante su residencia en EE.UU., Hagelin entabló una firme amistad con el criptólogo William Friedman, futuro alto funcionario de la NSA. Fue éste quien en 1957, le propuso a Hagelin una propuesta asombrosa: la NSA quería que Crypto AG creara una puerta trasera en cada aparato que vendía para poder leer todas las comunicaciones que lo atravesaban. Varios ex empleados han confesado que Crypto AG sí arreglo todos los aparatos que vendió desde ese momento en adelante. Durante treinta cinco años la NSA no tuvo que hacer grandes esfuerzos para conocer las comunicaciones secretas de los clientes de Crypto AG, una lista que incluía a Irán, Irak y la entonces Yugoslavia Fue el gobierno de Teherán quien detectó esta puerta trasera en 1992, exponiéndose a la luz pública el fraudulento hecho.

el hecho de que muchos errores de implementación no son estudiados en la literatura científica debido a que los académicos no tienen interés en la parte técnica y los técnicos carecen de la formación matemática. Por ello, la única forma en la que se puede aprender a prevenir estos errores es rompiendo sistemas una y otra vez, y documentando los resultados para crear las metodologías correspondientes.

La buena noticia acerca de la criptografía es que en este momento se tienen los algoritmos y protocolos que se necesitan para asegurar cualquier sistema informático. La mala noticia es que ésta es la parte sencilla, poner en operación los protocolos satisfactoriamente requiere una experiencia considerable. Mientras que los criminales informáticos sólo tienen que encontrar una debilidad en la seguridad para comprometer todo un sistema, los encargados de la seguridad tienen que defender cada vulnerabilidad posible. Las compañías por lo regular escogen bien la parte fácil (protocolos y algoritmos robustos), pero fallan al poner en operación los sistemas, dando como resultado entornos de trabajo inseguros globalmente. El mejor protocolo puede fallar sino se pone atención a su complejidad al momento de ponerlo en operación. La seguridad es una cadena y el romper un eslabón (el más débil), compromete a todo el sistema.

Redes:

- En el análisis de herramientas necesarias para un sistema de comercio electrónico seguro (capítulo 4), se puede ver la necesidad de implementar canales de comunicación segura a través de Internet. Aunque el presente trabajo no implementó dicho elemento de seguridad, se puede trabajar en él como tema de tesis ya que Java ofrece la extensión JSSE (y existe un desarrollo libre llamado OpenSSL) para implementar canales seguros de comunicación. Nosotros realizamos pruebas básicas con el JSSE de Sun, y podemos afirmar que sí funciona. Este tema requiere el manejo de certificados digitales y la programación de "sockets", lo cual implica ya un tema de tesis especializado.

- Otro tema importante es el uso de "firewalls" y sistemas detectores de intrusos. Como se puede ver en el capítulo 4 del presente documento, estas herramientas no criptográficas son fundamentales en la seguridad de la red de toda empresa (micro, chica, mediana o grande). Puede ser un buen tema de tesis evaluar los diferentes productos existentes en el mercado, o bien, como se puede diseñar y mejorar estos sistemas con nuevas arquitecturas de "hardware", nuevos algoritmos de búsqueda de patrones, de análisis, etc.

- Como último tema, cabe la posibilidad de utilizar la metodología de diseño de sistemas informáticos seguros que se utilizó en esta tesis, y aplicarla y mejorarla para el diseño de redes seguras de datos. Como se mencionó anteriormente, nuestro trabajo dio un mapa inicial, pero es necesario crear mapas más especializados; y este puede ser de gran utilidad porque es poca la información sobre esta subárea específica.

Comercio Electrónico:

- Crear portales para atender a gran cantidad de usuarios. En esta tesis se utilizó Windows 9x y el PWS de Microsoft, con una capacidad máxima de atención de 30 usuarios; pero si se quiere tener una solución comercial es necesario manejar Windows NT con IIS (aunque por la información en la comunidad "hacker" y "crackers", son muchas las fallas de seguridad de la arquitectura Microsoft) o manejar servidores Web con Linux. Levantar un servidor "Web" seguro para el comercio electrónico se puede convertir en un tema de tesis.

- Un tema muy ligado al anterior es el desarrollo del sitio comercial. En este trabajo se utilizaron los lenguajes Java, JavaScript, HTML, DHTML y ASP; para programar las páginas e interfaces necesarias para el Internet Explorer de Microsoft. Sin embargo, aunque por el momento este es el visualizador más popular, es necesario buscar como implementar dicho sitio tanto para otros navegadores de computadoras personales como HotJava y Navigator; así como para las nuevas generaciones de teléfonos celulares que ya

comienzan a tener capacidad de "browser" para Internet. No es conveniente "casarse" con una sola marca ni menospreciar los alcances de la comunicación móvil; y como describimos en un párrafo posterior, cada marca de navegador tiene sus características propias de seguridad que uno debe desentrañar y entender, antes de usarlas.

- Otro tema de interés en esta área, es el manejo de la publicidad y la mercadotecnia en el nuevo medio. Requerirá la interacción entre estudiantes de diferentes facultades, pero sería conveniente realizar esta investigación dado que se pueden crear nuevas teorías y perfiles de las comunidades virtuales, cibernautas, compradores electrónicos particulares o empresariales, etc.

- De igual forma, las bases de datos utilizadas por nosotros fueron hechas con Access y tampoco ofrecen gran capacidad; por lo cual se recomienda hacer desarrollos con bases de datos que permitan miles de consultas y puedan manejar gran cantidad de información. Ejemplos pueden ser SQL u Oracle.

- Un tema de importancia es el de desarrollar metodologías para crear los procesos digitales informáticos necesarios para aprovechar todas las ventajas del comercio electrónico. Es poca la información existente, por lo cual se convierte en un campo adecuado a las nuevas ideas.

- Investigamos el actual sistema bancario mexicano, véase anexo B, y detectamos la carencia de los sistemas de "pago a terceros en tiempo real de cuentas de diferentes bancos". Este tipo de pago es necesario para que el comprador cibernético pueda disponer inmediatamente del producto comprado, ya que el sistema actual utilizado retrasa el término de la operación de compra-venta por varias horas. Es necesario estar en contacto con el sistema bancario mexicano, pues ya esta en vías de desarrollo el sistema de pagos mencionado. Sin embargo, puede ser un tema de tesis el desarrollar un modelo de cómo pudiera funcionar interna y externamente dicho sistema de pagos (dentro de un banco, entre bancos de la misma nación y entre bancos de diferentes naciones), concepto conocido como "e-banking"; y como punto de inicio se puede utilizar la noción de "crypto engine de autorización" que fue mostrado en la presente tesis.

- La ciencia de las leyes da dos temas importantes: Las implicaciones legales de comerciar con habitantes de diferentes naciones, ya que el comercio electrónico salta las limitaciones geográficas y las leyes circunscritas a dichas fronteras. El otro tema, la validez de las herramientas y los documentos electrónicos utilizados en el comercio electrónico.

  En el caso de México, el 29 de abril del 2000 se concretaron algunas reformas legales que empezaron a asentar el marco legal para el comercio electrónico. Actualmente las empresas y los usuarios ya tienen plena seguridad en la oferta de los productos y servicios comercializados a través de la WWW, pues ya se le otorgó el carácter de acto jurídico a las operaciones comerciales hechas a través de medios electrónicos; con ello, se reconece plenamente el uso de medio electrónicos para la realización de actos comerciales, así como las características inherentes a este proceso: ejecución y regulación de los actos mercantiles, validez de los datos transmitidos y de los medios utilizados para ello y expresión de la voluntad de las partes. Aún no se ha otrogado validez jurídica y fiscal ni a la firma electrónica ni a la factura electrónica, paso muy necesario para simplificar los procesos (rediseñar aquellos conceptualizados en el uso del papel) y cerrar el círculo del comercio electrónico en nuestro país. En especial, no se ha definido claramente los elementos básicos de la factura electrónica, y menos, los mecanismos de protección necesarios; necesidad claramente detectada en el diseño del sistema de comercio propuesto en esta tesis, y por lo cual ya no se profundizo a detalle.

Dada la novedad y nuevos alcances que abarcan los temas anteriores, es probable que aquellos estudiantes que desarrollen los temas anteriores puedan encontrar más factores adversos a los que nosotros detectamos y mostramos en esta sección. A continuación resumimos los problemas y soluciones más importantes, ocasionados por dichos factores, a los cuales nos enfrentamos:

- El primer gran problema al cual nos enfrentamos fue que el JCE de Sun no podía ser descargado de su sitio, por la Ley de Armas y Municiones de EE.UU. (las herramientas criptográficas están consideradas como armas por dicha legislación). Por ello debimos recurrir a buscar JCEs alternativos, encontrando el de Cryptix y Bouncy Castle. Pero el segundo presentaba muchos problemas de implementación (que ya fueron corregidos en su nueva versión 106) por lo cual decidimos usar el primero. Cryptix presenta una buena implementación pero es muy escasa su documentación para instalarlo, en especial porque la poca que existe se enfoca más a los sistemas UNIX y hablan poco de los posibles problemas o "peculiaridades" de Windows. Además, sus programas ejemplo y de prueba están escritos para la versión antigua (la 3.2.0), lo cual nos llevo a rediseñar el código para poder utilizarlo con la nueva versión. Desgracidamente estas actividades tomaron bastante tiempo, y es probable que quien use JSSE u OpenSSL se enfrente a situaciones parecidas. Como dato importante, al navegar por las comunidades de "hackers" y "crackers" es posible conseguir el JCE de Sun.

- Es escasa la documentación sobre estos temas, en especial sobre un área muy especializada como la criptografía aplicada a Internet. Y la poca que existe, a veces es confusa o incompleta. En el caso particular de Microsoft, el modelo de seguridad de Java que esta casa de "software" utiliza es conceptualmente igual al de Sun; pero difiere a nivel funcional. Encontrar como hacer que un "applet" encriptará con las librerías de JCE requirió analizar el funcionamiento interno del navegador Internet Explorer, buscar parches que nos permitieran hacer el puente entre el modelo de seguridad de Sun y el modelo de seguridad de Microsoft, muchas pruebas que consumieron casi 2 meses de tiempo, así como el estudio de los permisos propios de Jscript (porque se encontró que la "Jscript engine" es un "engine" separado de la JVM, dentro del propio Internet Explorer) así también los permisos necesarios para que un "applet" tuviera acceso a archivos en un disco duro de un cliente remoto. Además, las páginas del sitio comercial desarrolladas con DHTML y ASP, sí son "vistas" correctamente por el navegador de Microsoft; pero al usar los de otras marcas, se muestran bastantes fallos.

- La metodología utilizada para el diseño de sistema informáticos seguros es muy laboriosa de aplicar Requiere analizar profundamente el bien informático a proteger, y si se aplica rigurosamente, se debe realizar este análisis a todos los componentes de todo el sistema. Consume demasiado tiempo porque se debe analizar cada fase del ciclo de vida del producto o servicio, así como las relaciones del bien informático con cada "ente" o componente que contacta; y se deben hacer varias iteraciones para detectar los principales atacantes, sus capacidades, las debilidades del sistema, los posibles puntos de ataque, así como las defensas a usar. Además, como utiliza una estructura de árbol (de matemáticas discretas) se corre el riesgo de no desarrollar correctamente las ramas o desarrollarlas demasiado. Como se observa en la figura 4-9 del capítulo 4, se definieron los niveles 0-4 de la estructura de árbol para contemplar todo el proceso de análisis realizado.

- El desarrollo del sitio comercial fue lento, en parte por falta de experiencia y en parte por algunas lagunas o incompatibilidades en los propios lenguajes. También, se llegó a probar una herramienta llamada "eBuilder" para el desarrollo del sitio de comercio electrónico; ésta generaba un buen resultado en páginas estáticas; pero no es muy recomendable para el desarrollo de sitios que deban ser interactivos con el cliente y mostrar la información dinámicamente.

Una reflexión importante al diseñar: en nuestra labor de ingenieros siempre debemos considerar el factor humano en nuestros diseños; más en el nuevo medio computadoras-Internet-WWW, donde se refleja y amplía la naturaleza humana.

En este nuevo terriotorio muchos sistemas son rotos por la gente que los usa. Muchos fraudes en sistemas comerciales son perpetrados por personas que están dentro de la organización. Además, en ocasiones los usuarios honestos pueden causar problemas porque ellos usualmente no tienen cuidado acerca de la seguridad. Ellos buscan simplicidad, conveniencia y compatibilidad muchas veces inclusive con sistemas inseguros. Estos usuarios escogen malos "passwords", los escriben en papelitos y dan sus datos personales a amigos y compañeros de trabajo; dejan su computadora encendida, etcétera.

Usualmente, la parte más difícil de la criptografía es convencer a la gente de que la use (crear las políticas de seguridad necesarias, así como dar la capacitación y las responsabilidades pertinentes). La seguridad es rutinariamente pasada por alto por oficinistas, gerentes y ejecutivos. Sólo cuando la criptografía es diseñada con cuidado y de acuerdo a las necesidades de los usuarios, esta podrá proteger sistemas, recursos y datos.

La historia nos demuestra que nunca se debe subestimar el gasto en dinero, tiempo o esfuerzo cuando de seguridad se trata. Siempre deberá asumirse lo peor: que el adversario es mejor de lo que realmente es; que la ciencia y la tecnología muy pronto serán capaces de realizar cosas que antes ni siquiera hubieran imaginado. El permitirse un margen de error en el diseño implica un poco más de seguridad de lo que realmente se necesita. Cuando lo inesperado ocurra, se estará preparado.

Y como conclusión final: el trabajo en equipo y el intercambio de ideas fue el factor clave para la realización del presente trabajo. Dada la enorme cantidad de información que se debió buscar, leer, entender, correlacionar, programar, probar y resumir; resalta el hecho de que para un proyecto grande es necesario que lo realice un equipo de personas. Además, las ideas, avances y el desarrollo que en estas páginas plasmamos; se apoyan en el trabajo de varios grupos humanos (los desarrolladores de Cryptix, Sun, Microsoft, así como las comunidades de "hackers" y "crackers") quienes, día a día, construyen el nuevo medio donde ya no estaremos tan limitados en tiempo y en espacio, aprovechando lo construido para mejorar e innovar.

Anexos

Anexo A: El modelo de seguridad de Java

Java fue diseñado para crear applets Java. Los applets Java permiten que el código pueda ser descargado directamente en un navegador Web. Esta tecnología fue una de las primeras en convertir un navegador "Web" en la infraestructura que soporta la ejecución de una aplicación cargada desde la "Web". Dicha infraestructura promete un nuevo paradigma en la informática diferente a la computación tradicional enfocada a equipos aislados. En la computación de equipos aislados, las aplicaciones son cargadas y ejecutadas por el usuario y su máquina. Cuando el usuario necesita realizar actualizaciones de la aplicación, primero se deben obtener dichas distribuciones de fuentes como CD o disquetes; para después realizar la actualización. Los applets Java permiten un nuevo paradigma en el cual el código móvil es descargado dinámicamente al navegador "Web" y automáticamente actualizado cada vez que uno revisita el sitio web del cual el código fue descargado.

Al navegar en Internet y acceder a un sitio "Web", el navegador trae una página la cual contiene un applet, el cual automáticamente se ejecuta en la máquina del cliente (navegante). Idealmente, la ejecución de dicho applet no debe afectar el funcionamiento y/o archivos de la máquina cliente (navegante); pero la realidad es otra: existe el **código malicioso** o **maligno**.

Para tener una idea clara de la naturaleza del código maligno, se presentan los siguientes ejemplos:

1. Un applet podría presentar fotografías obscenas, consignas políticas o ideológicas en la pantalla; o reproducir ruidos irritantes por el sistema de sonido del equipo.
2. Al tener acceso al sistema de archivos del navegante, se tiene un atentado contra el mismo si un applet puede: llenar el disco duro con archivos basura; borrar, dañar o encriptar dichos archivos sin el consentimiento del usuario.
3. Y si el código maligno tiene acceso al sistema de archivos y la capacidad de usar los servicios de comunicación, podría leer información personal del usuario (correo electrónico almacenado, contraseñas, documentos) y enviarlos por un flujo o por correo a través de Internet.

Los diseñadores de Java, conscientes de estos problemas, erigieron una serie de barreras y sistemas defensivos para conformar el **modelo de seguridad de Java**.

Un texto que trata a profundidad la seguridad en Java es [12].

A.1 Modelo de Seguridad y Evolución

Como primera defensa y presente en toda versión, fue que Java tuviera el carácter de un lenguaje seguro respecto a los tipos de datos y su manejo:

- especificaciones detalladas de los tipos de datos que puede manejar;
- arreglos verdaderos con verificación de límites;
- no tiene o maneja apuntadores a memoria.

