MODELO PARA LA AUTOMATIZACIÓN DE PROCESOS DE IDENTIFICACIÓN PERSONAL EN APLICACIONES Y SERVICIOS TELEMÁTICOS

Diana Carolina Bernal Escobar
Carlos Mario Cadavid Ramírez

Trabajo de Grado presentado como requisito parcial para optar al titulo de Ingeniero en Electrónica y Telecomunicaciones

Director:
Gustavo Adolfo Ramírez
Ingeniero en Electrónica y Telecomunicaciones

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICAIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN
2005

CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

1. CAPITULO I. INTRODUCCIÓN

Alrededor del auge de nuevos servicios ofrecidos a través de vías electrónicas se ha abierto paso a la agilización de una serie de procesos que anteriormente requerían de la presencia física de los individuos en un lugar y tiempo determinados. Con las redes telemáticas han aparecido cualquier tipo de aplicaciones y servicios de comunicación, transferencia de información, transacciones comerciales, educación, entre otros, que permiten mejorar la calidad de vida de las personas.

De esta manera, la información se ha convertido en el eje central de muchas actividades que pueden contribuir en un beneficio personal, o en un crecimiento corporativo. Se pueden citar muchas razones para argumentar el papel de la información en nuestros tiempos, que destacan la importancia de la seguridad en el acceso y en su tratamiento.

Entre las ideas que dieron origen a este proyecto se encontraba la necesidad de identificar plenamente a los usuarios que accedían a estos servicios y proteger la información que éstos enviaban a través de la red.

Igualmente desde el comienzo se manejó una hipótesis que consistía en que si se encontraba un mecanismo que garantizara el cumplimiento de estas necesidades, y los usuarios lo asimilaban correctamente, se incrementaría la confianza de los usuarios y esto se reflejaría en una mayor utilización de estos servicios, en especial los que comprometen información muy sensible, por ejemplo la información de tarjetas de crédito o cuentas bancarias.

A partir se estas inquietudes se generó el proyecto de grado denominado “Modelo para la Automatización de Procesos de Identificación Personal en Aplicaciones y Servicios Telemáticos”. El título previo al finalmente establecido agregaba “mediante la utilización de tecnologías de información y comunicación asociadas a la seguridad (TIC_S)”, pero esta segunda parte fue sustraída por razones estéticas.

El punto de partida de la investigación fueron las TIC_S, de donde se encontraron dos vertientes muy importantes de profundización, que son precisamente las tecnologías SW asociadas al tema de criptografía de claves públicas, y las tecnologías HW relacionadas con dispositivos de identificación y captura automática de datos. Tanto por el lado de la identificación personal, como del aseguramiento de la información se encontraba la utilidad de estas dos ramas de las TIC_S, así como la forma en que se complementaban. Este bagaje tecnológico abrió el camino para relacionar toda una serie de conceptos que nos condujeron a abordar el planteamiento del presente modelo.

En el planteamiento del modelo, lo más complicado fue definir que componentes eran necesarios y que temas abarcarían, para ofrecer una visión completa de la automatización de procesos de identificación y la protección de la información transmitida, proporcionando elementos de contexto para su aplicación, tecnologías alternativas, posibles sistemas, arquitectura, políticas de implementación y gestión, entre

otros. Luego de varios esquemas iniciales, el resultado final recoge estos elementos en cuatro componentes constitutivos del modelo, que se describen y detallan en el capítulo respectivo. Estos fueron desarrollados uno a uno, en el orden en que se despliegan en esta monografía y estuvieron sujetos a varios procesos de refinamiento.

El prototipo que valida el modelo, es un servicio de compra de bienes con autenticación de usuarios e implementación de un método de pago por medio de debito electrónico. La selección de esta aplicación obedeció a la facilidad que prestaba para incluir muchos elementos del modelo, además de requerir una alta protección en materia de seguridad tratándose de transacciones con dinero electrónico.

2. CAPITULO II. ARQUITECTURAS Y PLATAFORMAS PARA APLICACIONES Y SERVICIOS TELEMÁTICOS

La creciente introducción de tecnologías de procesamiento informático distribuido ha dado como resultado el surgimiento y evolución de algunas plataformas para aplicaciones y servicios telemáticos, ellas permiten solventar las necesidades actuales y prestaciones exigidas a nivel empresarial en el aspecto de desarrollo informático.

Hasta cierto punto estas plataformas son rivales competitivos, de forma que en este capítulo se hace un esfuerzo por sintetizar las características y servicios de las tres principales plataformas existentes para el desarrollo de aplicaciones y servicios telemáticos distribuidos, estas son: CORBA, .Net y J2EE. Al Finalizar se presenta una matriz comparativa entre las tres plataformas.

Introducción

Con el desarrollo del World Wide Web, específicamente Internet, a los usuarios se les proporciona información de una manera visualmente agradable y ampliamente distribuida, razones a que han contribuido a su inmensa popularidad y crecimiento exponencial. Por consiguiente, se han introducido diversos paradigmas para presentar la información denominada hypermedia[1]. Esta tendencia comenzó en la última década con varias iniciativas, pero recientemente el foco de atención se ha dirigido hacia el empleo de las plataformas software especializadas en lograr estos objetivos.

Las plataformas software, se vuelven cada vez más necesarias en el desarrollo de aplicaciones y servicios telemáticos, especialmente a nivel empresarial, donde son requeridas para agilizar actividades donde la información es el eje central.

La necesidad de gestionar información es un factor muy común en las empresas, de manera que se están invirtiendo grandes capitales en la construcción y gestión de sistemas u aplicaciones que permitan capturar, procesar y compartir información entre distintos usuarios. Así, la adopción de nuevas tecnologías es un factor importante para explotar las capacidades de un manejo adecuado de la información.

2.1. Arquitecturas para Aplicaciones y Servicios Telemáticos

Antes de entrar a describir las plataformas para aplicaciones y servicios telemáticos es necesario hacer una descripción de las arquitecturas existentes para el desarrollo de los mismos (arquitecturas 2-capas, 3-capas n-capas), teniendo en cuenta que toda plataforma es la implementación de una arquitectura,

[1] Hypermedia, integración de gráficos, sonido y vídeo en un sistema que permite el almacenamiento y recuperación de la información de manera relacionada.

2.1.1. Arquitectura 2-capas

En una aplicación tradicional 2-capas, el procesamiento de carga es entregado al PC cliente, mientras el servidor simplemente actúa como un controlador de tráfico entre la aplicación y los datos. Los sistemas cliente-servidor típicos están basados en esta arquitectura, por lo cual hay una clara separación de los datos y la lógica de presentación/negocio. A pesar de que esta arquitectura nos permite compartir datos a través de la empresa, tiene muchos inconvenientes, como:

- La lógica de negocio puede ser compleja y como esta se ejecuta en el cliente obliga a disponer de potente hardware para su ejecución.
- Hay un gran acoplamiento en los componentes. Un pequeño cambio en el cliente obliga a distribuir la aplicación a todos los puntos donde se ejecuta la aplicación.
- Cada cliente tiene que abrir una conexión con el servidor.
- La cantidad de datos que se envía a través de la red suele ser bastante grande ya que no se ha procesado en el servidor.
- En el modelo de "servidor grueso" los procedimientos almacenados presentan grandes problemas de portabilidad.
- El servidor es accedido públicamente por lo que existen riesgos de seguridad.
- La extensibilidad es muy pobre ya que la lógica de negocio y el cliente se encuentran altamente acoplados.

2.1.2. Arquitectura 3-capas

Una aplicación 3-capas está dividida en tres capas separadas lógicamente, cada una con un conjunto de interfaces bien definidas. La primera capa, corresponde a la capa de presentación y básicamente consiste en una interfaz de usuario gráfica. La segunda capa, corresponde a la capa de negocio, que consiste en la lógica de negocio o de presentación, y la tercera capa corresponde a la capa de datos, que contiene los datos necesarios para la aplicación.

2.1.3. Arquitectura n-capas

En esta arquitectura la lógica de la aplicación está dividida por funciones, no físicamente. Este tipo de sistemas pueden soportar un número de diferentes configuraciones. Una arquitectura n-capas se descompone en:

- *Una interfaz de usuario*, que maneja la interacción del usuario con la aplicación.
- *La lógica de presentación*, que define lo que la interfaz de usuario debe desplegar y cómo deben ser tratadas las solicitudes de usuario.
- *La lógica de negocio*, que modela las reglas de negocio de la aplicación, a menudo a través de la interacción con los datos de la aplicación.

Otras características generales de estos sistemas de n-capas son:

- Tienen una buena fiabilidad y disponibilidad.

- La lógica de negocio está separada del resto de capas. Un cambio a la lógica de negocio no implica la modificación de todos los clientes. Asimismo la capa de presentación nos permite modificar la interfaz de la aplicación sin tener la necesidad de realizar cambios en los clientes.
- El rendimiento suele ser muy bueno.
- Es un modelo con muy buena escalabilidad, tanto horizontal como vertical.
- La extensibilidad es excelente. Existe poco acoplamiento entre las diferentes capas.

2.2. Plataformas para Aplicaciones y Servicios Telemáticos

Una plataforma para aplicaciones y servicios telemáticos debe ofrecer una serie de servicios a los arquitectos y desarrolladores tendientes a facilitar el desarrollo de aplicaciones empresariales y brindar una amplia gama de funcionalidades a los usuarios. Normalmente una plataforma de este tipo tiene los siguientes requisitos:

- *Escalabilidad*. Es la capacidad de adaptación de un sistema a una nueva carga de funciones, esto es, dado el caso en que aumenten las funcionalidades, se puedan añadir servidores o ampliar los existentes sin que sea necesario realizar modificaciones.
- *Mantenibilidad*. Para permitir añadir y modificar los componentes existentes sin que se modifique el comportamiento del sistema.
- *Disponibilidad*. Para tener el soporte de arquitecturas tolerantes a fallos, sistemas de redundancia, etc., que aseguren que el sistema estará siempre disponible.
- *Extensibilidad*. Para hacer posible añadir nuevos componentes y capacidades al sistema sin que se vean afectados el resto de componentes.
- *Manejabilidad*. los sistemas deben ser fácilmente manejables y configurables.
- *Seguridad*. Para tener buenos sistemas de seguridad tanto a nivel de autenticación, como de autorización y de transporte.
- *Rendimiento*. Para ofrecer mecanismos que permitan aumentar el desempeño de manera transparente al usuario.

Las plataformas para servicios y aplicaciones telemáticas básicamente son la implementación de una arquitectura n-capas (definida en el punto 2.1.3). En la actualidad las plataformas para aplicaciones y servicios telemáticos más importantes son CORBA, .NET, y J2EE.

2.2.1. Plataforma CORBA

CORBA [CORBA] es un estándar publicado por el *Object Management Group* (OMG) para una red de objetos distribuida y heterogénea. En el año 2000, el consorcio OMG comenzó la publicación de la versión CORBA 3 que ofrece soluciones en tres áreas: integración en Internet, calidad de servicio, y una arquitectura de componentes para CORBA. Aporta un conjunto de especificaciones que, al ser incorporadas a las aplicaciones distribuidas, ofrecen una forma de conseguir la interoperabilidad entre sistemas distribuidos de naturaleza heterogénea. Para ello CORBA se centra en principios fundamentales: la separación entre interfaz e implementación, la independencia de localización y la independencia del fabricante, y la integración de sistemas a través de la interoperabilidad.

En CORBA todos los componentes son objetos. Cada objeto se puede implementar con un lenguaje de programación distinto y ejecutarse sobre cualquier plataforma hardware o sistema operativo. Para OMG, un objeto es una entidad que encapsula una funcionalidad a través de una interfaz. Un objeto ofrece servicios a través de sus operaciones y atributos que son visibles mediante su interfaz. Esta entidad permite a los clientes solicitar la realización de operaciones en un objeto con independencia de su localización. El elemento que permite la transparencia de localización y de acceso a los objetos es el *Object Request Broker* (ORB), que es el equivalente en software al bus que interconecta componentes. Las interfaces de los objetos se especifican en un lenguaje especialmente definido para este fin, IDL, que forma parte del estándar CORBA.

2.2.2. Servicios CORBA

- Los servicios de CORBA complementan el funcionamiento básico de los objetos que dan lugar a una aplicación. Estos servicios se amplían continuamente para añadir nuevas facilidades a los sistemas desarrollados con CORBA. Entre estos se destacan los relacionados con ciclos de vida (Life cycle) que define operaciones para crear, copiar, mover y eliminar objetos, eventos (Events) que permite registrarse para recibir eventos que pueden ser producidos por otros objetos, nombrado (Naming) que permite localizar objetos por un nombre, localizador (Trader) que permite localizar objetos por sus propiedades, persistencia (Persistente) que ofrece una interfaz para almacenar objetos, transacciones (Transactions) que proporciona coordinación transaccional, concurrencia (Concurrency) que proporciona un gestor de bloqueos, externalización (Externalization) que permite obtener y producir datos como streams, seguridad (Security) que brinda soporte a la autenticación, listas de control de acceso y confidencialidad, tiempo (Time) que permite definir y gestionar eventos temporizados, propiedades (Properties) que permite asociar propiedades a un objeto, consultas (Quero) que ofrece una interfaz SQL para realizar operaciones en objetos, entre otros.

2.2.3. La Plataforma .NET

Microsoft .NET [.Net] es un conjunto de tecnologías de software de Microsoft para conectar su mundo de información, gente, sistemas y dispositivos. Permite un nivel sin precedente de integración de software a través del uso de servicios Web XML: pequeños, discretos, bloques de aplicaciones construidos que se conectan con cada uno—así como a otras aplicaciones grandes—vía Internet. Microsoft .NET se caracteriza por la utilización de XML que es un estándar industrial compatible definido por la organización World Wide Web Consortium (W3C), que permite distribuir los datos entre una gran variedad de dispositivos digitales, permitiendo la colaboración e interacción de los sitios Web a través de los servicios basados en XML.

2.2.4. Servicios de .NET

- Básicamente los servicios de .NET son los ofrecidos por Microsoft y otros proveedores de servicios de Internet. Los servicios básicos de .NET son: servicios de identidad que se basan en el servicio Passport, los servicios de notificación y mensajería que integra la mensajería instantánea, el correo electrónico, fax, correo de voz y otras formas de notificación, los servicios de personalización que controlan el modo de envío de las notificaciones y mensajes, así como el momento en que se produce dicho envío, los servicios de almacenamiento .NET que son el equivalente digital de Internet a la caja de seguridad de un banco, en el que el usuario dispone de una llave que le permite controlar el acceso, el servicio de calendario que es un servicio de integración para los calendarios laborales, sociales y particulares que, junto con datos en tiempo real, permitirán que otros servicios Web determinen la disponibilidad del usuario, el servicio de directorio y búsqueda que permite la localización de servicios y usuarios, los servicios de entrega dinámica que permiten a Microsoft, los Independent Software Vendors (ISV), socios de soluciones y otros desarrolladores, ofrecer niveles incrementales de funcionalidad y actualizaciones automáticas seguras según demanda, sin necesitad de instalación ni configuración por parte del usuario.

2.2.5. La Plataforma J2EE

De acuerdo a la definición de Sun de J2EE [J2EE]: "J2EE define un estándar para el desarrollo de aplicaciones empresariales multicapa. J2EE simplifica las aplicaciones empresariales basándolas en componentes modulares y estandarizados, proporcionando un completo conjunto de servicios a estos componentes, y manejando muchas de las funciones de la aplicación de forma automática, sin necesidad de una programación compleja". J2EE es una especificación que proporciona un modelo de programación, que consiste en un conjunto de APIs y dirige la manera de construir aplicaciones J2EE.

Por otra parte, J2EE especifica cómo debe ser la infraestructura sobre la cual deben correr las aplicaciones. Esta infraestructura de aplicación es proporcionada por los contenedores de las implementaciones de J2EE. La plataforma J2EE es esencialmente un ambiente de servidor de aplicaciones distribuido, un ambiente java que provee lo siguiente:

- Un conjunto de API´s de extensión Java para construir aplicaciones. Estas APIs definen un modelo de programación para aplicaciones J2EE.
- Una infraestructura en tiempo de ejecución para hospedar y gestionar aplicaciones. Este es el servidor en tiempo de ejecución en el cual las aplicaciones residen.

2.2.6. Servicios de J2EE

Las aplicaciones distribuidas requieren acceso a un conjunto de servicios empresariales entre los que se incluyen procesamiento de transacciones, acceso a bases de datos, mensajería, etc. Sin embargo, en lugar de tener acceso a estos servicios a través de interfaces propietarias o no estándares, los programas de aplicación en J2EE pueden accederlos a través de un contenedor. La especificación de la plataforma J2EE 1.3 incluye un conjunto de extensiones estándar de Java que cada plataforma J2EE debe soportar. Entre estas se encuentran:

- JDBC. Esta API añade más eficiencia a la obtención de conexiones, conjunto de conexiones, transacciones distribuidas, etc.
- Enterprise JavaBeans (EJB). Esta API especifica un framework de componentes para aplicaciones distribuidas multi-capa. Establece un estándar para definir componentes del lado del servidor, y especifica una gran infraestructura en tiempo de ejecución para hospedar componentes del lado del servidor.
- Java Servlets. Esta API provee abstracciones orientadas a objetos para construir aplicaciones Web dinámicas.
- JavaServes Pages (JSP). Esta API enriquece las aplicaciones Web permitiendo el desarrollo de aplicaciones Web manejadas por formularios.
- Java Message Service (JMS). Provee una API para colas de mensajes, publicación y suscripción de tipos de servicios middleware orientado a mensajes.
- Java Transaction API (JTA). Permite la implementación de aplicaciones transaccionales distribuidas.
- JavaMail. Provee una plataforma independiente y un framework independiente de protocolo para construir aplicaciones e-mail basadas en Java.
- JavaBeans Activation Framework (JAF). Esta API es requerida por la API JavaMail para determinar el contenido MIME de un mensaje y determinar las operaciones que pueden ser realizadas en las diferentes partes del mensaje.

- Java Conector Architecture (JCA). Provee un mecanismo para integrar componentes de aplicaciones J2EE a sistemas de información legales.
- Java API for XML Parsing (JAXP). Esta API provee abstracciones para parsers XML API´s de transformación.
- Java Authentication and Authorization Service (JAAS). Provee mecanismos de autorización y autenticación para aplicaciones J2EE.