Estas restricciones hacen imposible que un programador usando Java pueda acceder a localidades arbitrarias de memoria para leer, escribir o cambiar información; o pueda realizar **sobreflujos** ("overflows") que dañen al sistema operativo del equipo para ganar privilegios.

Pero existe el hecho de crear o modificar un compilador de lenguaje C para producir códigos Java, por lo cual se anulan las salvaguardas proporcionadas por el lenguaje y el compilador Java. Por dicha razón, el modelo de seguridad cuenta con otras defensas, las cuales han ido evolucionando en las diferentes versiones de Java.

A.2 Java 1.0

La versión 1.0 de Java, provee un modelo de seguridad muy limitado conocido como **caja de arena** ("sandbox"). En este modelo de caja de arena, únicamente el código local tiene acceso a todos los recursos valiosos (archivos y nuevas conexiones a red) disponibles para la **Máquina Virtual Java** ("Java Virtual Machine", JVM). El código descargado de fuentes remotas, como los applets, únicamente tienen acceso a un número limitado de recursos. Por lo cual, el acceso al sistema de archivos y la capacidad de crear nuevas conexiones estaban limitadas para el código remoto.

Así fue la concepción de las primeros JVM's implementados en los navegadores.

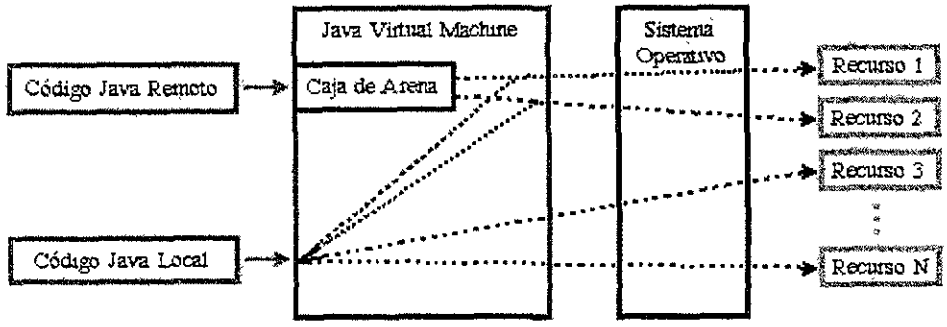


Figura A-1. Modelo de seguridad de Java 1 0

A.3 Java 1.1

El modelo de seguridad de Java 1 0 fue demasiado restrictivo. La visión de proveer aplicaciones descargables de la Web se trunco debido a que dichas aplicaciones no podían realizar operaciones fundamentales como el acceso a archivos o la creación de nuevas conexiones a red. Si los fabricantes de navegadores Web trataban el código remoto como código local, se abría camino para que código remoto malicioso pudiera corromper la máquina local. Por lo cual un paradigma de todo o nada se implanto en Java 1.1 al emplear un modelo de seguridad **basado en la confianza** o **de código confiable**.

Con el modelo de código confiable, el usuario puede designar a que código firmado, rúbrica de ciertos proveedores, se le permite tener el acceso total a los recursos. Por lo cual, uno puede confiar en ejecutar determinado código Java de la compañía X con acceso total a los recursos del sistema, tanto como uno puede confiar en la compañía X. La firma del código o applets le permite a una compañía X firmar sus aplicaciones de tal forma que uno puede verificar que dicho código realmente provienen de dicha empresa. Consecuentemente, a un applet firmado se le garantiza el acceso a todos los recursos de un sistema; mientras que los códigos desconfiables se le confina a la caja de arena

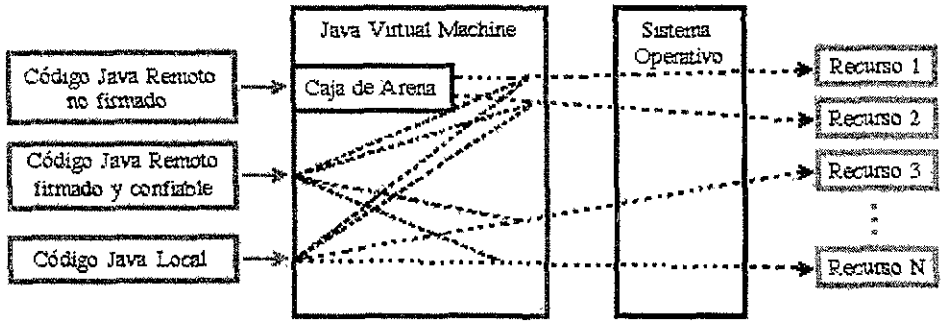


Figura A-2. Modelo de seguridad de Java 1.1

A.4 Java 2

A partir de la plataforma Java 2 (versión Java 1.2) se ha reforzado la seguridad de las aplicaciones con un modelo de seguridad de **"grano fino"** o **granular** o **configurable**. Ahora los códigos remotos y locales pueden ser confinados a utilizar únicamente dominios de recursos de acuerdo a políticas configurables. Por lo cual, algún código Java de la compañía X esta limitado a acceder a los recursos de un dominio definidos por una política específica, mientras que el código Java de la compañía Z sólo puede tener acceso a un conjunto de recursos delimitado por otro dominio.

Los dominios de acceso y las políticas de seguridad configurables hacen más flexible a la plataforma Java 2. Además se libera a los desarrolladores de la tarea de marcar a un código como local o remoto, por lo cual se permiten soluciones más extensas a los problemas de seguridad de aplicaciones Java; en lugar de enfocarse únicamente en problemas de seguridad de código móvil y applets Java.

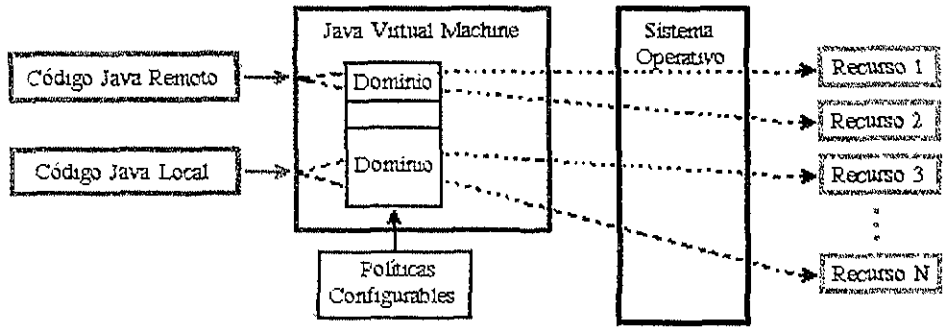


Figura A-3. Modelo de seguridad de Java 2

A.5 La arquitectura de seguridad de Java 2

Se describirá únicamente la arquitectura de seguridad de Java 2 debido a que dicha plataforma (actualmente formada por las versiones Java 1.2 x, Java 1 3 x y Java 1.4 beta de Sun), es la que se encuentra en uso

En la siguiente figura se muestran los principales componentes del conjunto de API's y mecanismos usados para proveer seguridad a las aplicaciones basadas en Java 2. En la parte inferior del diagrama se encuentra la **Arquitectura Esencial de Seguridad Java 2** ("Core Java 2 Security Arquitecture") y la **Arquitectura Criptográfica Java** ("Java Criptography Arquitecture", JCA); las cuales en conjunto forman la plataforma de seguridad de Java 2. En la parte superior del diagrama están las extensiones de seguridad Java, las cuales se comercializan por separado de la plataforma Java 2 pero son dependientes de ella.

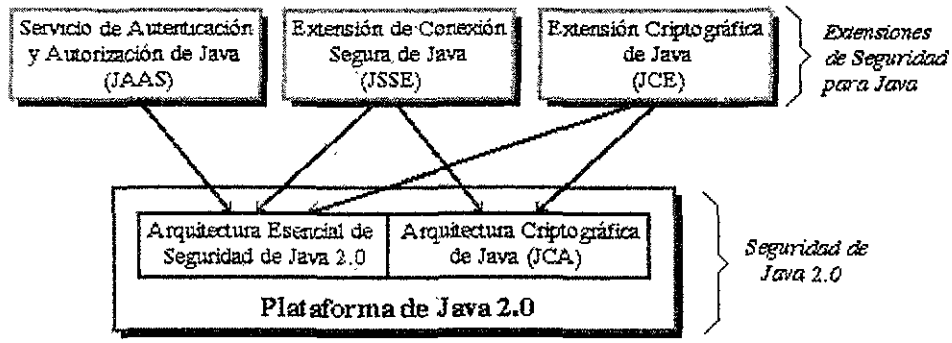


Figura A-4. Arquitectura de seguridad de Java 2

A.6 Arquitectura Esencial de Seguridad Java 2

La siguiente figura muestra la **Arquitectura Esencial de Seguridad Java 2** dentro del contexto de la plataforma Java 2, el sistema operativo, recursos del sistema y el código java corriendo sobre la plataforma Java 2. Las piezas que forman esta arquitectura son: **el verificador de código byte**, el **cargador de clases**, el **administrador de seguridad**, el **controlador de acceso**, los **permisos**, las **políticas** y los **dominios de protección**.

El **verificador de código byte** ("byte code verifier") verifica que los códigos bytes cargados desde una aplicación Java externa a la plataforma Java se adhieran a la sintaxis de la especificación del lenguaje Java. Es decir, se buscan intentos de fabricar apuntadores, ejecutar instrucciones o llamadas a métodos con parámetros no válidos, uso de variables antes de inicializarlas, etc.

El **cargador de clases** ("class loader") es el responsable de la traducción de los códigos bytes en constructores de clase Java que pueden ser manipulados por el **ambiente en tiempo de trabajo** ("runtime environment") de Java. Dentro del proceso de carga de clases, diferentes cargadores de clases pueden utilizar diferentes políticas para determinar cuando una clase especifica podría ser cargada por el ambiente de tiempo de trabajo. El cargador de clases y las clases (al tener incrustadas sus propias medidas de seguridad) de la plataforma Java 2 por sí mismos limitan el acceso a los recursos valiosos al interceptar las llamadas hechas al API de la plataforma Java y delegan al **administrador de seguridad** ("security manager") las decisiones sobre si dichas llamadas finalmente se deben ejecutar, o mostrar una pantalla en la cual se avise que un applet intenta una acción que viola las reglas de protección.

Todo esto se debe a que las clases pueden cargarse sobre la marcha de la ejecución del código, existiendo el peligro de que un applet cargue una de sus propias clases para reemplazar una clase nativa de la plataforma, logrando pasar las verificaciones de seguridad. Este ataque, denominado "ataque de caballo de Troya", se imposibilita debido a que cada clase tiene su propio espacio de

nombres (un tipo de directorio abstracto), y el cargador de clases siempre carga las clases nativas del sistema antes de cargar una clase de usuario.

Java 1.0 y 1.1 utilizan exclusivamente al administrador de seguridad para realizar dichas decisiones, mientras que las aplicaciones Java 2 pueden usar el **controlador de acceso** ("access controller") para realizar decisiones más flexibles y un control configurable de acceso. Finalmente, la ejecución del código no sería posible sin la **máquina de ejecución en tiempo de trabajo** ("runtime execution engine").

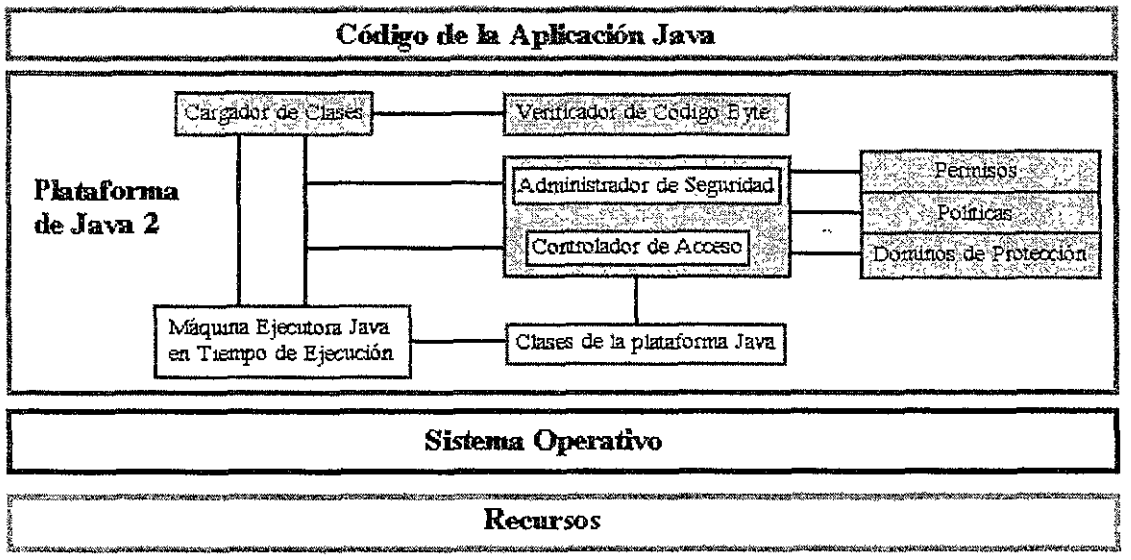


Figura A-5. Arquitectura esencial de seguridad de Java 2

El **control de acceso** es la adición más significativa en la plataforma de seguridad de Java 2, ayudando a extender el modelo de seguridad a un control configurable y acceso granular. Los **permisos** de Java 2 encapsulan las vías para designar las limitaciones de acceso y las autorizaciones asociadas a los recursos valiosos. Las **políticas** de Java 2 proveen los mecanismos necesarios para asociar dichos permisos con los recursos valiosos en una forma configurable. Finalmente, los medios para encapsular **dominios** del control de acceso también son provistos en la **Arquitectura Esencial de Seguridad de Java 2.**

El paquete *java.security* contiene las clases e interfaces que definen la **Arquitectura Esencial de Seguridad**. El paquete *java.security.acl* también contiene las clases para el control de acceso y las interfaces que eran esenciales en la arquitectura de seguridad de Java 1.1, pero han sido substituidas por nuevos constructores de control de acceso en Java 2. Finalmente, otras clases relacionadas a la seguridad están incrustadas en toda la colección de paquetes de la plataforma java.

A.7 Arquitectura Criptográfica Java

La **Arquitectura Criptográfica Java** ("Java Cryptography Architecture", JCA) provee una infraestructura para tener una funcionalidad criptográfica básica en la plataforma Java. El alcance de la funcionalidad criptográfica incluye la protección de los datos contra la corrupción usando funciones y algoritmos criptográficos para resguardar la integridad de los datos. Los algoritmos

criptográficos para la generación de firmas usados para la identificación de fuentes de datos y código también están incluidos dentro del JCA. Debido a que las llaves y los certificados son una parte esencial para la identificación de las fuentes de datos y códigos, también se incluyen API's para manejar dichos elementos.

La JCA incluida en la plataforma Java apareció por primera vez con Java 1.1. JCA provee las funciones criptográficas básicas para alcanzar los siguientes propósitos:

- Proveer la infraestructura para proteger la integridad de los datos almacenados o transferidos.
- Identificar al ente principal asociado a los datos que se están transfiriendo o se están recuperando de un almacén.
- Proveer la infraestructura para soportar la generación de llaves y certificados usados para identificar las fuentes de datos.
- Proveer una infraestructura a la cual se puedan conectar diferentes algoritmos criptográficos de diferentes proveedores de servicio.

A.8 Extensión Criptográfica de Java

Los términos encriptación y criptografía algunas veces son usados indistintamente. Sin embargo, Sun se adhiere a la definición de que la criptografía provee las funciones de integridad de datos e identificación de fuentes, la cual es implementada por el JCA. Por encriptación se entiende el uso de funciones para encriptar bloques de datos con el fin de añadir confidencialidad hasta que el dato sea desencriptado por el receptor autorizado. La **Extensión Criptográfica de Java** ("Java Cryptography Extension", JCE) se provee como una extensión de seguridad para realizar las tareas de encriptación.

En general, se puede argumentar lógicamente que la encriptación es un aspecto esencial de cualquier sistema seguro como para que Sun hubiera incluido al JCE dentro de la plataforma y no manejarlo como una extensión. Pero esta realidad se debe a las restricciones de USA en lo referente a la tecnología de encriptación. Si Sun hubiera incluido al JCE como una parte esencial dentro de la plataforma Java, la exportación de este lenguaje fuera de USA sería imposible.

A.9 Extensión de Conector Seguro de Java

Debido a que SSL ("Secure Sockets Layer") es uno de los protocolos para transmisión de datos encriptados más usado para la integridad y confidencialidad de las comunicaciones, Sun ha desarrollado la **Extensión de Conector Seguro de Java** ("Java Secure Socket Extension", JSSE) como una librería que permite a los programadores en Java usar dicho protocolo.