2.2.7. Matriz Comparativa de las Plataformas

CORBA	.NET	J2EE
Soporte de múltiples sistemas operativos	No soporta múltiples sistemas operativos. El mundo de .NET gira en torno al sistema operativo Windows y aunque se están intentando trasladar partes importantes de la plataforma a otros sistemas operativos, lo cierto es que existe todavía una dependencia total de la plataforma de Microsoft.	Soporte de múltiples sistemas operativos. Al ser una plataforma basada en el lenguaje Java, es posible desarrollar arquitecturas basadas en J2EE utilizando cualquier sistema operativo donde se pueda ejecutar una máquina virtual Java.
Controlada por un organismo serio, OMG	Un único dueño. La plataforma .NET está dominada única y exclusivamente por Microsoft. Esto supone un grave problema ya que es una única empresa la que puede añadir y quitar características según crea necesario. Además esto hace que la competencia sea nula y no se estimula la evolución de la plataforma.	Organismo de control. La plataforma J2EE está controlada por el Java Community Process (JCP) [JCP], organismo formado por más de 500 empresas, lo que garantiza la evolución de la misma.
CORBA es una plataforma de desarrollo muy compleja, aunque existen capas de abstracción que facilitan el desarrollo de aplicaciones, lo cierto es que desarrollar un simple programa de "Hola Mundo" no es una labor trivial.	Requiere desarrolladores poco experimentados: Bajo la plataforma de desarrollo de Microsoft es posible utilizar lenguajes como VB .NET que hacen muy sencilla la creación de aplicaciones y servicios telemáticos. De este modo es posible tener un equipo de desarrolladores poco experimentados y sin embargo crear fácilmente aplicaciones.	Aunque no es una plataforma tan compleja. La creación de aplicaciones bajo J2EE requiere normalmente desarrolladores más experimentados que los necesarios para desarrollar bajo .NET y CORBA.

La evolución de las especificaciones de CORBA está sujeta a demasiados pasos de burocracia, lo que origina que para ver novedades en la plataforma sea necesario esperar grandes cantidades de tiempo.	No existe una correspondencia exacta entre las partes de la plataforma .NET y soluciones libres. Existen proyectos como Mono para linux que están portando algunas de sus partes, aún así, no se puede crear una arquitectura completa utilizando solamente productos basados en software libre.	En la plataforma J2EE es posible crear arquitecturas completas basadas única y exclusivamente en productos de software libre. No sólo eso, sino que los arquitectos normalmente disponen de varias soluciones libres para cada una de las partes de su arquitectura.
Soporte de múltiples lenguajes	Soporte de múltiples sistemas lenguajes. Con .NET es posible desarrollar aplicaciones utilizando simultáneamente varios lenguajes de programación.	La plataforma J2EE depende exclusivamente del lenguaje Java. Sólo se puede utilizar este lenguaje para desarrollar aplicaciones lo que puede suponer un gran problema si nuestro equipo no dispone de los conocimientos suficientes o tiene otras preferencias.
En el año 2000, el consorcio OMG comenzó la publicación de la versión CORBA 3 que ofrece soluciones en tres áreas: integración en Internet, calidad de servicio, y una arquitectura de componentes para CORBA.	Con sólo cuatro años en el mercado, apenas ha salido algún proyecto importante desarrollado con esta tecnología. Su inmadurez hace que probablemente deba pasar algún tiempo hasta que sea más productiva.	Creada en el año 1997 como respuesta a la tecnología MTS de Microsoft, J2EE tiene ya seis años de vida y una gran cantidad de proyectos importantes a sus espaldas.

3. CAPITULO III. TECNOLOGÍAS DE INFORMACION Y TELECOMUNICACIONESS ASOCIADAS A LA SEGURIDAD (TIC_S)

Las tecnologías de la Información y las Comunicaciones asociadas a la seguridad (TIC_S) son herramientas utilizadas para verificar la identidad de un actor telemático (usuario o proveedor de una aplicación o servicio), al igual que proteger la información que se transmite a través de la red.

Este capítulo se divide en cuatro secciones, en la primera sección se describe la criptografía como base fundamental de los servicios de seguridad que se ofrecen en la red para proteger la información. En la segunda se ilustra las capacidades de la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure) para facilitar el cumplimiento de los principios básicos de las comunicaciones seguras, identificar actores telemáticos (usuario y proveedor) y proteger la información que estos comparten a través de una sesión en la red. En la tercera se exponen los protocolos más difundidos en el establecimiento de sesiones seguras en sistemas telemáticos. Por último, en la cuarta sección se presentan algunas de las tecnologías de identificación más utilizadas para usuarios de aplicaciones y servicios telemáticos, que tienen como objetivo la automatización de procesos de identificación u autenticación para aplicaciones y servicios telemáticos.

3.1. Criptografía

La criptografía es un mecanismo conocido desde la antigüedad que sirve para codificar información. Viene de la palabra “cripto” que significa oculto. La criptografía comprende una colección de técnicas para transformar los datos con la finalidad de ocultarlos y almacenarlos de una manera segura. A través de la criptografía es posible transformar la información de manera que ésta resulte inteligible sólo para personas autorizadas a acceder la información.

En [Sistemas_85], narran que la criptografía data de miles de años, desde cuando los griegos y romanos enviaban información codificada a los guerreros que se encontraban en el campo. Los griegos, por ejemplo, crearon un algoritmo en el cual reemplazaban una letra del alfabeto por otra, ubicando la letra correspondiente tres posiciones adelante, dando origen a una serie de cifrarios que se denominaron “cifrarios de sustitución”, toda vez que consistían en el reemplazo de un símbolo por otro. En Grecia y en Roma se popularizó otro método conocido como la “scitala spartana” o scitalus, que consistía en anudar una cinta de cuero alrededor de una vara sobre la que se escribía el mensaje de manera longitudinal a la vara. La cinta de cuero se desanudaba y se enviaba al extremo receptor que contaba con una vara similar para descifrarlo. Dado que en este esquema, a diferencia de los de sustitución, los caracteres conservan su valor (solo cambian su posición relativa a los demás caracteres del mensaje), se originó toda una familia de cifrarios conocida como “cifrarios de transposición”.

La criptografía comprende dos procesos complementarios: la encriptación y la desencriptación. La encriptación es el proceso por medio del cual un mensaje (texto

plano) es convertido en un segundo mensaje (texto cifrado) utilizando una función compleja (el algoritmo de encriptación) y una clave especial para realizar la encriptación. La desencriptación es el proceso inverso, con el que el texto cifrado es vuelto a transformar en el texto plano original utilizando una segunda función compleja y una clave para desencriptar.

Dependiendo de si las claves para encriptar y desencriptar la información son iguales o diferentes, la clase de encriptación es simétrica (claves iguales) o asimétrica (claves diferentes).

Así, los algoritmos que utilizan la misma clave para encriptar y desencriptar la información se denominan: algoritmos de clave simétrica y tal clave es una clave secreta. De otra parte los algoritmos de clave asimétrica son aquellos que utilizan una clave para encriptar y otra para desencriptar. La clave para encriptar, es llamada clave pública, puesto que ésta puede estar disponible públicamente sin comprometer el contenido secreto del mensaje o la llave de desencriptación.

Con la aparición de los computadores y su enorme potencia para realizar sustituciones y transposiciones la criptografía llegó a su edad adulta. En la década de los setentas de creó y popularizó el algoritmo DES[2] que según [Sistemas_85] es utilizado por casi la totalidad del sector financiero de Colombia y del mundo.

DES es un algoritmo de clave simétrica, lo que implica que utiliza la misma clave para cifrar el mensaje en el origen y para descifrarlo en el receptor. En la actualidad, se cuenta con un gran repertorio de algoritmos de cifrado asimétrico, incluso más poderosos que DES. Mayor información a cerca de algorimos de encriptación se encuentra en [RSA_labs].

La criptografía simétrica representa una gran dificultad que consiste en tener que acordar con antelación entre el emisor y receptor, la clave que se va a utilizar para cifrar los mensajes. Para estimar con mayor claridad este inconveniente, tómese como ejemplo un grupo de 100 participantes que deben poderse comunicar de manera confidencial con cada cualquiera de los miembros del grupo, esto supone que deben acordar en total 99*100/2= 4950 claves. Y si por razones de seguridad se deben cambiar las claves semanalmente, se deben crear procesos administrativos complejos de distribución segura para cada una de las 4950 claves.

En 1976, los matemáticos Diffie y Hellman dieron origen a la criptografía asimétrica, que utiliza dos claves: una pública y otra privada que deben cumplir con las siguientes características fundamentales:

1. La clave pública debe ser conocida por todos los participantes (Kpub).
2. La clave privada es únicamente conocida por el dueño legítimo (Kpri).

[2] DES: Data Encryption Standard. Es un algoritmo de cifrado simétrico.

3. Las claves operan en parejas: Kpri (Kpub(M)) = Kpub (Kpri(M)) = M, esto quiere decir que un mensaje (M) que ha sido cifrado con la Kpub sólo puede ser descifrado con la Kpri y viceversa.
4. No es posible obtener a partir de la clave pública de un usuario, su correspondiente clave privada.

Con este nuevo esquema criptográfico se supera la dificultad de la criptografía simétrica de tener que manejar una gran cantidad de claves. Así para el mismo ejemplo de los 100 participantes, solo se requieren 200 claves: 100 públicas y 100 privadas, a diferencia de las 4950 que se requieren para el mismo grupo de usuarios empleando criptografía simétrica. Por esta razón, la criptografía asimétrica ha tenido una gran acogida en los sistemas de protección de información confidencial.