La JSSE provee una interfase normalizada con la implementaciones necesarias para construir aplicaciones Java con SSL. Aún cuando se utilizaran diferentes implementaciones SSL, el desarrollador seguiría usando la misma interfase para las aplicaciones. La JSSE también provee una interfase normalizada para soportar otros protocolos como el TLS ("Transport Layer Security") y el WTLS ("Wireless Transport Layer Security").

A.10 Servicio de Autenticación y Autorización de Java

La extensión de **Servicio de Autenticación y Autorización de Java** ("Java Authentication and Authorization Service", JAAS) fue desarrollada para proveer una vía estándar de limitar el acceso a los recursos basándose en la autentificación de la identidad del usuario. Por lo cual se proveen API's para el "login" y "logout", permitiendo utilizar diferentes modelos de autenticación con una misma interfase; es decir, se usa la misma API para "Kerberos" o "SmartCards".

Anexo B: Situación Actual de las Redes Bancarias Mexicanas[2]

En México, la seguridad se está convirtiendo en una prioridad para empresas y personas, ya que los delitos informáticos se multiplican día con día. Ante esta situación, la tecnología de la información se ha convertido en la perfecta aliada de las dependencias de gobierno, instituciones financieras y demás empresas en general.

Día a día crece la necesidad de contar con alta seguridad en las transacciones electrónicas, a fin llevarlas a cabo sin que éstas sean "vistas" por extraños que además puedan hacer un mal uso de esta información. Los riesgos de quedar inconclusas o extraviadas es otro problema. Hablar de seguridad informática, de los esfuerzos y políticas que implementan las empresas, instituciones de gobierno, sector académico, industria, entre otras, no sólo implica entender la tecnología y herramientas que permiten poner barreras y filtros en las interconexiones de un sistema nervioso digital con el exterior, sino también entender y crear una nueva cultura hacia el individuo particular y al interior de cada institución, ya que el enemigo puede estar adentro y ni siquiera saber que el propio usuario es un riesgo.

En México ya existen varias empresas con servicios comerciales disponibles por Internet: Gandhi, Pedro Domeq, Submarino, etc.; sólo por mencionar algunas. Sin embargo, aunque el futuro es promisorio, aún hay que superar varios obstáculos para lograr un crecimiento mayor en el comercio electrónico, especialmente en lo relacionado con seguridad y formas de pago. En general, el gran problema al que se ha enfrentado el B2C es la desconfianza a enviar el número de tarjeta por la red, y que ésta pueda ser obtenida: en la transferencia del cliente a la tienda virtual o al violar la seguridad de un servidor en la tienda virtual. Por lo cual se propone enviar una autorización encriptada por el cliente, la cual solo puede ser desencriptada por el banco poseedor de la cuenta del cliente, y validada al cumplirse un estricto protocolo seguido por los diferentes entes participantes en las actividades comerciales por Internet.

B.1 Medio Bancario

Primero bosquejaremos brevemente el sistema bancario actual.

Cada banco esta formado por sus sucursales, su centro de información y su redes de conexión. Las sucursales se conectan a su centro de información por medio de una WAN propietaria en la cual todas las transferencias se realizan de forma segura. Además, su centro de información esta constituido por varias redes LANs y servidores Web y EDI. Todo esto en conjunto forma el medio intrabancario.

Los clientes de cada banco pueden hacer operaciones vía Web o EDI, donde dichas actividades son en tiempo real si las cuentas involucradas pertenecen al mismo banco, ya que se realizan únicamente dentro del medio intrabancario.

Para operaciones entre bancos se utiliza el medio interbancario, el cual consta de 3 redes.

1. Red SECOBAN, enfocada a la transferencia de los documentos de las operaciones y trabaja por lotes (normalmente se hacen remesas de documentos a enviar por la tarde o en la noche).

[2] La información presente en este anexo se obtuvo del Banco BITAL

2. Red ESPAGUA, controlada por el Banco de México, enfocada a la transferencia monetaria para la compensación de los documentos transmitidos por la red SECOBAN y opera en línea.
3. Red INDEVAL, controlada por el Banco de México, y enfocada a la interacción entre los bancos y las Casas de Bolsa.

Por sus características, se considera a los medios interbancario e intrabancario como seguros (redes privadas, sistemas cerrados, etc.)

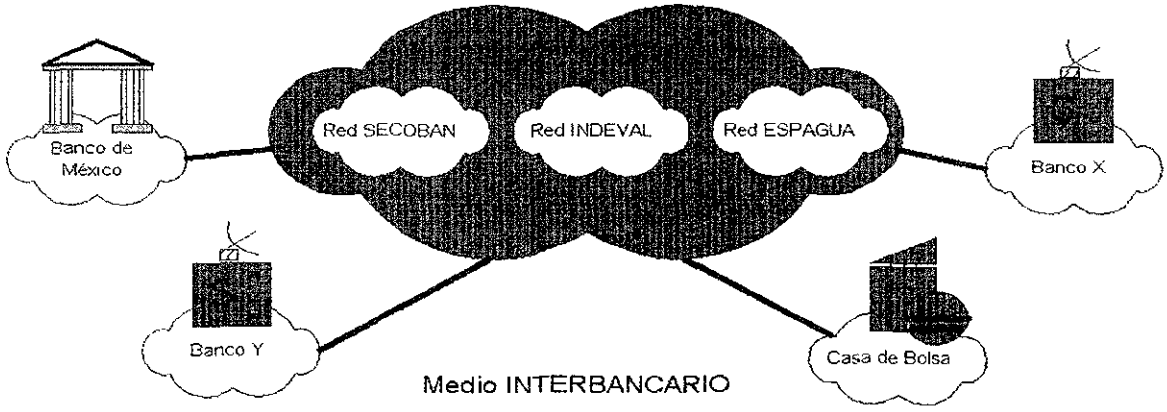


Figura B-1 Esquema del actual medio interbancario mexicano

En México, el esquema de "pagos a terceros" en tiempo real (necesario para el comercio electrónico) ha sido establecido únicamente para la transacción entre cuentas del mismo banco. De esta forma, si un a tienda virtual desea efectuar transferencias seguras "en línea", el negocio virtual debe abrir en cada banco de los que recibirá depósitos, una cuenta empresarial (lo mismo ocurre para la domiciliación de servicios) El "pago a terceros en tiempo real con cuentas de diferentes bancos" no esta establecido, pero en la actualidad esta en estudio su implementación. Por el momento, se utiliza el pago interbancario (más indirecto y no en línea pues actúa conforme a las políticas de la red SECOBAN) como una opción a esta situación.

Anexo C: Protección de las Comunicaciones en las Redes de Datos

En teoría, cuando personas desean comunicarse de forma segura, la encriptación puede ocurrir en cualquier capa del modelo de comunicaciones OSI ("Open Systems Interconnection", Interconexión de Sistemas Abiertos). En la práctica, éste proceso se realiza en las capas más bajas o en las más altas. Si ocurre en las capas inferiores, se le llama **encriptación de enlace por enlace** ("link-by-link encryption"), donde todo lo que viaje por ese enlace de datos particular es encriptado. Si la protección de la información se efectúa en las capas superiores, se le llama **encriptación de extremo a extremo** ("end-to-end encryption"); los datos son cifrados selectivamente y permanecen en dicho estado hasta que son descifrados por el receptor final a quien fueron enviados. Cada uno de estas dos alternativas tienen sus ventajas y desventajas [18, 216-217].

C.1 Encriptación de Enlace por Enlace

El lugar más fácil para añadir la encriptación es en la capa física. Las interfaces a la capa física por lo general son normalizadas y es fácil conectar artefactos de encriptación ("hardware") en este punto. Estos dispositivos encriptan toda información que pase a través de ellos, incluyendo datos de usuarios, información de enrutamiento e información de protocolos. Y pueden ser utilizados en cualquier tipo de enlace digital de comunicación. Por otro lado, los nodos de almacenamiento o conmutación inteligente entre el transmisor y el receptor necesitan descifrar el flujo de datos antes de procesarlo [18, 217-218].

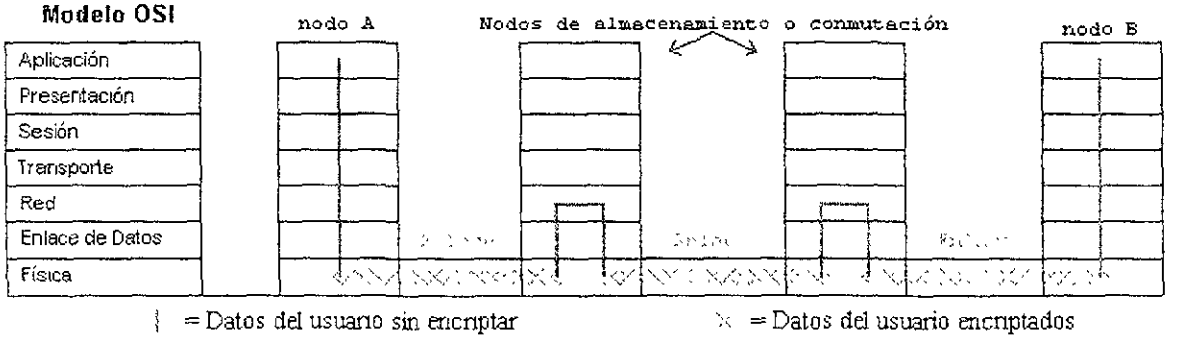


Figura C-1 Encriptación de enlace por enlace

Este tipo de encriptación es muy efectiva. Dado que todo es encriptado, un criptoanalista no puede obtener alguna referencia sobre la estructura de la información que viaja. El enemigo no tiene idea de quien esta hablando a quien, la longitud de los mensajes enviados, el número de veces que ellos se comunican al día, etcétera. Esto es llamado **seguridad en el flujo del tráfico** ("traffic-flow security"): al enemigo no solo carece del acceso a la información, tampoco puede accesar al conocimiento de donde y cuanta información esta fluyendo.

La seguridad no depende de ninguna técnica de manejo de tráfico. La administración de llaves es simple, únicamente los extremos de cada enlace necesitan una llave común, y está puede cambiar independientemente del resto de la red.

En el caso de una línea de comunicación sincrona, después de la inicialización la línea trabaja indefinidamente, recuperando automáticamente bits o errores de sincronización. La línea encripta todo mensaje enviado de un extremo del enlace al otro; y si no hay algún mensaje, sólo cifra y

descifra datos aleatorios. Un enemigo a la escucha no tiene idea cuando están siendo enviados mensajes y cuando no; no tienen idea cuando los mensajes inician y terminan. Lo único que ve es un torrente sin fin de bits con apariencia aleatoria.

En el caso de una línea de comunicación asíncrona, la diferencia es que el adversario puede obtener información sobre la razón de transmisión. Si esta información debe ser ocultada, se pueden enviar mensajes de relleno (valor aleatorio) durante los períodos inactivos.

El gran problema con la encriptación en la capa física es que cada enlace físico de la red necesita ser encriptado: dejar cualquier enlace sin encriptación pone en peligro la seguridad de toda la red. Si la red es grande, el costo puede incrementarse rápidamente hasta convertirse en prohibitivo. Además, cada nodo en la red debe ser protegido, dado que procesa información descifrada. Si todos los usuarios de la red son confiables y todos los nodos se encuentra en lugares seguros, esto es tolerable. Pero aún en las compañías más simples, la información debe mantenerse en secreto dentro del mismo departamento. Si la red, accidentalmente, direcciona mal o no reencripta la información y la transmite, cualquiera podrá leerla.

C.2 Encriptación de Extremo a Extremo

Existen dos aproximaciones para obtener una encriptación de extremo a extremo [18, 218-219]:

- Si el proceso se realiza en las capas intermedias de la arquitectura OSI.
- Si el proceso se realiza en las capas superiores de la arquitectura OSI.

Una opción es colocar el equipo de encriptación en las capas intermedias de la arquitectura OSI, entre la capa de red y la capa de transporte. Este dispositivo debe entender los datos de acuerdo a los protocolos superiores a la capa 3 y encriptar únicamente las unidades que transportan datos, para después ser combinadas con la información de enrutamiento no encriptada y ser enviadas a las capas inferiores para su transmisión

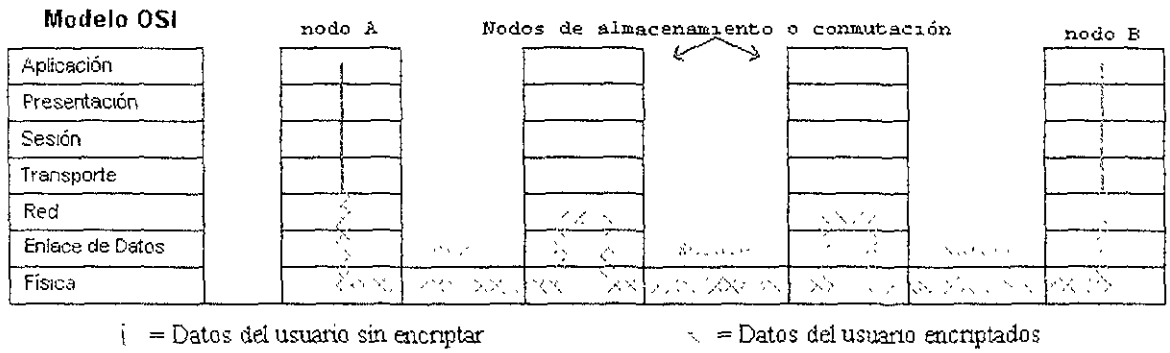


Figura C-2 Encriptación de Extremo a Extremo en las capas intermedias

Esta implementación evita el problema de *descifrar / procesar / cifrar* en cada nodo de la capa física. Al proveer encriptación de extremo a extremo, los datos se mantienen encriptados hasta alcanzar su destino final. El principal problema con la encriptación de extremo a extremo es que la información de enrutamiento de los datos no es encriptada; un buen criptoanalista puede aprender mucho de quien esta hablando a quien, cuantas veces y por cuanto tiempo; sin conocer el contenido de sus conversaciones Además, la administración de las llaves es más complicada, dado que se debe asegurar para cada par de usuarios tengan las llaves correctas a usar. Esto implica la existencia de un ente que genere las llaves de sesión o almacene las llaves públicas, ente sujeto a ataques por parte del enemigo.

Construir equipo para encriptación de extremo a extremo es difícil. Cada sistema de comunicación particular tiene sus propios protocolos. Algunas veces las interfaces entre las capas no están bien definidas, haciendo la tarea más complicada.

Si la encriptación se realiza en una de las capas superiores de la arquitectura de comunicación, como en la capa de aplicación o en la de presentación, entonces esta operación se vuelve independiente del tipo de red de comunicación utilizada. Todavía es una encriptación de extremo a extremo, pero la implementación no debe preocuparse en códigos de línea, sincronización entre módems, interfaces físicas, y todo eso. En los antiguos días de la encriptación electromecánica, el cifrado y descifrado se efectuaba fuera de línea; con este acercamiento estamos a un paso de esa antigua implantación.

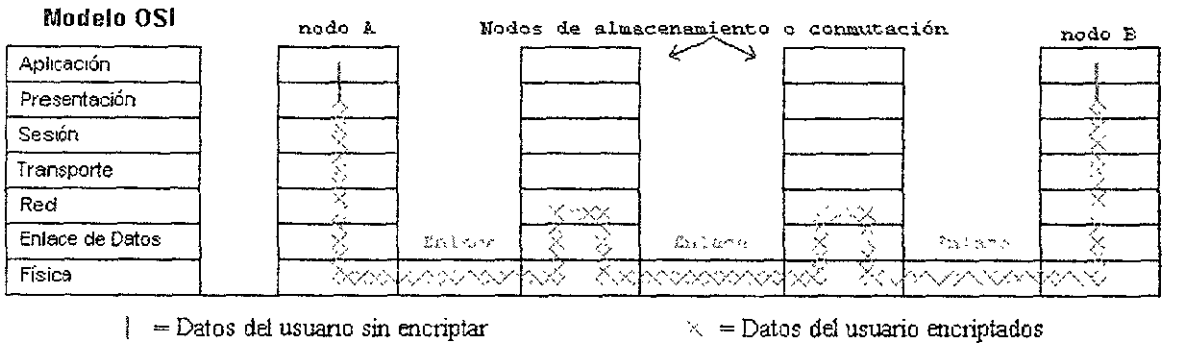


Figura C-3. Encriptación de Extremo a Extremo en las capas superiores

La encriptación en estas capas superiores interactúa con el "software" del usuario. Este "software" es diferente para cada arquitectura particular de computadora, y la encriptación debe ser optimizada para diferentes sistemas de computo. La encriptación puede ocurrir en el "software" mismo o en un "hardware" especializado. En el último caso, la computadora pasará los datos al "hardware" especializado para encriptarlo antes de enviarlo a las capas inferiores de la arquitectura de comunicación para transmitirlo. Este proceso requiere de inteligencia y no es factible para terminales tontas. Adicionalmente, pueden existir problemas de compatibilidad con diferentes tipos de computadoras.

La principal desventaja de la encriptación de extremo a extremo es que ésta permite el análisis de tráfico. Este análisis es el análisis de mensajes encriptados: de donde vienen, a donde van, que tan largos son, cuando son enviados, que tan frecuentes son, cuando estos coinciden con eventos como reuniones, etcétera. Mucha información importante esta dentro de estos datos, y un criptoanalista desea poner sus manos sobre ella.

C.3 Combinando las Dos

Combinando la encriptación de extremo a extremo con la de enlace por enlace, se obtiene la forma más efectiva para asegurar una red, aunque también es la más costosa. La encriptación de cada enlace físico hace imposible cualquier análisis del enrutamiento de información, mientras que la encriptación de extremo a extremo evita la fuga de datos no cifrados en los distintos nodos de la red. La administración de llaves para los dos esquemas puede ser totalmente separada: los administradores de la red pueden encargarse de la encriptación a nivel capa física, mientras que los usuarios tienen la responsabilidad de la encriptación de extremo a extremo [18, 219-220].

C.4 Tabla de Comparación

Características del esquema	De enlace por enlace	De extremo a extremo
Seguridad dentro de los "Hosts"	• El mensaje esta expuesto dentro del "host" transmisor. • El mensaje esta expuesto dentro de los nodos intermedios.	• Mensaje encriptado en el "host" transmisor. • Mensaje encriptado en todos los nodos intermedios.
Rol del usuario	• Aplicado por el "host" transmisor. • Invisible al usuario. • El "host" mantiene la encriptación. • Una facilidad para todos los usuarios. • Puede realizarse en "hardware". • Todo es encriptado.	• Aplicado por el proceso de transmisión. • El usuario aplica la encriptación. • El usuario debe encontrar el algoritmo. • El usuario selecciona la encriptación. • Se puede realizar fácilmente por "software". • El usuario decide si encripta o no los mensajes.
Implementación	• Requiere una llave por par de "hosts" • Requiere "hardware" o "software" de encriptación en cada "host". • Provee autenticidad del nodo.	• Requiere de una llave por par de usuarios. • Requiere "hardware" o "software" de encriptación por cada nodo. • Provee autenticidad del usuario.
Ventajas	• Fácil operación, todo lo transmitido por el enlace es encriptado. • Provee seguridad en el flujo de tráfico. • La encriptación es un proceso en línea.	• Mayor nivel de seguridad.
Desventajas	• Los datos en texto en claro, están expuestos dentro de los nodos intermedios.	• Requiere un sistema de administración de llaves más complejo. • El análisis del tráfico es posible. • La encriptación es un proceso fuera de línea

Esta tabla se obtuvo de [18, 221]

Anexo D: Equipos y Dispositivos de Seguridad

A continuación se presentan los dispositivos mínimos necesarios recomendables para proteger las redes de datos de los atacantes que puedan acceder a través de Internet o alguna otra red de datos conectada (LAN, MAN, WAN, etc.). Véase [23, 34-38] y [24, 34-37]

D.1 Firewalls

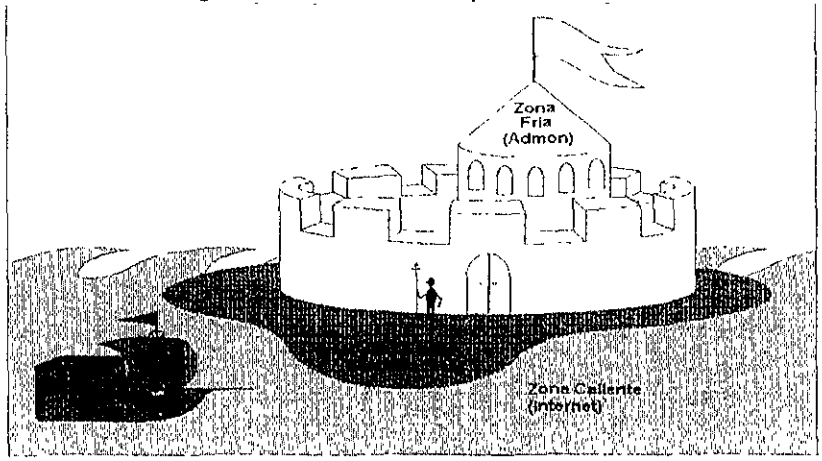
Un "firewall" es un dispositivo, generalmente mezcla de "hardware" y "software", que se coloca entre dos redes para regular la comunicación entre ellas; de acuerdo a criterios de seguridad previamente establecidos.

Generalmente se manejan dos redes: la corporativa e Internet (correcto para el caso de la Tienda Virtual y la Casa Musical; para el ente Banco se deben manejar 3: el medio intrabancario, el interbancario e Internet). El "firewall" determina cual información puede fluir entre los elementos de cada red Sin embargo, un "firewall" también se puede usar entre dos o más redes de una misma empresa e inclusive una empresa puede usar más de un firewall para salir a Internet o para aislar recursos.

Aunque existen un sin fin de formas de aprovechar la tecnología de "firewall", es muy común que tengamos, al menos, tres zonas distintas:

- **Zona caliente**. Así se denomina a Internet y a los elementos que están fuera de nuestra red. Esta zona no está gobernada por nuestras reglas, por lo que nos interesa regular el tráfico que proviene de esta zona.
- **Zona desmilitarizada**. Abreviada en inglés como DMZ, en ésta ponemos a los servidores "más expuestos", como el de Web, correo electrónico o el de nombres de dominio (DNS) A estos servidores no los podemos proteger demasiado, pues lo que queremos es que dialoguen continuamente con el mundo externo. Imagínese que el servidor Web de una empresa esté tan protegido que ningún usuario externo pueda acceder a él, poca utilidad tendría.
- **Zona Fría**. Así denominamos a la zona de nuestra red interna, y por tanto, aquella que queremos proteger más. En esta parte están los servidores corporativos, "mainframes", mini computadoras, enrutadores, PC's y toda la infraestructura que conforma la red de la organización.

Figura D-1 Zonas delimitadas por un "firewall"



Existen dos tipos principales de "firewalls", los cuales son:

D.1.1 "Firewall" de filtro de paquetes

Están basados en definir reglas o criterios de acuerdo al tipo de protocolo, puertos asociados, servicios o comandos que se permiten, tanto de entrada como de salida. Así, cuando un paquete quiere entrar a nuestra red, el firewall revisa su lista de reglas y determina si puede pasar o no. Hoy en día, la forma más común de implementar este tipo de firewall es a través de reglas de acceso en los propios ruteadores o "routers". De esta forma, al especificar dichas normas dentro del ruteador, habilitamos automáticamente un "firewall" de filtros de paquetes.

Estos "firewalls" también son conocidos como "Screening Routers", proveen acceso a nivel IP y pueden aceptar, rechazar o tirar paquetes de la red, basados principalmente en las direcciones fuente y destino, así como los puertos a través de los cuales se tiene acceso a la aplicación.

Este tipo de "firewalls" provee un nivel básico de seguridad a un precio relativamente bajo. Tienen un alto nivel de desempeño y son normalmente transparentes para los usuarios. Las debilidades principales de estos "firewalls" son:

1. Sólo operan en la capa de protocolo y no son seguros, ya que carecen de protección contra ataques provenientes de capas superiores.
2. Por lo general, son difíciles de configurar en el sentido de poder traducir las necesidades de aplicación en configuración de filtros de protocolos.
3 No pueden esconder la topología de redes privadas y, por lo tanto, pueden exponer la red privada al mundo exterior.
4. Tienen capacidades de auditoria limitadas.
5. Algunas aplicaciones de Internet no están soportadas por los "firewalls" de filtrado de paquetes.
6 No pueden soportar algunas políticas de seguridad tales como autentificación a nivel de usuarios y control de accesos a ciertos horarios.

D.1.2 "Firewall" de nivel de aplicación o basado en "proxies"

Un "firewall" de este tipo es aquel que está compuesto de uno o más módulos o "proxies", que actúan como intermediarios entre el usuario externo y las aplicaciones. De esta manera, los paquetes no viajan entre el usuario y los servidores; sino que se establece, por un lado, una conexión entre el usuario y el "firewall", y por otro, una conexión entre el "firewall" y el servidor. Para cada paquete generado por el usuario, el "firewall" revisa su contenido y si determina que es válido, entonces genera otro paquete entre él y el servidor final De acuerdo al producto, el "firewall" puede tener sólo un proxy, o uno para cada protocolo o servicio.

Nota el término "proxy" también se refiere a trasladar el contenido de un servidor remoto a uno local, para disminuir el número de accesos y carga de transferencia del servidor remoto

Los "firewalls" de nivel aplicativo proveen control de acceso a nivel capa de aplicación, en otras palabras, actúan como "gateways" (puertas o pasarelas de acceso) entre dos redes. Este tipo de "firewalls" tienen la habilidad de examinar el tráfico en detalle y tienen las siguientes ventajas:

1 Entienden los protocolos en la capa de aplicación, y por lo tanto pueden defenderse de todos los ataques.
2 Generalmente son más sencillos de configurar, por lo que no es necesario un conocimiento detallado de protocolos de bajo nivel.
3 Pueden esconder la topología de redes privadas

4 Cuentan con herramientas de auditoria para monitorear el tráfico y manipular los archivos de registro que contienen información como: direcciones fuente y destino, tipo de aplicación, identificación y claves de usuarios, tiempo de inicio y finalización el acceso, y el número de bytes de información transferida en todas las direcciones.
5 Pueden soportar políticas de nivel aplicativo que incluyen la autentificación a nivel de usuario y controles de acceso por horarios.

Los "firewalls" de nivel aplicación son normalmente más lentos, ya que tienen que revisar todo el tráfico.

De la misma manera, son intrusivos, es decir, cambian el sistema operativo de la máquina donde se instalan; son restrictivos y normalmente requieren que los usuarios cambien su comportamiento o utilicen "software" especializado para poder cumplir con las políticas establecidas. Por estas razones este tipo de "firewalls" no son transparentes para los usuarios.

La segunda generación de "firewalls" de nivel aplicativo resuelve el problema de transparencia para el usuario sin comprometer el desempeño. Estos muros de seguridad ofrecen los siguientes beneficios adicionales:

1. Pueden ser usados como "firewalls" de Intranet por su transparencia y, generalmente, mayor desempeño.
2. Pueden proveer traducción completa de direcciones de red, adicional a la capacidad de esconder la topología de las redes privadas.
3. Pueden soportar mecanismos más avanzados de autentificación a nivel usuario.

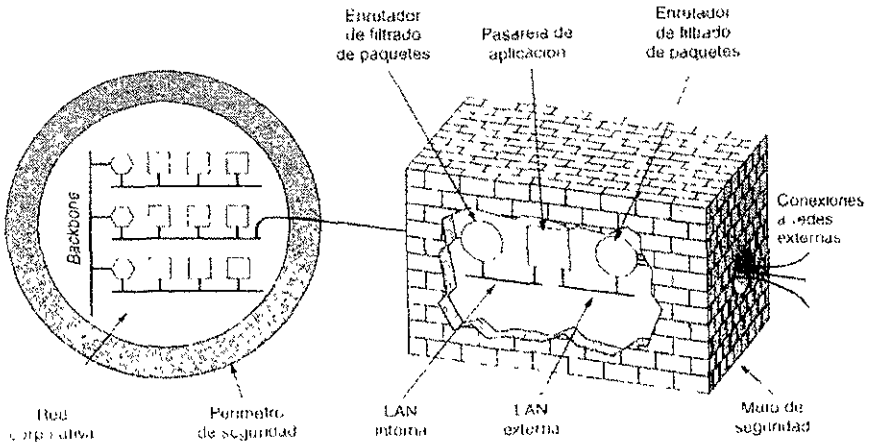


Figura D-2. Muro de seguridad que consiste en dos filtros de paquetes y una pasarela de aplicación.

D.2 Detectores de Intrusos

De forma general, un **detector de intrusos** o **sistema para la detección de intrusos** es un mecanismo (puede ser mezcla de "hardware" y "software") que monitorea la red o algún servidor y que, al detectar un patrón de comportamiento anormal que se puede asociar con un ataque de seguridad, envía una alarma e, incluso, activa una o varias acciones para frenar o contrarrestar dicho ataque.

Existen dos grandes tipos de detectores de intrusos los que vigilan la red y los que cuidan a cada servidor En ambos casos, la meta es detectar patrones de ataque y dar aviso cuanto antes

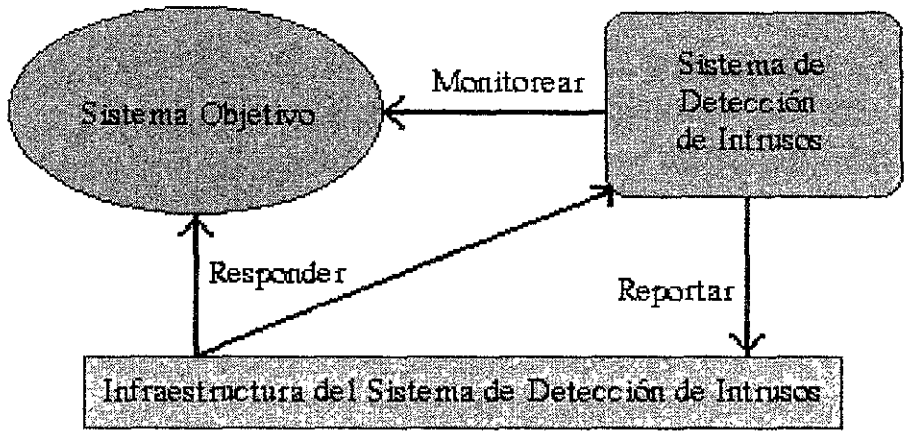


Figura D-3. Mecanismo General de un Sistema Detector de Intrusos

Así, por ejemplo, un detector para red que se coloque justo atrás del "firewall", podrá detectar si alguien que ya entró a nuestra red intenta realizar ataques, explotando vulnerabilidades conocidas de los sistemas. De esta forma, podría descubrir que un usuario externo hace "radiografías" de una red interna a través de comandos "ping", "traceroute" y otros; o que alguien más quiere violar la seguridad del servidor "Web" al enviarle como campo de forma HTML una cadena de caracteres inválida (un ataque para el desbordamiento de memoria temporal llamado "buffer overflow"), la cual puede ocasionar que el atacante entre con privilegios de administrados al sistema.

Todo lo anterior lo descubrió el detector para red, pues espía todo el tráfico que pasa por el segmento (en esta parte se parece a un analizador de protocolos, al poner la tarjeta de red en modo "promiscuo") y trata de detectar ataques o comportamientos sospechosos, tanto del tráfico que sale como del que entra.

Los detectores basados en el servidor vigilan (de forma similar) que las configuraciones del equipo, ciertos archivos o directorios, algunas cuentas especiales (como administrador o "root") y ciertos comandos especiales del sistema operativo no tengan comportamientos fuera de lo normal.

¿Por qué es necesario un detector de intrusos si ya se tienen "firewalls"? Por desgracia éstos no protegen de todos los ataques Un ejemplo típicamente los "firewall" deben dejar "abierto" el puerto 80 hacia el servidor "Web" (pues éste es el puerto que usa el protocolo HTTP), sin embargo existen ataques que sólo necesitan utilizar dicho puerto para sabotear el servidor "Web".

Esto nos lleva a que los detectores de intrusos y los "firewalls" son tecnologías complementarias, es deseable integrarlas para facilitar la administración, y lograr respuestas más ágiles y automatizadas ante ataques

Como un ejemplo de esta finalidad: existe un usuario externo que ataca el servidor "Web" e intenta encontrar vulnerabilidades de "buffer overflow" en las formas HTML. En este caso, una secuencia ideal de respuesta al ataque podría ser:

1. El detector de intrusos se da cuenta del ataque.
2. Envía un mensaje a la consola del administrador de seguridad.
3. El detector le envía una orden al firewall para que "cierre" la conexión a ese usuario.
4. El firewall cierra la conexión
5. La consola del detector de intrusos nos avisa que el ataque ha sido frenado

La consola del detector de intrusos también nos sugiere cambios a la configuración del servidor "Web" que había sido atacado (en este caso, más que a la configuración, es a la forma de programar formas HTML).

Una consideración importante en cuanto al uso de esta tecnología es que los detectores de intrusos vienen configurados de fábrica en modo "paranoico". En otras palabras, cualquier cosa que parezca un ataque genera una alarma en la consola del detector. Por lo cual es recomendable reconfigurarlos al momento de instalarlos.

Otra consideración importante para el caso de los detectores enfocados a red: si es instalado justo atrás del "firewall" (la situación más típica), no podrá ver todos los ataques que tratan de realizar sobre la red; sólo aquellos que ya han pasado por dicha defensa. Sin embargo, en configuraciones de mayor nivel de seguridad, es necesario poner detectores antes y después del "firewall", e incluso en las entradas y salidas entre la red corporativa.