Por medio de la criptografía asimétrica, conocida también como criptografía de claves públicas, la infraestructura de claves públicas, PKI (Public Key Infraestructure), puede derivar servicios que garantizan la seguridad de una comunicación, tal como se describe a continuación. En la figura 1, se ilustra un esquema que describe las clases de técnicas criptográficas y los algoritmos más populares asociados a cada una de ellas.

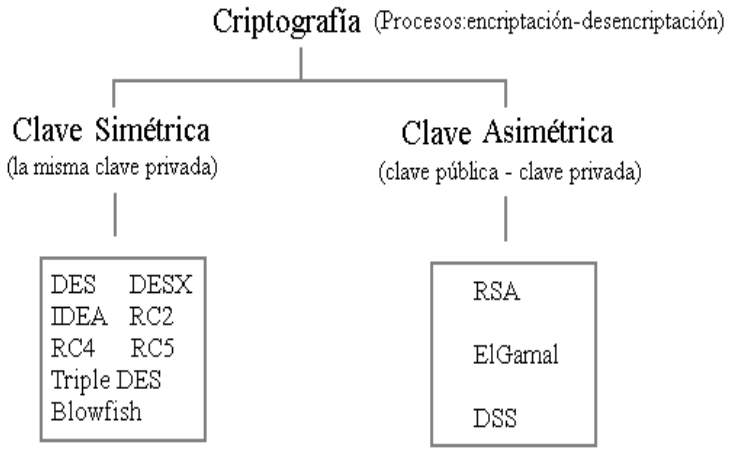


Figura 1. Técnicas criptográficas y algoritmos. Información sobre los algoritmos se encuentra en [RSA_labs].

3.2. Infraestructura de claves públicas

De acuerdo con la definición de [Chaparro], "La Infraestructura de claves públicas PKI, es el medio que facilita el acceso a las claves públicas, asegurando a sus usuarios la correspondencia unívoca de las mimas con sus respectivos propietarios. Este concepto se ha establecido en los últimos años y se ha usado como punto de referencia para proyectar una nueva generación de aplicaciones que hagan posible la provisión de servicios de seguridad a gran escala, sobre todo en sistemas abiertos como Internet".

El propósito de una infraestructura de claves públicas (PKI) es facilitar a las organizaciones el uso de la criptografía de claves públicas. La criptografía de claves públicas resulta esencial para el comercio electrónico, Internet, Intranet y otras aplicaciones que requieran seguridad distribuida.

La criptografía de claves públicas facilita el cumplimiento de los principios básicos de las comunicaciones seguras, que son muy valiosos en los procesos de identificación o autenticación de agentes telemáticos (usuarios-proveedores de servicios) y en el aseguramiento de la información compartida entre ellos, estos son: confidencialidad, autenticidad, integridad y no repudio.

La mayoría de los modelos de PKI se basan en el uso de certificados digitales, siendo los mas utilizados aquellos que manejan el formato X509. Un certificado es en esencia un vínculo entre una clave pública y los atributos que identifican una determinada entidad. En el modelo de certificación mas difundido, éste vínculo es mantenido por organizaciones que actúan como un tercero de confianza, cuya función es dar fe de la correspondencia entre los datos de un certificado y su correspondiente clave pública. Estas por lo general adoptan la forma de Autoridades de Certificación o CAs (Certificate Authorities).

Las capacidades de la PKI en conjunto con otros conceptos como certificados digitales, entidades certificadoras y firmas digitales se amplían a continuación.

3.2.1. Confidencialidad

La confidencialidad consiste en mantener una comunicación por completo privada, protegiendo la información de ser leída por actores externos. Para lograr la confidencialidad se utiliza la criptografía, que encripta o cifra la información que es transmitida, de manera que si es interceptada por agentes externos a través del medio de transmisión, éstos no la puedan descifrar.

En una comunicación confiable con criptografía asimétrica, cada participante cuenta con una clave pública (Kpub) y una privada (Kpri). Un ejemplo de comunicación confiable se ilustra en la figura 2, si un usuario A quiere enviar un mensaje al usuario B, debe tomar el mensaje M y cifrarlo con la clave pública de B (que por ser pública es conocida por todos los usuarios), esto es: mensaje cifrado = Kpub_B (M). Cuando el mensaje cifrado viaja a través de la red, puede ser visto por todos los usuarios, pero únicamente el usuario B puede descifrarlo ya que es el único que conoce la clave privada de B (correspondiente pareja de la clave pública de B); y que puede realizar la operación: (Kpri_B) (Kpub_B (M)) = M, para obtener el mensaje original.

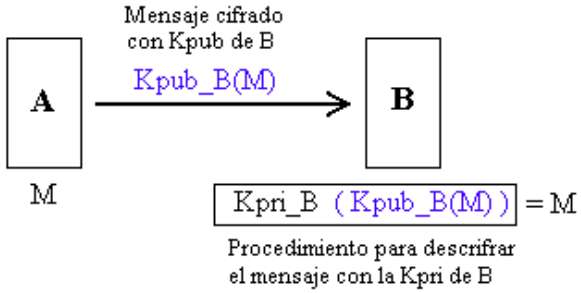


Figura 2. Esquema de envío de mensaje confidencial.

Los algoritmos de encriptación mayormente utilizados, sobretodo en el dominio del comercio electrónico son: DES (Data Encription Standart) de clave simétrica y el RSA (en honor a sus autores Ronald Rivest, Adi Shamir, and Leonard Adleman) de clave pública o asimétrica.

El algoritmo de encriptación estándar DES, de clave simétrica, fue introducido por IBM en 1975 con la cooperación de varias agencias gubernamentales. DES es de dominio público y ha contado con la asesoría de de muchos expertos desde su aparición. DES es el algoritmo comercial más desarrollado, y es utilizado por muchas organizaciones y sistemas para cifrar mensajes críticos y datos. DES es un cifrador de bloque, lo que indica que cifra datos en bloques de 64 bits y utiliza una clave de 64 bits. En realidad sólo 56 bits son utilizados para encriptar/desencriptar datos, mientras que los otros 8 bits operan como bits de paridad. El uso de 56 bits permite la creación de una clave con 2^{56} distintas posibilidades. Con todo esto, en los últimos años, han aparecido muchos casos en donde se ha vulnerado DES, [Cracking_DES], rompiendo la clave que se utiliza para encriptar. Esto hizo necesaria la creación de otro algoritmo de encriptación simétrica mas avanzado, el AES (Advanced Encription Standar).

De otro lado, el algoritmo de clave pública RSA es un estándar para sistemas de clave asimétrica que utilizan claves públicas y privadas para encriptar y desencriptar datos. Este algoritmo es utilizado en mayor medida para encriptar y para hacer firmas digitales.

El algoritmo de clave pública "RSA" y el de clave simétrica "DES" usualmente se utilizan juntos, puesto que RSA es relativamente lento para encriptar bloques grandes de datos, para los cuales DES es muy apropiado.

3.2.2. Integridad

Consiste en verificar que la información no ha sido alterada en su recorrido a través del medio de comunicación. Para lograrlo se utilizan las funciones matemáticas de "message digest[3]" o funciones de "hashing". Las funciones de Message Digest convierten la información de un archivo (grande o pequeño) en un único número, típicamente entre 128 y 256 bits de longitud. Las mejores funciones matemáticas combinan las siguientes propiedades matemáticas:

- Cada bit de la función de message digest es influenciado por cada bit de la función de entrada.
- Si algún bit de la función de entrada es cambiado, cada bit de salida tiene un 50% de probabilidad de cambiar.
- Dado un archivo de entrada y su correspondiente message digest, debe ser computacionalmente infactible encontrar otro archivo con el mismo valor de message digest.

[3] Message digest: Comprimido del mensaje.

Según Grarfinkel, las funciones Message digest son llamadas también funciones hash de una vía, porque ellas producen valores que son difíciles de invertir y resistentes a los ataques. Los message digest no son utilizados en operaciones de encriptar y desencriptar. En su lugar, éstos son utilizados en la creación de firmas digitales, códigos de autenticación de mensajes (MACs, Message Autentication Codes), y en la creación de claves de encriptación de frases empleadas en validación de accesos.

Para ejemplificar la utilización de la función de message digest o hashing, supóngase que un usuario B quiere verificar la integridad de un mensaje que le ha enviado un usuario A. Es decir, quiere comprobar que el contenido del mensaje no fue modificado por agentes externos en su trayecto a través de la red. Para hacerlo, compara el hashing del mensaje original con el hashing del mensaje que llega.

Para hacer posible la verificación de integridad de un mensaje, el usuario A debe calcular el hashing del mensaje h(M) y cifrarlo con su clave privada Kpri. Así el mensaje que envía el usuario A, a través de la red es: Kpri_A(h(M)). Nótese que al mismo tiempo se está comprobando la autenticidad del usuario que lo envía, pues sólo el usuario A conoce la Kpri de A. Por esta misma razón se logra que el usuario A no pueda negar haber firmado ese mensaje (No-repudio).

Cuando el usuario B recibe éste mensaje, calcula por su cuenta el h(M), luego toma el mensaje recibido (Kpri_A(h(M))) y le aplica Kpub_A (que es conocida por todos los usuarios), y compara el hashing obtenido con el hashing calculado y enviado inicialmente por el usuario A. Si el resultado es el mismo, el mensaje no sufrió ninguna modificación a su paso a través del medio de transporte (integridad).

El esquema descrito se ilustra en la figura 3.