Y una consideración más para los detectores enfocados a servidor: lo más recomendable es poner uno por cada servidor de misión crítica. Las implicaciones de este enfoque son financieras: una empresa pequeña sólo necesitará invertir unos 4000 dólares para proteger su sitio "Web", mientras que una institución bancaria requerirá cientos de miles de dólares para proteger su sitio "e-banking" y en general toda su red a nivel nacional.

Anexo E: Medios de transporte

E.1 SMTP (Simple Mail Transfer Protocol)

El mecanismo básico de transporte de correo a través de Internet queda definido por SMTP (Simple Mail Transfer Protocol). El RFC 822 describe el formato de los mensajes intercambiados. Según este estándar, cada mensaje consta de dos partes:

1. **"header"** (cabecera): contiene la información necesaria para que el mensaje llegue a su destino. El formato de la cabecera es definido también por el estándar y está formada por un conjunto de pares clave / valor estructurados.
2. **"body"** (cuerpo o contenido): la información que debe recibir el destinatario. Esta información estará siempre en formato de texto de siete bits (US-ASCII).

E.2 MIME (Multi-purpose Internet Mail Extensions)

MIME es un protocolo de intercambio de objetos a través de Internet. Se desarrolló inicialmente para enriquecer los intercambios de correo electrónico, limitados según el RFC 822 a ASCII de siete bits, habiéndose extendido a otros muchos protocolos. El formato MIME permite el envío de texto enriquecido (8 bits), gráficos, ficheros de audio, vídeo, etc. En MIME, cada objeto de mensajería se encapsula en un envoltorio que especifica tanto su semántica como el medio de codificación utilizado. La caracterización semántica hecha en la cabecera permite asociar los datos con su mecanismo de transporte (codificación) y con su significado, de forma que el remitente y el destinatario utilicen coordinadamente los datos intercambiados.

E.3 PEM (Privacy Enhanced Mail)

PEM es un sistema similar a MIME y desarrollado en paralelo con éste para crear objetos de mensajería seguros Incluye cifrado, autenticación y gestión de claves y permite el uso de algoritmos simétricos y de clave pública. Con el desarrollo de MIME, PEM es, de alguna forma, repetitivo, por lo que se ha visto desplazado por S/MIME. De hecho, lleva más de dos años en estado de borrador.

E.4 MOSS (MIME Object Security objectS)

MOSS (también conocido como PEM-MIME) es una extensión de MIME derivada de PEM que aporta exclusivamente lo que le falta a MIME para obtener las garantías deseadas: claves, firmas digitales, certificados, etc. De este modo se consigue un intercambio seguro de objetos. De acuerdo con la propia naturaleza de MIME, es posible aplicar diferentes servicios de seguridad a cada parte del mensaje.

Este estándar ha sufrido críticas debido a sus requerimientos, que son extremadamente flexibles. Fruto de esta flexibilidad puede ocurrir que dos agentes de correo diferentes, ambos soportando

MOSS, sean incompatibles. Esta flexibilidad es, en parte, una reacción a la rigidez de PEM, la cual le hacía impopular entre los usuarios.

E.5 S/MIME (Secure-Multipurpose Internet Mail Extensions)

S/MIME es un protocolo que añade firmas digitales y cifrado a los mensajes MIME. MIME, en sí mismo, no proporciona ningún servicio de seguridad. S/MIME define esos servicios, utilizando criptografía de clave pública, siguiendo la sintaxis definida en el PKCS#7.

S/MIME ha sido adoptado recientemente por un gran número de compañías como FTP Software, Qualcomm, Microsoft, Lotus, VeriSign, Netscape o Novell.

E.6 S-HTTP (Secure HTTP)

Secure HTTP es un protocolo propuesto por Enterprise Integration Technologies (EIT), patrocinado por el consorcio CommerceNet y desarrollado en la actualidad por Terisa Systems. Constituye una extensión del protocolo HTTP, incorporando cabeceras MIME para aportar confidencialidad, autenticación, integridad e irrenunciabilidad de las transacciones.

Utiliza un sistema inspirado en PEM, añadiendo suficientes cabeceras a cada transacción para lograr cada uno de los objetivos propuestos. Las transacciones HTTP constan simplemente de una petición de parte del cliente que produce una respuesta del servidor. S-HTTP especifica que el cliente envíe directamente toda la información pertinente: claves, certificados, códigos de integridad, etc. (incluyendo la posibilidad de referenciar secretos compartidos accesibles en forma externa: intercambios previos o bases de datos comunes). El servidor responde siguiendo la misma filosofía PEM. El protocolo soporta varios mecanismos criptográficos y negocia los modos y opciones de estos mecanismos.

E.6.1 Evaluación de S-http

Las principales ventajas de S-HTTP son su flexibilidad y su integración dentro de HTML (extensiones al lenguaje similares a las introducidas periódicamente por Netscape en sus navegadores).

Entre sus debilidades podemos señalar los efectos derivados de mantener la compatibilidad hacia atrás y la necesidad de implementar servidores que soporten las extensiones a HTML aportadas por el protocolo S-HTTP.

E.7 SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL) es un protocolo diseñado por Netscape Communications Co., que dispone un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él. Proporciona conexiones seguras sobre una red insegura como es Internet, asegurando las siguientes características

- conexión privada: la información se cifra utilizando criptografía de clave simétrica
- autenticación: usando criptografía de clave pública.
- integridad: la integridad de los mensajes se asegura usando firmas digitales

Además, proporciona características adicionales:

- extensibilidad: es capaz de soportar nuevos protocolos en el futuro.
- eficiencia: al utilizar compresión, minimiza el tiempo necesario para establecer la conexión.
- compatibilidad: productos con diferentes versiones de SSL pueden interoperar entre sí.

SSL se compone de dos partes diferenciadas:

a) "**Handshake Protocol**": se encarga de establecer la conexión y determinar los parámetros que se van a utilizar posteriormente (fundamentalmente se trata de establecer cual va a ser la clave simétrica que se utilizará para transmitir los datos durante esa conexión).
b) "**Record Protocol**": comprime, cifra, descifra y verifica la información que se transmite.

Este sistema es transparente para las aplicaciones finales, que simplemente saben que el canal se encarga de proporcionarles confidencialidad entre extremos. Por tanto, podemos situar protocolos como HTTP, FTP, NNTP o Telnet.

E.7.1 Modo de funcionamiento

El denominado "Handshake Protocol" se compone dos fases: autentificación de servidor y autentificación de cliente; no siendo obligatoria esta última. En primer lugar, el servidor, respondiendo a una petición del cliente, le envía su certificado y las preferencias en lo que a algoritmos de cifrado se refiere. En ese momento, el cliente genera una clave maestra, la cifra con la clave pública del servidor y la transmite al servidor. El servidor recobra la clave maestra y se autentifica respecto al cliente devolviendo un mensaje cifrado con la clave maestra. Los datos siguientes son cifrados con claves derivadas de esta clave maestra.

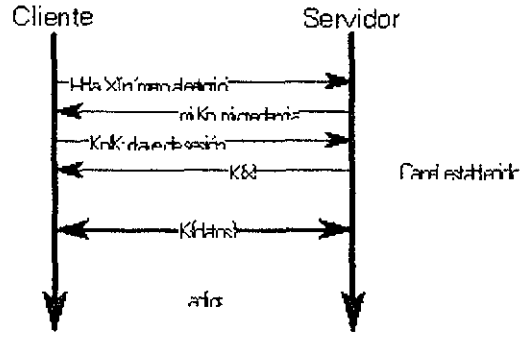


Figura E-1. Establecimiento de un canal seguro con SSL

En la segunda fase opcional, el servidor envía un reto al cliente. Éste se autentifica respecto al servidor retornándole el reto firmado digitalmente por el cliente, así como su certificado (el cual incluye su clave pública).

E.7.2 Algoritmos utilizados

Una gran variedad de algoritmos criptográficos son soportados por SSL. Durante la fase de acuerdo o "handshaking", se utiliza RSA (clave pública). Después del intercambio de claves, se usan unos cuantos algoritmos, entre los que se incluyen RC2, RC4, IDEA, DES y Triple-DES. Como función resumen se usa MD5 o SHA-1. Los certificados siguen el formato X.509.

E.7.3 Implementación

Los diferentes protocolos que utilizan los servicios de SSL usan puertos diferentes a los que les correspondería si no fuesen sobre SSL. La IANA ha reservado los siguientes puertos para su uso por SSL:

433: HTTP sobre SSL (https)
465: SMTP (correo electrónico) sobre SSL (ssmtp), no confirmado.
563: NNTP (servicio de noticias, News) sobre SSL (snntp), no confirmado.

El protocolo SSL está, gracias a los esfuerzos de Netscape, ampliamente extendido. La presencia de "https://" en el URL de un servidor indica se trata de un servidor "seguro" y que debe utilizarse SSL en la comunicación entre dicho servidor y cliente (navegador). Los navegadores más extendidos (Netscape Navigator y Microsoft Internet Explorer) son capaces de utilizar SSL. Esto queda indicado (en el caso de Netscape Navigator) de la siguiente forma:

- la llave de la parte inferior izquierda del navegador aparece completa, no partida como habitualmente (en los casos del MS Internet Explorer y de Netscape Communicator aparece un candado cerrado en la esquina inferior izquierda).
- aparece una línea azul en el límite superior de la línea de visualización de la pantalla del navegador.
- la información del documento alojado en el servidor seguro incluye los datos del certificado que avala al servidor seguro.

Los servidores más populares de la empresa Netscape (Commerce Server, FastTrack Server y Enterprise Server) soportan SSL, con las habituales limitaciones de exportación (clave RC4 de 40 bits para los productos vendidos fuera de EE.UU. o Canadá). El servidor más extendido a escala mundial, Apache, posee una versión SSL, Stronghold, con la ventaja añadida de que, al haber sido desarrollado fuera de los EE.UU., puede vender la versión "completa" de SSL con claves de 128 bits. El servidor de Microsoft, Internet Information Server 2.0, que viene de serie con Windows NT 4.0 no soporta SSL. Las últimas versiones (IIS 4.0) soportan plenamente el estándar (junto con protocolos propios como PCT).

E.7.4 Conclusión

A diferencia de S-HTTP, que es un protocolo substitutivo de HTTP, SSL extiende su soporte a otros protocolos habituales en Internet. Esta es una de las principales ventajas que aporta este último. Mientras que S-HTTP proporciona cifrado en el nivel de aplicación (en este caso WWW), SSL lo hace en el nivel de conexión, proporcionando un canal seguro en el nivel de red Por lo demás, S-HTTP y SSL pueden convivir, utilizándose uno u otro en diferentes instantes de una transacción comercial, o incluso utilizándose simultáneamente.

El sistema es tan robusto como lo sea el menos seguro de los algoritmos que utilice. Claves públicas cortas o claves DES o RC4 de 40 bits deben utilizarse con precaución. Estos son los problemas que plantean las leyes de EE UU.

La principal desventaja de SSL no estriba en sus fundamentos teóricos o implementación, sino, fundamentalmente, la menor protección que proporcionan las versiones exportables de los productos basados en este protocolo. También debe tenerse especial cuidado en decidir qué autoridades de certificación y qué certificados son fiables.

Anexo F: Interfaz Java - JavaScript

El siguiente apartado explica de forma general la forma en la que se puede controlar el comportamiento de un applet Java haciendo uso de botones, controles, cajas de selección y texto (propios de HTML), apoyándose en el manejo de eventos, objetos y funciones de JavaScript.

Como sabemos, JavaScript es un lenguaje de programación creado explícitamente para ampliar las capacidades de los navegadores y el lenguaje que éstos están acostumbrados a utilizar (HTML). Por su parte, Java, al ser un lenguaje de alto nivel, orientado a objetos y de gran potencia, nos permite hacer muchísimas cosas. Los límites de Java son tan bastos como la capacidad del programador Sin embargo, aún cuando esta afirmación es cierta, en la práctica los applets Java carecen de los medios necesarios para interactuar con elementos de formularios HTML, o definen sus propios elementos dentro del contexto del applet; con lo cual la operación desde la página "Web" de dichos elementos se vuelve demasiado elaborada, por no decir imposible.

La solución a este problema se resuelve al incorporar JavaScript dentro del código de las páginas de Internet, así como al adicionar un objeto "JSObject" dentro del applet. Veamos esto con detalle:

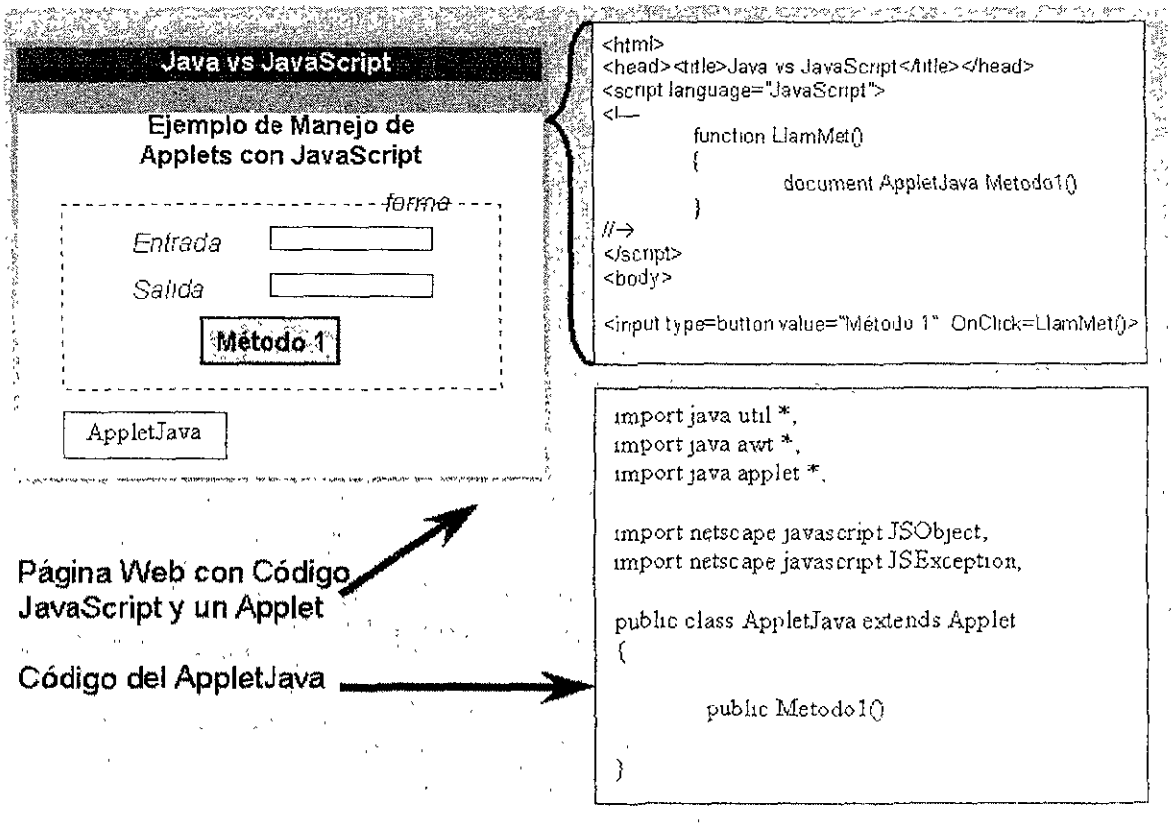


Figura F-1 Pagina "Web" con rutinas en Java y JavaScript

El diagrama anterior muestra una pagina "Web" que contiene, dentro de su cabecera, una función JavaScript cuyo nombre es *LlamMet* (abreviación de "Llamada a Método") Dicha función es

disparada por un método *OnClick* definida dentro de las propiedades del objeto botón que está en el interior de la forma.

De igual forma, podemos observar que, dentro de esta misma página "Web", en la esquina inferior izquierda, aparece un applet Java cuyo nombre es "AppletJava". Dicho objeto, aun cuando no parece tener una función en nuestra página ya que no presenta ningún aspecto definido (es únicamente un cuadro gris), será el encargado de tomar los datos de entrada, aplicarles algún tipo de transformación matemática, que en nuestro caso usaremos como cifrador, y finalmente, desplegar dichos datos en el recuadro de salida.

Antes de comenzar a analizar el código fuente de cada una de las secciones, debemos entender el funcionamiento general de este software. Para ello, pensemos en la cadena de eventos que se suceden después de que el usuario ha hecho la solicitud de la página "Web" al servidor que la contiene:

1. Inmediatamente después de que el servidor de Internet recibe la petición de carga de la página "Web", envía las instrucciones HTML que la componen y espera que el navegador le indique que ha terminado de "armar" la página web con éxito.

2. Al comenzar a recibir las etiquetas HTML, el navegador detecta un par de etiquetas <script>, con lo cual el navegador entiende que todo el código que se encuentra dentro de ellas se deberá tratar como funciones o programas.

3. Después, el navegador comienza a tomar las etiquetas HTML que forman el cuerpo de la página Web conforme estas van llegando. Al mismo tiempo, con las etiquetas (y los archivos o información asociada) recuperadas, comienza a "construir" la página "Web" que el usuario verá en su navegador.

4. Después de un tiempo, el navegador detecta una etiqueta <applet> y solicita entonces el archivo binario definido en la opción "code" de dicha etiqueta. Es importante señalar aquí que si el applet tiene definido el método *init()*, el código presente dentro de este método se ejecutará inmediatamente después de haberse cargado el applet. Cualquier otro método se ejecutará solamente hasta después de que algún otro objeto lo invoque

5 Al finalizar la carga de la página, el usuario vera una caja de texto en la cual se solicita la cadena a encriptar (o de la que se obtendrá su "función resumen"), una segunda caja de texto en la cual se dará el resultado, un botón que al ser pulsado dispara el proceso de cifrado y un applet

6. Al pulsarse el botón de acción, el manejador de eventos de JavaScript llama una función la cual, a su vez, hace un llamado a un método del applet. La razón por la que se define así es para el caso en el que tengamos varios algoritmos de cifrado; es decir, si nuestra página Web tuviera varios algoritmos de cifrado (cada uno de los cuales definido en métodos distintos del applet), se podría programar el proceso de toma de decisión en JavaScript, lo cual es mucho más sencillo y eficiente.

7. De acuerdo al método invocado, el applet realizará una serie de operaciones y transformaciones, y el resultado final será desplegado en la caja de texto de salida.

F.1 Análisis de Código

A continuación mostramos el código HTML, JavaScript y Java de nuestro ejemplo

Página "Web" y JavaScript

```
<html>
<head><title>Java vs JavaScript</title></head>
<script language="JavaScript">
<!—
        function LlamMet()
        {
                document.AppletJava.Metodo1()
        }
// Esta es la función que dispara el Método del applet
//à
</script>
<body>
<form name="forma"> <!—Se define la forma que contiene los JSObjects à
<table>
<tr><td>Entrada</td><td><input type=text name="T_Entrada"></td></tr>
<!—Se define la caja de texto donde el usuario ingresará datos à
<tr><td>Salida</td><td><input type=text name="T_Salida"></td></tr>
<!—Se define la caja de texto donde el usuario verá el resultado
<tr><td colspan=2>
<input type=button value="Método 1" name="Bton" OnClick="LlamMet();">
<!— Al pulsar el botón se dispara la función que llama al método del applet à
</td></tr>
</table>
</form>
<applet code="AppletJava.class" name="AppletJava" height=50 width=50 MAYSCRIPT>
</applet>
</body>
</html>
```

Es importante hacer notar la propiedad *MAYSCRIPT* que está definida en la etiqueta del applet ya que éste le dice al applet que tendrá que interactuar con JavaScript.

Por otra parte, en algunas circunstancias el usuario definirá ciertas constantes o "pasará" determinados parámetros al applet, antes de que éste ejecute algún método. Esto se lleva a cabo al definir entre las etiquetas de <applet> una o más etiquetas de parámetros <param>. A través de estas etiquetas, si existe alguna variable global dentro del applet, su contenido puede ser modificado desde el código HTML.

Ejemplo:

Si estoy utilizando un cifrador de Cesar (en el cual una letra se cambia por su respectiva "n" posiciones más adelante), podemos definir una caja de selección la cual, al cambiar de valor, indica al cifrador de cuantas letras será el corrimiento

```
<select name="Corrimiento">
<option value=3>Tres</option>
<option value=6>Seis</option>
<option value=9>Nueve</option>
</select>

<applet                code="CifradorCesar.class"
MAYSCRIPT>
<param
Nm=document.forma.Corrimiento.value>
```

```
import java.applet.*;

import netscape.javascript.JSObject;
import
netscape.javascript.JSException;

public class CifradorCesar extends
Applet
{
        public Int Nm,
```

Volviendo al ejemplo que hemos estado analizando, el código Java de nuestro applet será:

```
import java.applet.*;// Se definen los paquetes que contienen las librerías
import java.awt.*;
import java.io.*;
import netscape.javascript.JSObject;                    // Este es el paquete que contiene el JSObject
import netscape.javascript.JSException;

public class AppletJava extends Applet
{
        public String texto;            // Definición de Variables
        public String CadEnt,
        public String CadSal;
        JSObject Ventana;               // Definición de los Objetos de la Página Web
        JSObject Documento;
        JSObject Forma;
        JSObject NomTxtPln;
        JSObject MesDigTxt;

        public void init()
        {
                Ventana=JSObject.getWindow(this);
                // Se asigna la ventana en la cual se esta ejecutando el applet

                Documento=(JSObject) Ventana.getMember("document");
                // Se asigna la página Web en la cual se esta ejecutando el applet

                Forma=(JSObject) Documento.getMember("forma");
                // Se toma la forma que se encuentra dentro del documento

                NomTxtPln=(JSObject) Forma.getMember("T_Entrada");
                // Se asigna la caja de texto de entrada dentro de la forma

                MesDigTxt=(JSObject) Forma.getMember("T_Salida"),
                // Se asigna la caja de texto de salida dentro de la forma
        }
        // El método init() sirve para dar de alta los objetos de la página Web
        // y que estos sean reconocidos por el applet.

        public void Metodo1()
        {
                try
                {
                        String CadEnt=(String) NomTxtPln.getMember("value");
                        // Se asigna el contenido de la caja de texto a una cadena

                        ClaseCifrador CIF = new ClaseCifrador(CadEnt);
                        // Se efectúa el cifrado

                        String CadSal = Conversion byteArrayToHexString(CIF),
                        // Se transforma el contenido a Hexadecimal

                        MesDigTxt.setMember("value",CadSal),
                        // Se asigna el resultado de la operación a la caja de texto de salida
                }
                catch (NoSuchAlgorithmException e)
                {
                        System.out.println("No pudo efectuarse el cifrado");
                        System.exit(0);
                        // Mensaje de error
                }
        }
        // Este método es el encargado de efectuar las operaciones
}
```

Debe hacerse notar que en este ejemplo no están definidas las clases "ClaseCifrador" y "Conversion" ya que el análisis de los mismos es un tema extenso. Sin embargo, estas notas sirven para darse cuenta del proceso general usado para la definición de interfases.

Anexo G: Factores a Considerar al Comprar por Internet

1. No proporcionar información de su Tarjeta de Crédito, Cuentas de Inversión o Cheques para navegar a través de Internet, a menos que hayas solicitado algún producto o servicio.

2. Verificar que las páginas sean seguras (deberá aparecer un candado cerrado en la esquina inferior).

3. Sólo proporcionar datos confidenciales a sitios que cuenten con prestigio y que ya sean conocidos por usted.

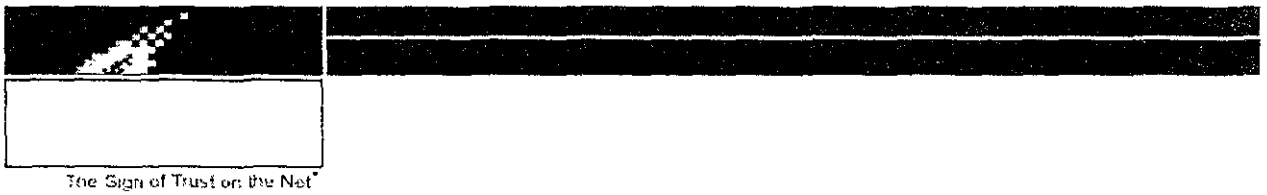
4. Nunca proporcionar a terceros el código de seguridad o password que asignan algunos sitios para efectuar compras.

5. Leer cuidadosamente los términos de uso y garantía.

6. Conservar el folio, comprobante o cualquier dato que respalde la compra.

7. Asegurarse de que el comercio no realice cargos a su cuenta después de que la compra sin que así usted haya solicitado.

8. Cerciorarse de que el sitio comercial cuente con una página o un certificado emitido por un tercero confiable a través del cual usted pueda comprobar la seriedad del negocio. A continuación se muestra un ejemplo:



The Sign of Trust on the Net™

WWW.SUBMARINO.COM.MX is a VeriSign Secure Site

Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.

Name	WWW.SUBMARINO.COM MX
Status	**Valid**
Validity Period	24-Nov-2000 - 21-Dec-2001
Server ID Information	Country = MX State = Distrito Federal Locality = Mexico City Organization = Submarinet SA de CV Organizational Unit = Submarino Mexico Organizational Unit = Terms of use at www.verisign.com/rpa (c)00 Common Name = www.submarino.com.mx

If the information is correct, you may submit sensitive data (e.g , credit card numbers) to this site with the assurance that:

- This site has a VeriSign Secure Server ID.
- VeriSign has verified the organizational name and that SUBMARINET SA DE CV has the proof of right to use it.
- This site legitimately runs under the auspices of SUBMARINET SA DE CV

- All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties.

To ensure that this is a legitimate VeriSign Secure Site, make sure that:

1. The original URL of the site you are visiting comes from WWW.SUBMARINO.COM MX.
2. The URL of this page is https://digitalid.verisign.com.
3. The status of the Server ID is Valid

Figura G-1. Página "Web" de un sitio seguro para comercio electrónico

Anexo H: Manejo de Audio en Java

H.1 Introducción al API de Sonido de Java ("Java Sound API")

El API de sonido de Java es una aplicación de bajo nivel que controla las salidas y entradas de sonido, incluyendo tanto audio digitalizado como datos provenientes de la Interfase Digital de Instrumentos Musicales ("Musical Instrument Digital Interface, MIDI"). El API de Sonido de Java provee control explicito sobre las capacidades normalmente requeridas para las entradas y salidas de sonido.

H.2 Muestreo de Audio

Una señal de audio es una señal u onda que puede ser medida y transformada, mediante el uso de micrófonos, de una señal acústica (compresión de aire que viaja por la atmósfera) a una señal eléctrica. Posteriormente, esta señal eléctrica pasa a través de un convertidor analógico-digital y mediante un proceso de muestreo se obtiene su representación digital. El muestreo, se refiere a tomar valores de la señal en determinados intervalos de tiempo. Esto puede observarse en la figura siguiente:

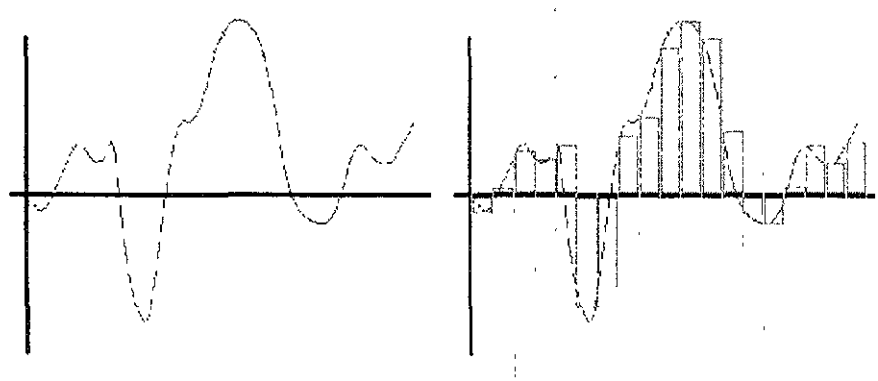


Figura H-1: Señal de Audio y Muestreo

El API de sonido de Java no especifica una configuración de hardware de audio; este ha sido diseñado para permitir que diferentes componentes puedan ser instalados sobre el sistema y accedan a él a través del API.

En este ejemplo, un dispositivo tal como una tarjeta de sonido tiene varios puertos de entrada y de salida, y mezcla todas ellas a través de software. El mezclador puede recibir datos que provengan de un archivo, un flujo de una red, son generados "al vuelo" por un programa de aplicación, o son producidos por un sintetizador de audio.

H.3 ¿Qué es MIDI?

A diferencia de un sonido muestreado, el cual es una representación de dicho sonido en sí mismo, la información de MIDI solo especifica como crear un sonido, especialmente sonidos musicales. La información MIDI no describe sonidos directamente; de hecho, sólo describe eventos que afectan al sintetizador de sonido. De esta forma, MIDI se comporta como un enorme piano en el que, a través de las teclas, los pedales, "switches" y demás controles, genera sonidos.

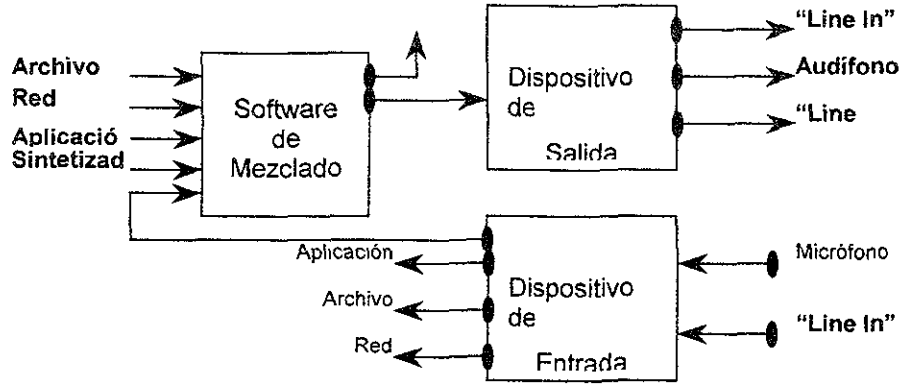


Figura H-2: Arquitectura de Audio Típica

H.4 Interfases para Proveedores de Servicios

Además de los paquetes propios de Java para el manejo de archivos y la configuración de sonido del sistema (javax.sound sampled y javax.sound.midi), existen dos paquetes más (javax.sound.sampled.spi y javax.sound.midi.spi) que permiten a los desarrolladores crear nuevos recursos para audio común y MIDI.

La implementación del API de sonido de Java permite manejar los servicios básicos de sonido, a través de la Interfase para Proveedores de Servicio (SPI) pueden ser creados servicios adicionales más sofisticados.

H.5 Revisión General del Paquete "javax.sound.sampled"

Este paquete centra su trabajo en el transporte de los datos de audio. Su tarea principal será cómo mover los bytes de audio formateado hacia y fuera del sistema. Estas tareas involucran: abrir y cerrar archivos y administrar "buffers" (almacenes temporales) para producir sonido en tiempo real.

"Streaming" (flujo) es la palabra con la que nos referimos a un movimiento constante de bytes que generan audio en tiempo real. En otras palabras, un flujo de audio es simplemente un conjunto continuo de información de sonido que llega más o menos a la misma velocidad a la que se almacena o reproduce. En el modelo de flujos, particularmente para el caso del audio, usted no necesita saber de antemano que tan grande es el archivo de sonido y cuando terminará este de llegar. Simplemente se requiere de un "buffer" de audio que almacene temporalmente los datos hasta su reproducción o almacenamiento definitivo.

Por otro lado, cuando los datos son reproducidos desde un archivo, el API de sonido de Java permite reproducir el sonido sin necesidad de crear un "buffer" Esto se debe a que el programa asume que se tiene todo el archivo de datos necesario y además, dicho archivo no es tan grande

como para saturar la memoria. En este caso, todo el archivo de sonido puede ser precargado completo en la memoria para su reproducción tantas veces como se desee. Por esta misma razón, al momento de reproducir un archivo que se encuentra almacenado, su reproducción se efectúa de forma casi instantánea.

H.6 Formatos de Audio para Datos y Archivos

Por formato de audio nos referimos a la forma en la que se representa el sonido de acuerdo a un cierto estándar. El API de sonido de Java distingue entre formatos de datos y formatos de archivos.

Un formato de datos nos habla de la forma en la cual se interpretan los bytes en bruto. Los formatos de datos están representados por el objeto "*AudioFormat*", el cual incluye los siguientes atributos:

- Técnica de codificación
- Número de canales
- Tasa de muestreo
- Número de bits por muestra
- Tasa de trama ("frame")
- Tamaño del trama ("frame") en bytes
- Orden de los bytes.

Una trama es un contenedor que lleva los datos de todos los canales en un momento determinado. Para un codificador PCM, las tramas simplemente son un conjunto simultaneo de muestreos en todos los canales.. En este caso además, la tasa de la trama es igual a la tasa de muestreo. Por otra parte, para otro tipo de codificadores la tasa de "frame" puede ser completamente diferente a la tasa de muestreo. Por ejemplo, un archivo codificado en MP3 (el cual no esta especificado directamente por el API de sonido de Java y debería ser soportado por una implementación de otro proveedor de servicio), cada trama contiene un conjunto de datos comprimidos para una serie de muestras, no solo una muestra por canal. Debido a que cada trama encapsula una serie completa de muestras, la tasa de trama es más lenta que la tasa de muestreo.