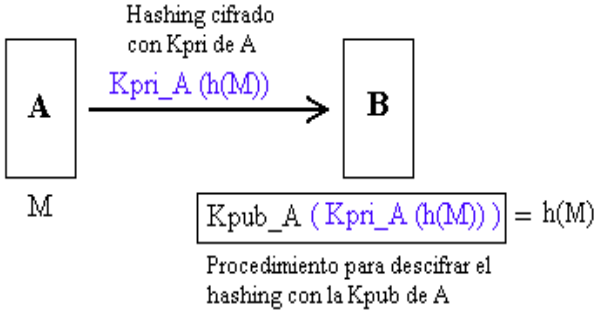


Figura 3. Esquema de verificación de integridad del mensaje.

Los algoritmos de message digest (MD) mas utilizados son: HMAC, MD2, MD4, SHA, el MD5 (Message Digest Algorithm 5) definida en el RFC 1321 y el SHA-1 (Secure Hash Standard). Más información sobre estos algoritmos está disponible en [RSA_labs] .

MD5 define una función de hashing de 128 bits de largo y es muy popular en aplicaciones en Internet. Por otro lado SHA1-1 define una función de hashing de 160 bits de largo y ha sido muy utilizado en productos que tienen que ver con el gobierno federal de los Estados Unidos. SHA-1 se considera 2^{32} veces más seguro que el MD5.

3.2.3. Autenticidad

Consiste en verificar que el usuario es quien dice ser. Al enviar un mensaje firmado con la clave privada de un usuario identificado ante una organización conocida como "tercera parte de confianza", se puede verificar que el mensaje realmente ha sido enviado por el usuario que esté registrado como portador de la clave pública que hace pareja con la clave privada que firma el mensaje. Obsérvese la figura 3.

Este esquema de autenticación utiliza las denominadas "firmas electrónicas", a través del siguiente procedimiento: primero el emisor firma el documento con su respectiva clave privada (sistema de claves asimétrico), con esto no puede negar la autoría, pues solo él tiene el conocimiento de esa clave, aminorando el riesgo por revocación del mensaje transmitido (no-repudio). Luego, el receptor comprueba la validez de la firma por medio de la utilización de la clave pública vinculada a la clave privada que firma el documento y con la cual es posible descifrar el mensaje.

Por ejemplo, para identificarse a si mismo, un usuario A que desea enviar un mensaje a un usuario B, el usuario A debe enviar el mensaje encriptado con su clave privada al usuario B. Cuando el usuario B recibe el mensaje, éste desencripta el mensaje utilizando la clave pública del usuario A. Una desencriptación correcta confirma que el emisor del mensaje es el usuario A, ya que el mensaje fue encriptado con la clave privada del usuario A, que sólo él conoce.

La legislación Colombiana, a través de la ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones; define para la aplicación de los requisitos jurídicos de los mensajes de datos, en el artículo 7, el concepto de **firma** así: "Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a.) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; b.) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado". Así, al hablar de firma en materia de comercio electrónico, se hace referencia a firma electrónica.

Existen dos puntos de quiebre de este esquema de autenticación, que corresponden mas a errores o responsabilidades humanas que a falencias del modelo. La primera de ellas es que el usuario preste, pierda o le sea robada la clave privada y caiga en manos de personas que la utilicen para acceder a los servicios que posee el dueño original. Y la segunda es que la tercera parte de confianza no tenga el suficiente cuidado al verificar la identidad de un usuario por medios convencionales (p.e. inspección de la cédula, fotos, biometría) y le otorgue un certificado con una falsa identidad.

3.2.4. No repudio

Consiste en asegurar que un usuario no pueda negar una acción que ha ejecutado. En el caso del envío de un mensaje, se asegura que éste ha sido enviado por su emisor original, de tal forma no pueda negar su envío. El esquema de aseguramiento de no repudio de la infraestructura de claves públicas plantea que si el usuario firma con su clave privada, que debe ser de su exclusivo conocimiento, no puede negar haber enviado ese mensaje. Esta propiedad también se ilustra en la figura 2.

3.2.5. Entidades Certificadoras

Una autoridad Certificadora (CA) es un tercero de confianza que tiene su propia clave pública y clave privada. Su función es emitir certificados digitales a sus usuarios firmados con su clave privada. Los usuarios de una entidad certificadora pueden ser instituciones, empresas, servidores web, usuarios de servicios web, entre otros.

Es responsabilidad de la Entidad Certificadora verificar por medios tradicionales (notario, inspección de cédula, pasaporte, fotografías recientes, biometría, documentación, etc) la identidad del usuario que va a adquirir un certificado, o la veracidad de la institución, empresa u otra organización.

La filosofía que hay detrás de los certificados digitales es la confianza y credibilidad que brinden las autoridades certificadoras. Para aceptar un certificado de cualquier entidad, éste debe estar firmado por una autoridad certificadora. A su vez, esta autoridad debe tener un certificado firmado por otra autoridad de mayor jerarquía o mayor credibilidad (p.e. el gobierno). De esta manera, la cadena de confianza es la esencia de la validación de certificados. En una transacción electrónica, debe haber una entidad certificadora de confianza para las partes involucradas que esté en un nivel superior de la jerarquía de entidades. Por ejemplo, Thawte es un nombre de confianza en la industria de las autoridades certificadoras de Estados Unidos y ofrece un programa para enlazar a la cadena, autoridades de certificación menos conocidas, que proveen certificados a sus usuarios, siendo firmados con la clave privada de Thawte. Durante la verificación, los usuarios siguen la cadena de certificados hasta la autoridad final (Thawte) y de esta manera se establece la confianza requerida para llevar a cabo cualquier tipo de transacción. Este servicio es usualmente utilizado por organizaciones que implementan una entidad certificadora cerrada, para su uso interno, y que requieren que su certificado raíz sea firmado por una autoridad reconocida como Thawte.

La mayoría de los buscadores Web incorporan firmas de entidades certificadoras reconocidas. Estas firmas se utilizan para verificar la identidad de un sitio Web cuando se realiza una conexión. Para soportar conexiones seguras y para que éstas sean autenticadas, un sitio Web debe registrarse con una autoridad de certificación que se encuentra en la lista de las autoridades certificadoras de confianza en el buscador Web de los usuarios finales.

Así, cuando alguien se conecta a un sitio Web a través de una sesión SSL[4](que maneja certificados digitales), el certificado de registro es transferido hacia el navegador Web del usuario. Para comprobar si el certificado del sitio Web ha sido firmado por una autoridad certificadora de confianza, se debe calcular el hashing de los campos del certificado (hashing(version, serial number, algorithm Id, Issuer, Period of validity, User, User's Public Key)) y compararlo con el hashing de los mismos campos almacenado en el campo signature (firma) del certificado.

Dado que el campo signature del certificado es el hashing de los demás campos del certificado cifrado con la clave privada de la entidad certificadora que lo emitió, esto es: Signature = Kpri_CA (hashing(demás campos)), el navegador intenta descifrar éste hashing, aplicando las claves públicas de las CAs de confianza que tiene registradas al campo signature así: Kpub_CA (Signature) = Kpub_CA (Kpri_CA(hashing(demás campos)). En el caso que logre descifrar el hashing, éste es comparado con el calculado inicialmente y si el resultado de la comparación indica que los hashing son iguales, el sitio Web queda autenticado; de lo contrario aparece un mensaje en el que se indica que la CA no es reconocida como entidad de confianza.

Los usuarios del navegador Netscape 4.x reconocen que un sitio Web ha sido autenticado y se ha establecido un canal seguro, cuando aparece un icono de un candado en la esquina inferior izquierda de la interfaz del navegador. Cuando no se ha establecido un canal seguro, el candado aparece abierto. Los usuarios de Microsoft Internet Explorer verán un icono de un candado en la esquina inferior izquierda cuando se establece una conexión segura. Cuando la sesión no es segura, no aparece el icono.

En Colombia, la Superintendencia de Industria y Comercio autoriza y vigila el funcionamiento de las entidades de certificación. La ley 527 define dos tipos de entidades de certificación:

- Cerradas: Permiten que una entidad ofrezca servicios de certificación sin exigir remuneración por ello. Un certificado digital de ese tipo sólo autoriza actividades entre una entidad y sus suscriptores, (p.e. una empresa con sus clientes).
- Abiertas: permiten una utilización más generalizada del certificado digital, tales como el intercambio de información entre diferentes entidades y sus respectivos suscriptores. Se permite el cobro por el servicio. En Colombia la única entidad de este tipo es Certicamara.

3.2.6. Certificados Digitales

Con el fin de promover la interoperabilidad entre diferentes fabricantes, la ITU-T emitió la recomendación X.509 en la que describe un formato estándar para certificados digitales. Los campos de un certificado digital X.509 tiene la forma ilustrada en la tabla 1.

[4] SSL: Secure Sockets Layer: protocolo de conexión segura a través de Sockets.

Version
Serial Number
Algorithm Id
Issuer
Period of validity
User
User´s Public Key
Signature

Tabla 1. Estructura de un certificado digital X.509.

La descripción de cada campo se presenta a continuación:

- **Version:** versión de la norma X.509 sobre la cual se generó el certificado. La última versión es la 3.0.
- **Serial Number:** número consecutivo que le asigna la entidad certificadora a cada certificado emitido por ella. Es responsabilidad de la CA garantizar que éste identificador sea único en su dominio.
- **Algorithm Id:** nombres de los algoritmos de clave pública y de hashing utilizado. Los más utilizados, RSA-MD5 o DSS-SHA.
- **Issuer:** Nombre de la entidad certificadora que emite el certificado.
- **Period of validity:** Fecha de validez del certificado.
- **User:** Nombre del usuario cuya clave pública se está certificando.
- **User´s Public Key:** Clave pública de usuario.
- **Signature:** hashing de los campos anteriores cifrado con la clave privada de la entidad certificadora.