Por otro lado, los formatos de archivos especifican la estructura del archivo de sonido incluyendo no sólo los datos de sonido "en crudo", sino toda la información almacenada en el archivo.

Los diferentes formatos de sonido tienen diferentes estructuras Estos formatos pueden tener diferentes arreglos de datos en la cabecera del archivo. Una cabecera contiene información descriptiva que típicamente precede la información de audio muestreada.

Los formatos de archivo del API de sonido de Java está representado por el objeto "*AudioFileFormat*", los cuales contienen:

- El tipo de archivo
- La longitud del archivo en bytes
- La longitud, en tramas, de los datos de audio contenidos en el archivo
- Un objeto "AudioFormat" que especifica los datos del formato de audio del archivo

Cabe destacar que, el API de sonido de Java maneja de forma directa archivos de sonido codificados mediante un PCM lineal. De esta forma, los formatos de archivo que maneja este API de forma "natural" son:

1. .WAV formato para PC's
2. .AIFF formato para Mac
3. .AU formato para UNIX

H.7 ¿Qué es un Mezclador?

Muchos API's de sonido hacen uso de la noción de dispositivos de audio. Un dispositivo es comúnmente un software de interfase para un dispositivo físico de entrada o salida.
En el API de sonido de Java, los dispositivos son representados por un objeto llamado "Mixer" (Mezclador). El propósito de este objeto es un manejador de uno o más flujos de audio tanto de entrada como de salida. Un objeto mezclador represa las capacidades que tienen varios dispositivos físicos para conjuntar o mezclar información de audio.

Para entender como funciona este objeto, tómese como referencia una mezcladora de audio como la usada en los sistemas de sonido profesionales.

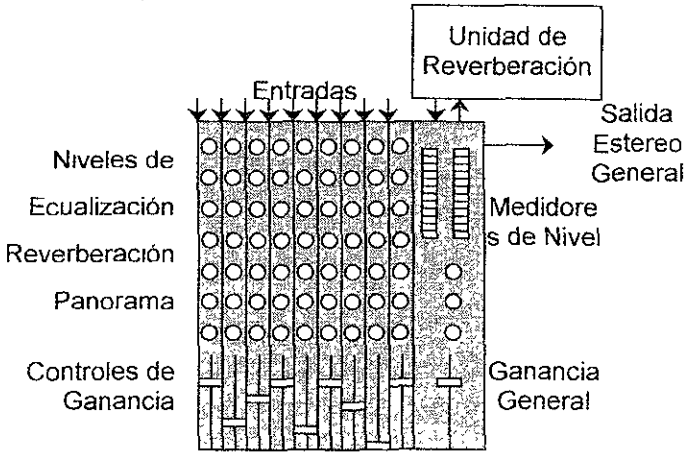


Figura H-3. Consola de Mezclado Profesional

Una mezcladora profesional tiene pistas, cada una de las cuales representa una dirección a través de la cual una señal simple de audio pasa a través de la mezcladora para su procesamiento. La pista tiene perillas y otros controles a través de los cuales puede ajustarse el volumen y el "panorama" (colocación de la imagen estéreo) de la señal. También el mezclador tiene un bus separado para efectos de reverberación, y este bus se conecta con una unidad interna o externa de reverberación. Una mezcladora profesional envía la serie se señales procesadas y mezcladas como una señal única a un bus de salida, el cual típicamente va a una unidad de almacenamiento ("cassette") o a algún altavoz

H.8 ¿Qué es una Línea?

Una línea es un elemento de audio digital que dirige el movimiento de los datos de audio a través del sistema. Usualmente, la línea es un canal de entrada o salida del mezclador. Los puertos de entrada y salida del objeto Mixer también son líneas. Otro tipo de líneas son aquellos que resultan ser entradas o salidas de los programas de aplicación de sonido Estos canales o rutas son análogos a las pistas ("tracks") de un reproductor multipistas conectado a una mezcladora profesional.

Una diferencia importante entre las líneas del API de sonido de Java y las líneas de una mezcladora profesional física, es el hecho de que una línea en el API puede ser mono o multicanal (estéreo)

H.9 Revisión General del Paquete "javax.sound.midi"

El estándar MIDI define un protocolo de comunicación para dispositivos de música electrónica, tales como teclados electrónicos y computadoras personales. Los datos MIDI pueden ser transmitidos sobre cables especiales durante conciertos en vivo o pueden ser almacenados, bajo un estándar especial, en archivos que posteriormente serán reproducidos y/o editados.

MIDI es tanto una especificación de "hardware" como de "software". Para entender el diseño de MIDI debemos entender que este fue diseñado pensando en reproducir eventos que suceden en instrumentos electrónicos (tal como pulsar una tecla) o por instrucciones enviadas desde una PC al sintetizador de audio.

Los dispositivos de "hardware" conocen o tienen almacenadas secuencias de notas que son reproducidas por el sintetizador, permitiendo al músico o compositor "tocar" determinada melodía en vivo. Posteriormente, fueron desarrolladas interfases que permiten conectar los instrumentos musicales con el puerto serial de una computadora; de esta forma, se pueden manipular computacionalmente las entradas de este puerto. Hoy en día sin embargo, mediante la incorporación de tarjetas de audio que tienen integradas microcircuitos capaces de efectuar todo el trabajo del sintetizador MIDI, muchos usuarios se limitan únicamente a trabajar con el sintetizador de música digital.

La especificación de MIDI destinada a los elementos de hardware, detalla el uso y función de cada uno de los "pines" para los cables de las interfases MIDI. Por su parte, la porción de la especificación que explica los lineamientos generales que debe seguir la implementación en software, se concentra en la estructura de datos y como los dispositivos sintetizadores deben responder a ellos, es decir, como deben reproducirlos. Es importante entender que los datos MIDI pueden ser secuenciados o moverse en flujo.

H.10 Flujo de Datos MIDI

En la primera parte de la especificación de MIDI se describe lo que es conocido como "protocolo de línea MIDI". Este protocolo el cual fue el primero en ser creado, asume que los datos MIDI proceden de un cable o interfase MIDI. Este cable transmite señales digitales desde un dispositivo MIDI a otro; dichas señales, al llegar al sintetizador, son reproducidas.

Los diferentes tipos de mensajes se distinguen por el primer byte en el mensaje, conocido como el byte de estatus. Los bytes posteriores a este se conocen como bytes de datos.

El protocolo de línea de MIDI define un modelo de flujo de datos para MIDI. De esta forma, cuando se trabaja con este protocolo, se asume que los datos deberán ser reproducidos (o tocados) conforme estos van llegando Los datos en si poseen la información de sincronización y cada evento es procesado conforme en recibido y se asume que todos llegan en el tiempo correcto.

H.11 Secuencias de Datos en MIDI

Por otra parte, el estándar de archivos de MIDI es la parte de la especificación que limita al protocolo de línea en cuando a que para que el primero funcione, requiere adicionalmente de una señal de sincronía

Un archivo MIDI es un archivo digital que contiene eventos que deberán ser reproducidos por el sintetizador en cualquier momento posterior a su creación, por esta razón, y a diferencia del

protocolo de línea el cual se reproduce sobre la marcha, es necesario una pieza adicional de información que indique en que momento debe ocurrir cada evento.

Esta información adicional en un archivo MIDI se conoce como secuencia. Un archivo MIDI estándar contiene una o más pistas, por esta razón, la secuencia es un bit que se coloca en determinados puntos del archivo para "orquestar" la reproducción.

Glosario

- A -

Acceso legal: Acceso por parte de terceras personas o entidades, incluyendo gobiernos, al texto en claro, claves criptográficas, y/o datos cifrados, de acuerdo a ley.

Active Server: Una colección de tecnologías de servidor que se entregan con Windows NT. Estas tecnologías proporcionan un modelo de componentes y secuencias de comandos coherente de servidor, así como un conjunto integrado de servicios del sistema para administración de las aplicaciones componentes, acceso a bases de datos, transacciones y mensajería.

Active X: Conjunto de tecnologías de Microsoft las cuales permiten interactividad con el material existente en el WWW.

Address Resolution Protocol (ARP): Protocolo de Resolución de Direcciones. Es el protocolo de Internet utilizado para crear un mapa dinámico de las direcciones en las áreas de red locales. Permite la conversión de una dirección Internet en una dirección numérica.

Administrador de transacciones: Un servicio del sistema responsable de coordinar el resultado de las transacciones con el fin de conseguir atomicidad. El administrador de transacciones asegura que los administradores de recursos toman decisiones coherentes sobre si la transacción debe realizarse o no.

ADO (ActiveX Data Objects): Objetos ActiveX para Datos. Un conjunto de interfaces de acceso a datos, basadas en objetos y optimizadas para las aplicaciones enfocadas a Internet y centradas en manejo de datos. ADO está basado en una especificación publicada y se incluye con Microsoft Internet Information Server y con Microsoft Visual InterDev.

Advanced Research Projects Agency Network (ARPANET): Red pionera de Internet fundada por ARPA -una agencia gubernamental norteamericana del Departamento de Defensa- en 1969. ARPANET conectaba ordenadores que intercambiaban paquetes de información mediante lineas en "leasing" y sus investigaciones en redes sirvieron de base para el actual sistema.

Algoritmo: Regla o proceso a seguir para realizar una tarea o llegar a la solución de un problema.

Amenaza: Circunstancia o evento que puede causar una denegación de servicio o una destrucción, revelación o modificación de datos no autorizada

American National Standards Institute (ANSI): Instituto Nacional Americano de Normas. Organización encargada de aprobar las normas con que se rigen diferentes sectores en los Estados Unidos -incluyendo ordenadores y comunicaciones- y en la que se agrupan asociaciones profesionales, compañías y asociaciones gremiales; es miembro de la International Organization for Standardization (ISO).

Applet: Programa o aplicación de pequeño tamaño – comúnmente programado en el lenguaje Java de Sun Microsystems.

API (Application Program Interfaces): Interfaces de Programación de Aplicaciones. Un conjunto de rutinas que un programa de aplicación utiliza para solicitar y efectuar servicios de nivel inferior ejecutados por el sistema operativo de un equipo. También es un conjunto de convenciones de llamada en programación que definen cómo se debe invocar un servicio a través de la aplicación.

Arquitectura Cliente-Servidor: Un modelo de computación mediante el que las aplicaciones cliente que se ejecutan en un escritorio o en un equipo personal tienen acceso a la información contenida en servidores remotos o en equipos "host". La parte cliente de la aplicación suele estar optimizada para la interacción con el usuario, mientras que la parte servidor proporciona la funcionalidad centralizada multiusuario.

Asociación Mexicana de Estándares para el Comercio Electrónico (AMECE): Organismo de reciente creación cuya misión es la de normalizar las reglas y formatos a utilizar en el comercio electrónico. Interactúa con organismos públicos nacionales, en especial la SHCP de México, así como con organismos internacionales e instituciones privadas.

Autentificación: Proceso por el cual se garantiza que el usuario que accede a un sistema de ordenador es quién dice ser. Por lo general, los sistemas de autenticación están basados en el cifrado mediante una clave o contraseña privada y secreta que sólo conoce el auténtico emisor.

Autoridad Certificadora: Entidad que da testimonio de la pertenencia o atribución de una determinada firma digital a un usuario o a otro certificador de nivel jerárquico inferior.

Autorización: En lo referente a equipos, especialmente a equipos remotos de una red que están disponibles para más de una persona, el permiso concedido a un individuo para usar el sistema y los datos almacenados en él. La autorización la establece normalmente un administrador del sistema y la comprueba y acepta el equipo. Esto requiere que el usuario proporcione algún tipo de identificación, como un código o una contraseña, que el equipo pueda comprobar con sus registros internos. Los términos permiso y privilegio son sinónimos de autorización.

- B -

Browser: Navegador, visualizador; programa o aplicación para navegar a través del Web (WWW), tal como Netscape o Internet Explorer. Permite al usuario acceder a documentos, imágenes y ficheros localizados en servidores "Web".

Bug: Fallo de diseño o seguridad en un programa o equipo.

- C -

Certificado Digital: Un archivo, obtenido de una entidad emisora de certificados, que se utiliza para comprobar el origen de los datos enviados a través de una red; también se denomina certificado de autentificación.

Cifrado: Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave. Véase la sección 1.2 del presente documento donde se da un análisis más detallado del uso de este término.

Cheats: Códigos especiales que permiten hacer trampa en un programa.

Clave criptográfica: Parámetro que se utiliza junto con un algoritmo criptográfico para transformar, validar, autentificar, cifrar o descifrar datos.

Clave de sesión / Clave de cifrado: Clave utilizada en algoritmos simétricos para cifrar y descifrar los mensajes en una única sesión

Clave Privada: Clave personal que no es conocida por el resto de los usuarios y que es utilizada para crear firmas digitales y, dependiendo del algoritmo, para descifrar mensajes cifrados con la correspondiente clave pública.

Clave Pública: Clave de usuario que es conocida por el resto de los usuarios y que es utilizada para verificar firmas. Dependiendo del algoritmo, se usa para cifrar mensajes que pueden ser descifrados con su correspondiente clave privada.

Clave Simétrica: Clave única usada en los algoritmos simétricos tanto para cifrar como para descifrar un mensaje.

Código de bytes: El formato ejecutable de código Java que se ejecuta en la Máquina Virtual de Java ("Java Virtual Machine", JVM) Java. También se denomina código interpretado, pseudo código, "byte code" y p-code.

Cookie: Fichero de texto instalado en el directorio del navegador, en el que se guarda información sobre preferencias del usuario y datos diversos, que activan ciertas respuestas por parte de otros sistemas a los que se conecta.

Confidencialidad: Característica o atributo de la información por el cual la misma sólo puede ser revelada a los usuarios autorizados en tiempo y forma determinados.

Control de acceso: Los elementos e instrumentos de salvaguarda necesarios para garantizar a los usuarios la seguridad de los datos y demás activos del sistema de comunicación y sus aplicaciones.

Correo Electrónico (E-mail): Un sistema mediante el cual un usuario de un equipo puede intercambiar mensajes con otros usuarios (o grupos de usuarios) por medio de una red de comunicaciones. El correo electrónico es una de las aplicaciones más populares de Internet.

Cracker: Intruso; individuo que intenta penetrar en un ordenador o sistema informático, ilegalmente y generalmente con intenciones malsanas -a menudo confundido con hacker.

Criptografía: Ciencia que mediante el tratamiento de la información, protege a la misma de modificaciones y utilización no autorizada. Utiliza algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro extremo.

- D -

Datos: Representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas.

Datos personales: Cualquier información referente a una persona identificada,

Depositario de la clave: Persona o entidad que está en posesión o tiene el control de las claves criptográficas. El depositario de la clave no es necesariamente el usuario de la misma.

DES: Data Encryption Standard. Algoritmo de cifrado / descifrado, diseñado y reglamentado en EEUU.

Descifrado: Función inversa al cifrado.

DHTML: HTML dinámico. Un conjunto de innovadoras características presentes en Internet Explorer versión 4.0 que pueden usarse para crear documentos HTML que cambian su contenido dinámicamente e interactúan con el usuario. Al usar DHTML, los autores pueden aportar a las páginas "Web" efectos especiales sin depender de programas del servidor.

Disponibilidad: El hecho de ser accesibles y utilizables los datos, informaciones o sistemas de información en el tiempo deseado y del modo requerido.

- E -

EDI (Electronic Data Interchange): Intercambio Electrónico de Datos. Protocolo creado a principios de los años 70 para permitir, a las grandes compañías, la transmisión de información a través de sus redes privadas; y el cual se ha tratado de adaptar a los actuales sitios "Web" corporativos.

Encriptación: Acción de proteger la información mediante técnicas criptográficas ante modificaciones o utilización no autorizada. Véase la sección 1.2 del presente documento donde se da un análisis más detallado del uso de este término.

Entidad Emisora de Certificados (Certificate Authorithy): Una entidad que emite, administra y revoca certificados.

Excepción: Una condición anormal o error que se produce durante la ejecución de un programa y que requiere la ejecución de software fuera del flujo normal de control.

- F -

FAQ (Frequently Asked Questions): Preguntas Frecuentemente Preguntas. Lista de preguntas que se efectúan con gran frecuencia, y sus respuestas. Existen cientos de FAQs sobre los temas más diversos y su objetivo es evitar un aluvión de preguntas obvias - sobre todo a los "newsgroups".

File Transfer Protocol (FTP): Protocolo para la Transferencia de Archivos. Protocolo que permite enviar y recibir ficheros - de un ordenador a otro - dentro de Internet; hay miles de sitios en la red que ofrecen ficheros y programas de todo tipo de forma desinteresada.

Finger: Programa diseñado para localizar individuos o usuarios de la Red, recogiendo información tal como nombre real, correo sin leer, última vez que se conectaron, etc. (algunos servidores rechazan los pedidos de "finger" que les llegan).

Firewall: Traducido literalmente *muro de fuego*; conceptualmente significa *muro corta-fuego* en la lengua inglesa . Se trata de un programa y/o equipo que protege a una red de otra red. En su concepción más simple, el "firewall" permite que una máquina acceda a Internet desde una red local, pero impide que las otras máquinas fuera de esa red accedan a la máquina.

Firma digital: Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Consiste en una transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posea el mensaje inicial y la clave pública del firmante, pueda determinar de forma fiable si dicha transformación se hizo utilizando la clave privada

correspondiente a la clave pública del firmante, y si el mensaje ha sido alterado desde el momento en que se hizo la transformación. Es un sello integrado en datos digitales, creado con una clave privada, que permite identificar al propietario de la firma y comprobar que los datos no han sido falsificados.

- G -

Gateway: Pasarela, dispositivo, ordenador o programa que conecta redes - que normalmente serían incompatibles - permitiendo el intercambio de información entre ellas; también llamado "router".

Gopher: Sistema de búsqueda de documentos y ficheros mediante menús jerárquicos del material disponible en Internet: el usuario utiliza un programa "gopher" que accede a la información de cualquier "gopher" accesible y la suministra de forma unificada. El World Wide Web (WWW), más moderno, lo está suplantando con su hipertexto.

- H -

Hacker: Experto en los entresijos de programas, ordenadores, sistemas, redes en general e Internet en particular. En lenguaje de la Red, el "hacker" es un personaje no perjudicial quien no debe ser confundido con el "cracker" .

HTML (HyperText Markup Language): Lenguaje de Marcaje de Hiper Texto. Lenguaje utilizado en el WWW para crear páginas "Web" que se conectan con otros documentos - se trata de códigos que dictan el formato y composición de la página, estructurándola de forma que sea accesible y creando enlaces con otras páginas o ficheros de la red.

HTTP (HiperText Transfer Protocol): Protocolo para transferir ficheros o documentos en el WWW.

- I -

Integridad: Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

International Organization for Standardization (ISO): Organización Internacional para la Normalización. Organización fundada en 1946 responsable de establecer normas internacionales en diversas áreas - incluyendo comunicación e información.

Interfaz: Un grupo de operaciones o métodos relacionados lógicamente que proporciona acceso a un objeto componente.

Interoperabilidad: Interoperabilidad de métodos criptográficos es la capacidad técnica de que varios métodos criptográficos funcionen conjuntamente.

Intranet: Red de comunicación interna o privada que utilizan empresas u organizaciones, diseñada en base a los protocolos de Internet y que puede estar o no conectada a Internet.

IP (Internet Protocol): Protocolo de Interred. Protocolo estándar utilizando por los sistemas que se comunican por el Internet.

ISAPI (Internet Server Application Program Interfaces): Interfaz de Programación de Aplicaciones de Servidor Internet. Una interfaz de programación de aplicación que reside en un equipo servidor para el inicio de los servicios de software ajustados para el sistema operativo Microsoft Windows NT. Es una API para desarrollar extensiones para Microsoft Internet Information Server y otros servidores HTTP compatibles con la interfaz ISAPI.

ISP (Internet Services Provider): Proveedor de Servicios de Internet. Es una organización, una compañía o una institución docente, que permite a los usuarios remotos tener acceso a Internet proporcionándoles conexiones de acceso telefónico o mediante la instalación de líneas dedicadas.

- J -

Java: Lenguaje de programación desarrollado por Sun Microsystems con un código compatible con todas las plataformas de ordenadores, por lo que puede ser recibido a través de Internet y utilizado de inmediato sin temor a virus o daño a los ficheros.

JavaScript: Un lenguaje de secuencias de comandos que evolucionó a partir del lenguaje "LiveScript" de Netscape y que se hizo más compatible con Java. Utiliza una página HTML como interfaz.

- K -

Kerberos: La base de la mayoría de los servicios de seguridad del Entorno de Computación Distribuida (Distribuited Computing Enviroment, DCE). Kerberos proporciona un uso seguro de los componentes de software distribuidos.

- Ll -

Llave (Key): Frase o conjunto de caracteres que permiten descodificar un mensaje cifrado.

- M -

Máquina Virtual Java: El mecanismo que el lenguaje Java utiliza para ejecutar el código de bytes de Java en un equipo físico. La máquina virtual convierte el código de bytes a la instrucción nativa del equipo de destino.

Métodos criptográficos: abarca las técnicas, servicios, sistemas, productos y sistemas de gestión de claves criptográficas.

- N -

Navegador. Véase Browser.

No repudio: Propiedad que se consigue por medios criptográficos, que impide a una persona o entidad negar haber realizado una acción en particular relativa a datos (como los mecanismos de no rechazo de autoría (origen); como demostración de obligación, intención o compromiso; o como demostración de propiedad).

Notario Electrónico (Trusted Third Parties, TTP): Entidad pública o privada encargada de la emisión de certificados digitales que atestigüen la autenticidad de los propietarios de los mismos.

- O -

Objeto: Es la unidad básica de la programación orientada a objetos, la cual comprende rutinas y datos, y es tratada como una entidad discreta. Un objeto se basa en un modelo específico, donde un cliente que utiliza los servicios de un objeto obtiene acceso a los datos del objeto a través de una interfaz que consta de un conjunto de métodos o funciones relacionados. El cliente puede llamar después a estos métodos para realizar operaciones.

ODBC (Open DataBase Connectivity): Conectividad Abierta a Bases de Datos. Una interfaz de programación de aplicaciones que permite a las aplicaciones tener acceso a datos desde diversas especificaciones estándar de orígenes de datos para acceso a bases de datos multiplataforma.

Operadores de red: Entidad pública o privada que haga disponible la utilización de una red de telecomunicación.

OSI (Open Systems Interconnection): Interconexión de Sistemas Abiertos. Arquitectura modular para red desarrollada por la ISO, la cual usa siete capas para soportar comunicaciones abiertas entre equipos de diferentes fabricantes.

- P -

Página "Web": Un documento de la WWW. Las páginas pueden contener prácticamente cualquier cosa, por ejemplo noticias, imágenes, peliculas y sonidos.

Páginas de Servidor Activo (Active Server Pages, ASP): Un entorno de secuencias de comandos de servidor que ejecuta secuencias de comandos ActiveX y componentes ActiveX en un servidor. Los programadores pueden combinar secuencias de comandos y componentes para crear aplicaciones basadas en "Web".

PGP (Pretty Good Privacy): Privacidad Bastante Buena Programa de libre distribución, escrito por Phil Zimermann; el cual impide mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser interpretados por personas no autorizadas. También puede utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autentificación del autor

Proveedores de acceso: Organizaciones que suministran la infraestructura técnica necesaria para que los usuarios puedan conectarse a Internet. Para usuarios domésticos, lo habitual es utilizar una conexión a través de la red telefónica básica mediante un módem.

Proveedores de contenido: Personas u organizaciones que publican informacion de cualquier tipo en Internet, ya sea utilizando recursos propios o los suministrados por un proveedor de acceso

- Q -

Query: Consulta. Mensaje solicitando el valor de una variable o conjunto de variables.

- R -

RSA: Rivest-Shamir-Adleman. Algoritmo criptográfico de cifrado de clave asimétrica, utiliza una clave para cifrar y otra para descifrar.

- S -

SDK (Software Development Kit): Conjunto de herramientas para el desarrollo de software. Herramientas de una compañía específica, utilizadas por los programadores para crear nuevas aplicaciones.

Servidor "Web": Es el programa que, utilizando el protocolo de comunicaciones HTTP, es capaz de recibir peticiones de información de un programa cliente (navegador), recuperar la información solicitada y enviarla al programa cliente para su visualización por el usuario.

Servidor "Web" seguro: Servidor "Web" que utiliza protocolos de seguridad (SSL, S-HTTP o PCT) al ejecutar transacciones con él. Un protocolo de seguridad utiliza técnicas de cifrado y autenticación como medios para incrementar la confidencialidad y la fiabilidad de las transacciones.

SET (Secure Electronic Transactions): Transacciones Electrónicas Seguras. 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 encriptando 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 MasterCard y tiene un amplio apoyo de la comunidad bancaria mundial.

Sistema de gestión de claves: Sistema para la generación, almacenamiento, distribución, revocación, eliminación, archivo, certificación o aplicación de claves criptográficas.

Sistemas de información: Ordenadores, instalaciones de comunicación y redes de ordenadores y de comunicación, así como los datos e informaciones que permiten conservar, tratar, extraer o transmitir, incluidos los programas, especificaciones y procedimientos destinados a su funcionamiento, utilización y mantenimiento.

Sniffer: Programas utilizados por los "crackers" y "hackers" para recabar información no cifrada de una red, principalmente nombres de usuario y contraseñas; para luego utilizarla en ataques y entradas a ordenadores.

SSL (Secure Sockets Layer): Capa de Conectores Seguros. Protocolo, creado por Netscape, para crear conexiones seguras al servidor, de tal modo que la información viaja encriptada a través de Internet.

- T -

TCP/IP (Transmission Control Protocol / Internet Protocol): Protocolo para Control de Transmisión/ Protocolo de Interred. Conjunto de protocolos que definen Internet, permitiendo que diferentes tipos de ordenadores - con diferentes sistemas operativos - se comuniquen entre sí.

Telnet: Protocolo de comunicaciones estándar que conecta un ordenador con Internet, convirtiéndolo en una terminal del sistema.

- U -

URL: Acrónimo de Universe Resource Locator. Este término hace referencia a una dirección web.

- W -

World Wide Web (WWW, Web, W3): Telaraña de Alcance Mundial. Sistema de información global distribuido desarrollado por investigadores del CERN en Suiza, que utiliza el protocolo HTTP para enlazar páginas mediante mecanismos de hipertexto (lenguaje HTML).

Worm (Gusano): También conocido como "Great Worm", fue introducido por Robert T. Morris en Internet en noviembre de 1998 y se propagó de tal manera que colapsó más de seis mil sistemas.

- X -

X509: Norma estándar que define un entorno de autentificación y seguridad. Forma parte de la norma X.500 de UIT -T.

Bibliografía y Referencias

Libros

1 **Baker, David**
Et al.
Java Expert Solutions
1ª. Edición
EE.UU., QUE Corporation, 1997
ISBN 0-7897-0935-x

2 **Bobadilla Sancho, Jesús**
Alonso Villaverde, Santiago
HTML Dinámico a través de Ejemplos
1ª. Edición
España, Editorial Alfaomega, 2000
ISBN 970-15-0506-9

3 **Bobadilla Sancho, Jesús**
et al.
HTML Dinámico, ASP y JavaScript
1ª. Edición
España, Editorial Alfaomega, 2000
ISBN 970-15-0530-1

4 **Cohan, Peter**
El negocio está en Internet
1ª. Edición
México, Pearson Educación, 2000
ISBN 970-17-0371-5

5 **Cooper, Frederic**
et al.
Implementing Internet Security
1ª. Edición
E.E.U.U., New Riders Publishing, 1995
ISBN 1-56205-471-6

6 **Danesh, Arman**
Tatters, Wes
1ª. Edición
JavaScript 1.1 Developer's Guide
E E.U.U., Editorial Prentice Hall, 1997

7 **Dertouzos, Michael**
¿Qué será? (cómo cambiará nuestras vidas el nuevo mundo de la informática)
1ª. Edición
México, Editorial Planeta, 1997
ISBN 968-406-597-3

8 **Doherty, Donald**
Manning, Michelle
Aprendiendo Borland JBuilder 3 en 21 días
1ª. Edición
México, Pearson Educación, 1998
ISBN 970-17-0325-1

9 **Gates, Bill**
Los negocios en la era digital
1ª. Edición
México, Plaza & Janes Editores, 1999
ISBN 968-11-0353-X

10 **Halsall, Fred**
Comunicación de datos, redes de computadoras y sistemas abiertos
4ª. Edición
México, Pearson educación, 1998

11 **Hopson, K.C.**
Ingram, Stephen
Developing Professional Java Applets
1ª. Edición
E.E.U.U., SAMS Publishing, 1996
ISBN 1-57521-083-5

12 **Jaworski, Jaime**
Perrone, Paul
Java Security Handbook
1ª. Edición
E.E.U.U., SAMS Publishing, 2000
ISBN 0-672-31602-1

13 **Lemay, Laura**
Perkins, Charles L.
Aprendiendo Java 1.1 en 21 Días
1ª. Edición
México, Editorial Prentice Hall, 1998
ISBN 970-17-0054-6

14 **Mattelart, Armand**
La Comunicación-Mundo (historia de las ideas y de las estrategias)
1ª. Edición
México, Siglo Veintiuno Editores, 1996
ISBN 968-23-2016-X

15 **Menezes, Alfred**
et al.
Handbook of Applied Cryptography
4ª. Edición
EE.UU., Editorial CRC Press, 1997
ISBN 0-8493-8523-7

16 **Negroponte, Nicholas**
Ser digital
1ª. Edición
Mèxico, Editorial Océano de Méxìco, 1996
ISBN 968-6321-89-6

17 **Rumbaugh, James**
et al.
Modelado y diseño orientado a objetos (metodología OMT)
1ª. Edición
España, Prentice Hall Internacional, 1996
ISBN 0-13-240698-5

18 **Schneier, Bruce**
Applied Cryptography (protocols, algorithms and source code in C)
2ª. Edición
EE.UU., Editorial John Wiley &Sons, 1996
ISBN 0-471-11709-9

19 **Tanenbaum, Andrew S.**
Redes de Computadoras
3ª. Edición
México, Editorial Prentice Hall, 1997
ISBN 968-880-958-6

20 **Walnum, Clayton**
Java by Example
1ª. Edición
EE.UU., QUE Corporation, 1996
ISBN 0-7897-0814-0

21 **Walther, Stephen**
Levine, Jonathan
Aprendiendo Programación para E-Commerce con ASP en 21 dias
2ª. Edición
México, Pearson Educación, 2000
ISBN 968-444-528-8

Revistas y Publicaciones periódicas

22 **Bancomer**
Cuatro consejos para comprar por Internet
Publicación ENTRE AMIGOS, folletín informativo para tarjeta habientes de Bancomer
Enero 2001, México

23 **Castillo, Ulises**
Seguridad en Internet (partes 3 de 4)
ARTÍCULO Revista RED. la comunidad de expertos en redes
Mayo 2001, México, Páginas: 34-38

Páginas Web

35 ASP, SDK y Personal Web Server de Microsoft http://www.microsoft.com

36 Bouncy Castle http://www.bouncycastle.org

37 Código Fuente JavaScript y Java de RSA y SHA-1 http://pajhome.org.uk/crypt/

38 Code Signing for Java Applets http://www.suitable.com/Doc_CodeSigning.shtml

39 Counterpane http://www.counterpane.com

40 Cryptix http://www.cryptix.org

41 Criptografía http://www.dat.etsit.upm.es/~mmonjas/cripto/01.html

42 Estándar SHA-1 http://www.itl.nist.gov/fipspubs/fip180-1.htm

43 JDK 1.3 http://www.java.sun.com

44 RSA http://www.rsa.com

45 Seguridad en Redes http://www.map.es/csi/silice/Seg1.html

46 S-HTTP http://www.iec.csic.es/criptonomicon/shttp.html

47 VISA http://www.visa.com

Ayudas en línea

48 Documentación HTML del API del CryptixJCE

49 Documentación HTML del API del Cryptix3.x.x

50 Documentación HTML del API del JCE versiones Beta, EA y EA2, creadas por Sun Microsystems

51 Documentación HTML del API del JCE creado por Bouncy Castle

52 WinHelp para Sun-JDK 1.3.1 de Franck Allimant

53 WinHelp SDKDOCS de Microsoft JDK 4.0

54 WinHelp JAVADOCS de Microsoft JDK 4.0

55 WinHelp INTEGRATION de Microsoft JDK 4.0

Diccionarios

56 **Guardia, Remo**
Diccionario Porrúa de sinónimos y antónimos de la lengua española
7ª. Edición
México, Editorial Porrúa, 1992
ISBN 968-452-124-3

57 *The New Merriam-Webster Dictionary*
E.E.U.U , Merriam-Webster Inc. Publishers, 1989
ISBN 0-87779-900-8

58 **Ramón García-Pelayo y Gross**
Diccionario Pequeño Larousse Ilustrado
8ª. Edición
Francia, Imprimerie LAROUSSE, 1972
20541K-10-71

La presente tesis fue realizada para obtener el título de Ingeniero en Telecomunicaciones de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, y presentada por:

Gabriel Aldama Ramírez
Correo electrónico: gabo001@yahoo.com

José Francisco Mares Canales
Correo electrónico: paco_mc@hotmail com e ingmares@infosel.net.mx

Agosto 2001