Los certificados son inalterables ya que cualquier modificación realizada al certificado invalidará el campo Signature (por propiedades de las funciones hashing) y en consecuencia la alteración es fácilmente detectada.

La entidad certificadora sólo conoce la clave pública de sus clientes, no la clave privada, pues si la conociera estaría en capacidad de firmar por ellos. En caso que el usuario sea victima de pérdida o robo de su clave privada, debe reportar ésta situación a la entidad certificadora, para que ésta proceda a revocar el certificado. Para tal fin, cada entidad certificadora debe publicar en su servidor, su lista de certificados revocados (CRL, Certificate Revocation List).

Los pasos básicos a tener en cuenta para comprobar la validez de un certificado son:

1. Verificar que el campo signature del certificado es correcto. Para lograrlo, se debe, por un lado calcular el hashing de todos los campos del certificado (menos el signature) y por otro, aplicar la clave pública de la entidad certificadora al campo signature. Si los dos resultados coinciden, el certificado no ha sido alterado.

2. Verificar que el certificado no esté vencido. Esto implica revisar que el campo Period of Validity sea todavía válido.

3. Consultar en la lista de certificados revocados (CRL) del servidor de la entidad certificadora que emitió el certificado, si el certificado ha sido revocado o suspendido, a través del Serial Number del certificado.

3.2.7. Firmas Digitales

Las firmas digitales son un tipo de firma electrónica que permiten autenticar el emisor y comprobar la integridad del mensaje. La firma digital consiste en un conjunto de caracteres que acompaña a un documento o texto y dos claves, una pública y una privada por medio de las cuales se encripta el contenido. El procedimiento de generación de la firma digital comprende los siguientes pasos:

1. El SW del firmante aplica un algoritmo hash sobre el texto a firmar (algoritmo matemático unidireccional, es decir, lo encriptado no se puede desencriptar), obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Luego, el extracto es firmado con la clave privada del autor, y posteriormente es añadido al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

2. El software del receptor, previa introducción en el mismo de la clave pública del remitente (obtenida a través de una autoridad de certificación), descifra el extracto cifrado del autor.

3. Finalmente, calcula el extracto hash correspondiente al texto del mensaje recibido, y si el resultado coincide con el extracto anteriormente descifrado se considera que el mensaje no ha sufrido ninguna alteración, es decir que es integro. El caso contrario significaría que el documento sufrió una modificación posterior y por tanto no es válido.

En la ley 527 de 1999, la firma digital se encuentra definida en articulo 1 literal c como: "**Firma digital:** se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento conocido, vinculado con la clave del iniciador y el texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación". El artículo 28 de la misma ley establece que la firma digital tendrá "la misma fuerza y efectos que el uso de una firma manuscrita", si aquella incorpora los siguientes atributos:
a. Es única a la persona que la usa.
b. Es susceptible de ser verificada.
c. Está bajo el control exclusivo de la persona que la usa.
d. Está ligada a la información o mensaje, de tal manera que si estos son cambiados, la firma digital es inválida.
e. Esta conforme a las reglamentaciones adoptadas por el gobierno nacional.

Notas importantes acerca de la firma digital:
1. Es un valor numérico que se adhiere al mensaje de datos.
2. El valor numérico es obtenido por un procedimiento vinculado a la clave del iniciador, lo que permite verificar al emisor del mensaje. (no repudio y autenticidad del emisor).
3. Permite verificar que el mensaje inicial no ha sido modificado después de efectuada la transformación. (integridad).
4. Permite determinar si el mensaje ha sido escrito por la persona que firma. (integridad, no repudio, autenticidad).

3.3. Protocolos para el establecimiento de sesiones seguras

Como es conocido, Internet ha hecho posible el transporte de información alrededor de todo el mundo, eliminando fronteras geográficas, sociales y culturales, convirtiéndose en medio de comunicación, investigación, educación, negocios, entre muchas otras. Asociado a todas las actividades que se han viabilizado a través del uso de Internet, se encuentra el transporte de información sensible, privada o de carácter confidencial, haciéndose necesaria la creación de mecanismos que aseguren la información transmitida. Como respuesta a esta necesidad surgieron los protocolos de establecimiento de sesiones seguras, a través de los cuales es posible crear un canal privado de comunicación entre las partes involucradas en una comunicación.

Los protocolos que se abordan a continuación, SSL y SET, han sido los más utilizados para la protección de datos sensibles asociados a transacciones electrónicas, por lo tanto éstos han jugado un papel muy importante en el auge de operaciones que se realizan a través de Internet.

3.3.1. SSL (Secure Socket Layer)

El protocolo de conexión segura a través de Sockets SSL, provee un canal de conexión segura entre clientes y servidores Web que utilizan el protocolo para establecer sesiones Web. Es importante hacer énfasis en este punto porque a diferencia de otros protocolos estándar para internet como TCP/IP, SSL debe ser seleccionado por los clientes y servidores Web. Esto es, hacer un enlace a una página Web SSL (o utilizando el prefijo URL https://) para que el cliente Web invoque el protocolo que permite conectarse a un servidor habilitado SSL.

SSL es un protocolo que se encuentra sobre la capa TCP/IP, tal como lo ilustra la figura 4.

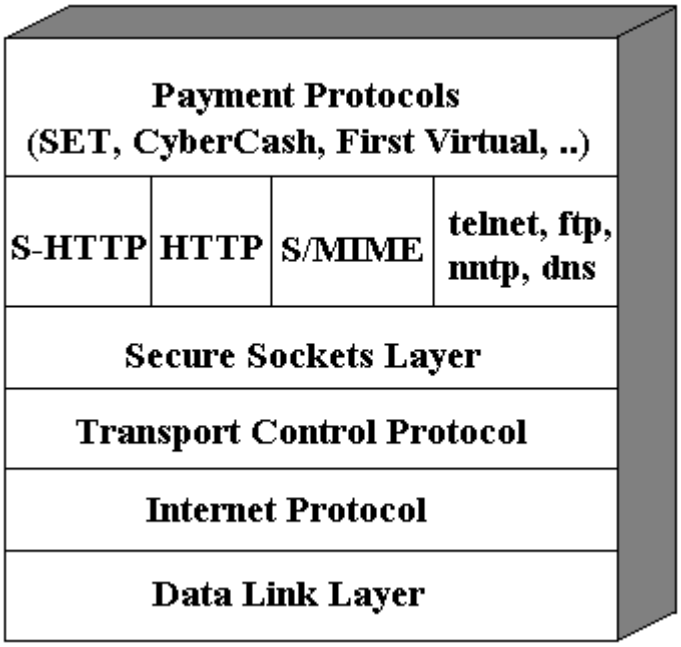


Figura 4. Pila de protocolos.

Hay que recordar que el protocolo TCP provee confiabilidad pero no seguridad en la transmisión de paquetes. SSL proporciona comunicaciones seguras, autenticación del servidor e integridad a los mensajes. Tal como se ilustra en la figura 4, SSL se encuentra en medio de las capas de transporte y sesión, debajo de la capa de aplicación. De acuerdo a esto y a que toda capa inferior provee servicios a la capa superior, las aplicaciones que utilicen SSL tendrán una conexión segura provista por SSL, entrega confiable de paquetes provista por TCP, y el enrutamiento de paquetes provisto por IP y el resto de servicios provistas por las capas inferiores (que no se ilustran en la figura), como el acceso a la red y las formas de enviar datos a través de diversos medios de transmisión.

Dado que SSL se encuentra sobre las capas TCP/IP, SSL puede asegurar las comunicaciones de un gran número de aplicaciones que se realizan a través de la red.

Considerando el caso de un comprador Web que desea conseguir un libro a través de una librería virtual. El comprador y el vendedor no se conocen. El comprador desea que la transacción se conserve confidencial de tal forma que sólo el vendedor conocerá que libro va a comprar y el número de la tarjeta de crédito que va a ser utilizado en la transacción. En la figura 5 se ilustran los pasos del establecimiento de una sesión SSL.

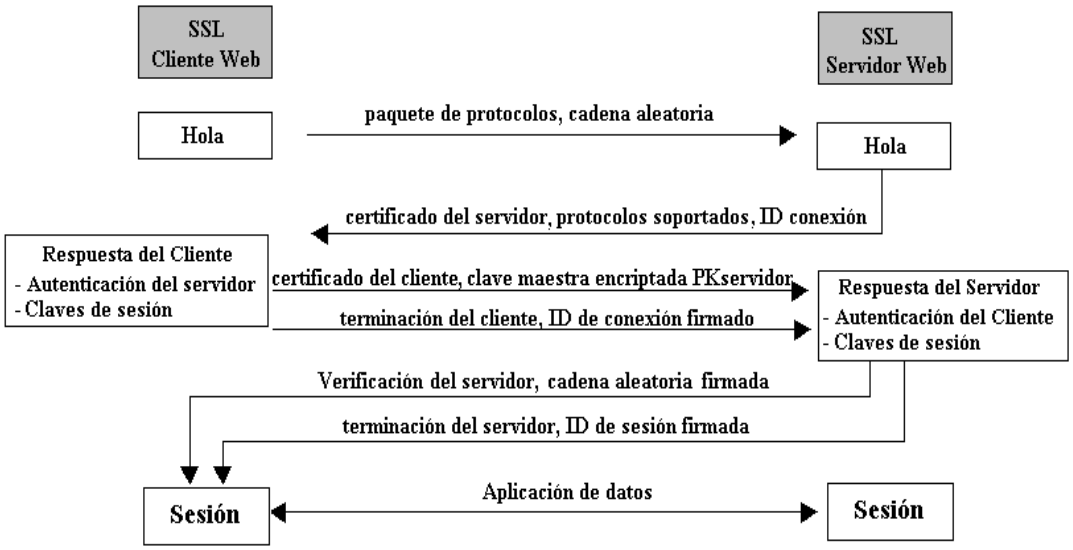


Figura 5. Establecimiento de una sesión SSL.

A continuación se ilustra la manera como se establecería una conexión segura en el caso de que un comprador quiera adquirir un libro a través de comercio electrónico.

Cuando se inicializa una conexión segura, el navegador del comprador envía un mensaje "Hola" al servidor, que comprende el paquete de protocolos seguros que el servidor soporta y una cadena aleatoria generada por el navegador. La cadena aleatoria es única para la sesión y será utilizada al cerrar la inicialización de la sesión para verificar que se ha establecido una conexión segura. El paquete de protocolos seguros abarca: algoritmos que a través del intercambio de claves permiten establecer una sesión privada, protocolos de encriptación de clave privada para obtener confidencialidad en las transacciones, y algoritmos de hashing para proveer integridad a la información transmitida. Antes de establecer una conexión segura, SSL intenta autenticar el servidor. En respuesta del "Hola del Cliente", el servidor responderá con un "hola del servidor" que comprende un certificado de servidor estándar X.509, una confirmación de los protocolos que el servidor puede soportar y que son preguntados por el cliente, y un identificador aleatorio de conexión. Igual que con la cadena aleatoria, el identificador de conexión será utilizado en el cierre del protocolo para determinar si una sesión segura se ha establecido.

El certificado del vendedor de libros debe estar firmado por una autoridad certificadora (CA) en la que el cliente confíe (la clave pública de la CA debe estar almacenada en el SW del navegador del cliente), para que el servidor pueda ser autenticado. El navegador del cliente comparará la firma digital en el certificado del servidor con la clave pública de la CA almacenada en la tabla de CAs que trae el SW del navegador. Si el certificado digital del vendedor ha sido emitido por una entidad certificadora, este debe estar firmado con la clave privada de la CA. La emisión del certificado por parte de la CA es verificada cuando el navegador compara la firma utilizando la clave pública almacenada en su tabla de claves públicas de las CAs.

Una vez que el servidor del vendedor ha sido autenticado por el navegador del cliente, el navegador del cliente genera una clave maestra para ser compartida únicamente entre el cliente y el servidor. Esta clave sirve para generar las claves utilizadas en la encriptación simétrica y en el aseguramiento de la integridad de la información. La clave maestra es encriptada con la clave pública del servidor y enviada al vendedor.

Desde que se genera la clave maestra, tanto el cliente como el servidor generan dos juegos de parejas de claves simétricas para asegurar los mensajes entrantes y salientes. Dado que el cliente y el servidor han acordado utilizar un protocolo común y ambos están empleando la misma clave maestra, las parejas de claves simétricas serán idénticas.

Una pareja de claves es utilizada para encriptar el tráfico saliente del cliente y desencriptar el tráfico entrante del servidor. La otra pareja de claves simétricas es utilizada para encriptar los mensajes salientes del servidor y desencriptar los mensajes entrantes del cliente. Para propósitos de seguridad, es importante notar que el navegador del cliente genera la clave maestra compartida. Esto asegura desde la perspectiva del cliente, que el servidor no está empleando las mismas dos parejas de claves simétricas para otras sesiones. Adicionalmente, la clave maestra es aleatoriamente generada para cada sesión. Incluso si esta clave fuera encontrada por coincidencia, ésta no podría utilizarse para desencriptar otras sesiones con otros vendedores o futuras sesiones con el mismo vendedor.

Dos pasos finales verifican la seguridad en el establecimiento de una sesión segura. La "terminación del cliente" encripta el identificador de conexión aleatorio del servidor utilizando la clave de escritura del cliente. Si el servidor tiene la misma clave maestra, la clave de lectura del servidor desencriptará el identificador aleatorio de conexión. El servidor sabrá que una conexión segura ha sido establecida si el identificador de conexión desencriptado es el mismo que el servidor envió en el mensaje Hola. La "terminación del servidor" completa el establecimiento de un canal seguro. El servidor utiliza la clave de escritura del servidor para encriptar la cadena aleatoria enviada por el cliente en el mensaje Hola. La cadena aleatoria encriptada es devuelta al cliente. El cliente desencripta la cadena utilizando la clave de lectura del cliente y la compara con la cadena aleatoria original enviada al servidor. Si resultan ser iguales, el cliente tendrá la seguridad que una conexión segura ha sido establecida.

A través de esta serie de pasos que involucra criptografía de clave pública y privada, el comprador Web puede establecer una conexión segura con un servidor de un vendedor autenticado.

3.3.2. SET (Secure Electronic Transactions)

El protocolo de transacciones electrónicas seguras, SET, fue desarrollado por VISA, Mastercard y otras compañías, para asegurar los pagos con tarjetas de crédito a través de

Internet. SET se construyó sobre la base de la utilización de la criptografía de claves públicas para validar la autenticidad de las partes involucradas en una transacción con tarjeta de crédito. Los principales objetivos de SET son:

- Proveer a los comerciantes la seguridad de que el cliente que está utilizando una tarjeta de crédito es el legítimo dueño de la tarjeta de crédito.
- Proveer a los clientes la seguridad de que los comerciantes pueden aceptar tarjetas de crédito y que están vinculados a una institución que provee servicios de transacciones con tarjeta de crédito.
- Proveer integridad y confidencialidad a las transacciones de pagos a través del proceso de autorización.

SET emplea la tecnología de claves pública como método primario de establecimiento de confianza entre las partes. Todas las partes involucradas en una transacción tienen certificados digitales. Todas las partes dejan sus certificados SET públicamente disponibles, lo cual habilita que una parte envíe información utilizando la clave pública de la otra parte. Utilizando SET, los clientes pueden enviar los datos directamente a la organización financiera que autoriza los pagos, y los datos de la tarjeta no son expuestos al comerciante. Esto hace una diferencia clave con SSL, pues allí el comerciante tiene claro acceso a la información de la tarjeta de crédito del cliente.

Un certificado SET contiene la siguiente información:

- La clave pública del portador del certificado (portador puede ser: portador de la tarjeta, comerciante, pasarela de pagos, institución financiera a la que se encuentra adscrito el comerciante).
- Identificación única del portador del certificado.
- Firma digital de la entidad certificadora que expide el certificado.
- Hashing del número de la cuenta para pagos con cargo a tarjeta y/o número serial único.
- Algoritmo de firma.
- Periodo de validez (expedición y expiración del certificado).

En las figuras 6 y 7 se ilustran respectivamente los esquemas de pago utilizando el protocolo SSL y SET.

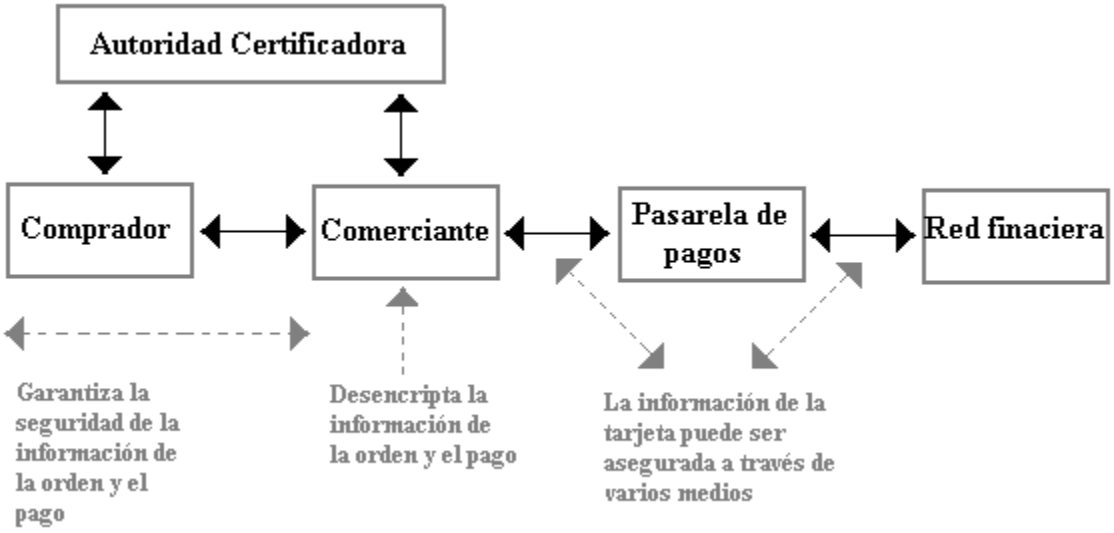


Figura 6. Seguridad en una transacción SSL.

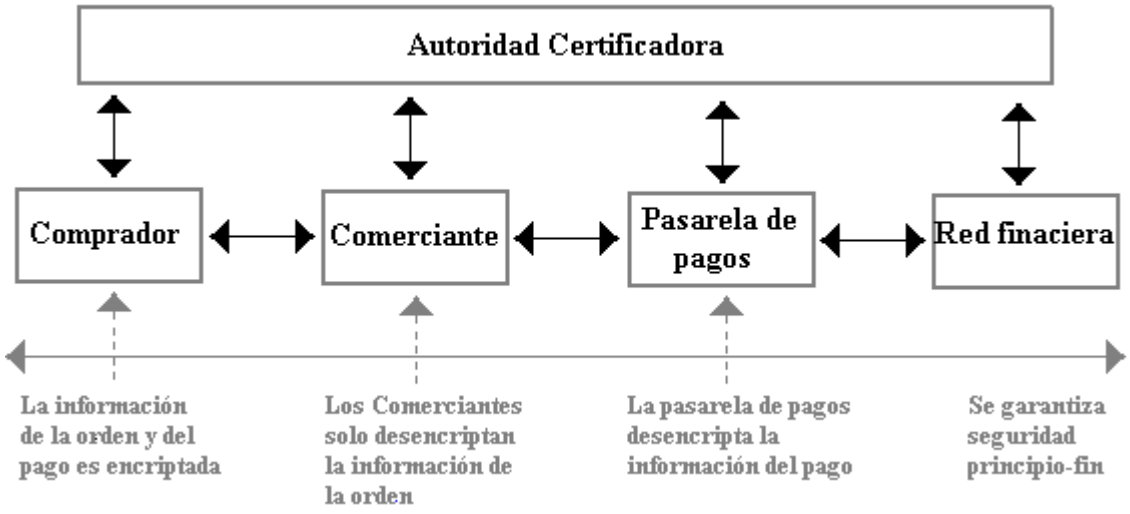


Figura 7. Seguridad en una transacción SET.

El proceso que se ilustra en la figura 7 es el siguiente:

1. El portador de la tarjeta, obtiene un certificado SET de una autoridad certificadora (CA) como VeriSing. De esta manera, provee a la CA información pertinente que incluye nombre, institución financiera que le proporcionó la tarjeta, dirección domiciliaria y demás.
2. La CA autentica y valida tanto al portador de la tarjeta como a la institución financiera que proporcionó la tarjeta, antes de entregar el certificado SET.
3. Igualmente, el comerciante debe solicitar a la CA un certificado que lo acredite como comerciante, identificándose a si mismo y proporcionando información pertinente acerca de la institución financiera que le proveerá el servicio de transacciones seguras para pagos con tarjeta de crédito. El comerciante necesita

esta información antes de que pueda procesar las instrucciones para pagos SET desde el cliente e interactuar con la pasarela de pagos.

4. Una vez registrados, el cliente y el comerciante pueden iniciar una transacción SET.
5. El cliente visita la página Web del comerciante, selecciona los productos a comprar y llena la forma de orden correspondiente. La transacción de pagos inicia cuando el cliente hace clic en "pagar".
6. El SW del cliente envía la orden y la información de pago al comerciante: el software SET del cliente crea dos mensajes; uno que se envía al comerciante y contiene la información de la orden de compra, el total de la compra y el número de orden, y otro que se envía al banco y contiene la información referente al pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetado en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.
7. El comerciante responde con la apropiada información de autenticación. El comerciante también se autentica a si mismo ante la pasarela de pagos que utilizará para continuar la transacción del cliente.
8. El comerciante pasa la información de pago al banco: el software SET del comerciante genera una solicitud de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.
9. El banco verifica la validez de la solicitud: el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una solicitud de autorización, lo firma y lo envía al banco que expidió la tarjeta del cliente.
10. El banco emisor de la tarjeta del cliente autoriza la transacción: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la información de la cuenta del cliente, en caso de que no haya problemas, aprueba la solicitud de autorización, la firma y la regresa al banco del comerciante.
11. El banco del comerciante recibe la autorización de la transacción: una vez recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción, la firma y la envía al servidor del comerciante.
12. El servidor del comerciante finaliza la transacción: el servidor del comerciante da a conocer que la transacción de la tarjeta fue aprobada y muestra al cliente la conformidad de pago, procesa la orden de compra del cliente y finalmente inicia el proceso de distribución de los bienes que compró el cliente.
13. El comerciante captura la transacción: en la fase final de SET el comerciante envía un mensaje de "captura" a su banco, esto confirma la compra y genera el descuento en la cuenta del cliente, así como la acreditación del monto a la cuenta del comerciante.

14. El banco emisor de la tarjeta del cliente, envía los reportes de pago de crédito al cliente: el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.

3.4. Tecnologías de identificación y captura automática de datos

En esta sección se describirán las tecnologías de identificación y captura automática de datos (AIDC)[5] más utilizadas, con el objetivo de ofrecer una ilustración básica de los principios de estas tecnologías, sus ventajas y sus aplicativos más comunes.

Las tecnologías de identificación y captura automática de datos se dividen en dos grandes grupos: Tecnologías de reconocimiento de aspectos biométricos y las tecnologías de transporte de datos.

Las tecnologías de transporte de datos se caracterizan básicamente por almacenar y facilitar el transporte de información. Entre ellas se encuentran: los códigos de barras, las tarjetas de banda magnética y los dispositivos de almacenamiento electrónico (tarjetas magnéticas, tarjetas inteligentes y dispositivos de identificación por radiofrecuencia).

De otra parte, las tecnologías de reconocimiento de aspectos biométricos se subdividen en aquellas que permiten distinguir aspectos biométricos estáticos o que tiene que ver con la anatomía (rostro, geometría de la mano, características del Iris, huellas digitales), y aquellas que reconocen aspectos biométricos dinámicos (timbre y tono de la voz, forma de escribir, comportamientos (forma de caminar)).

Las tecnologías de identificación y captura automática de datos comprenden la sección de herramientas hardware que pueden contribuir como mecanismo de seguridad en el acceso a aplicaciones y servicios telemáticos, pues su apoyo a los servicios ofrecidos por la infraestructura de claves públicas en la verificación de la identidad de un usuario, abre paso a la creación de sistemas automáticos de identificación a través de entornos abiertos como Internet.

3.4.1. Tecnologías de reconocimiento biométrico

La biometría es la ciencia que trata la aplicación de la estadística y de modelos matemáticos al estudio de fenómenos biológicos y rasgos físicos personales adaptables al reconocimiento. De esta forma la biometría habilita la identificación o verificación de la identidad de forma automática de un individuo, empleando sus características biológicas, psicológicas y de conducta. Estas características propias de cada individuo

[5] AIDC: Automatic Identification and Data Capture. Identificación y captura automática de datos. Campo de estudio.

que son objeto de análisis de las tecnologías de reconocimiento biométrico, deben cumplir los siguientes requisitos:

- **Universalidad:** Se refiere a que cada individuo debe poseer aquella característica.
- **Unicidad:** No es posible que dos personas coincidan con la misma característica biométrica.
- **Permanencia:** La característica biométrica debe permanecer inmutable en el tiempo.
- **Capturabilidad:** la característica biométrica debe poder ser medida cuantitativamente.

En la tabla 2 que se ilustra a continuación, se evalúan algunos aspectos biométricos y el grado de cumplimiento de las características mencionadas anteriormente.

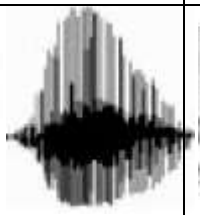
Aspecto Biométrico **Característica**	**Huella digital**	**Iris**	**Voz**	**Geometría facial**	**Geometría de la mano**
					
Universalidad	Restricción por Discapacidades	Restricción por Discapacidades	Restricción por Discapacidades	Restricción por desfiguración	Restricción por discapacidades
Unicidad	Alta	Alta	Baja	Baja	Media
Permanencia	Alta	Alta	Baja	Media	Media
Capturabilidad	Media	Media	Media	Alta	Alta

Tabla 2. Características Biométricas y grado de cumplimiento de los requisitos básicos.

Por su parte, alrededor de estas tecnologías de reconocimiento biométricos, se han desarrollado sistemas de identificación personal automáticos, que en resumen realizan las siguientes funciones:

- Obtención de la muestra biométrica del usuario final.
- Extracción de los datos de la muestra.
- Comparación de los datos obtenidos con los existentes en la base de datos.
- Decisión sobre la correspondencia de datos.
- Exposición del resultado de la verificación.

A continuación, se ilustrarán algunas de las tecnologías biométricas mas utilizadas en el reconocimiento de personas.

3.4.1.1. Reconocimiento de la huella digital

El reconocimiento de la huella digital es la técnica más antigua de identificación personal. Los primeros estudios científicos sobre la huella digital datan de mediados del siglo XVI, sin embargo el uso de huellas digitales como medio de identificación no ocurrió sino hasta mediados del siglo XVIII. En 1859 William Herschel descubrió que las huellas digitales permanecían inmutables en el tiempo y eran únicas para cada individuo; de tal forma que estableció el uso de las huellas digitales como medio de identificación, firma legal de documentos y autenticación de transacciones.

En los primeros años del siglo XX, la huella digital fue aceptada como un instrumento válido para la identificación personal, pero para esa época, la verificación manual de la huella digital no dejaba de ser un proceso largo, tedioso y costoso.

En 1980, Henry Faulds creó un sistema para clasificar las huellas digitales que reduciría la dificultad del proceso de comparación requerido para verificar la identidad de un individuo, clasificándolas por sus características fisiológicas. [Internacional Biometric Club].

Otros estudios se encaminaron hacia el diseño e implementación de sistemas automáticos de identificación de la huella digital (AFAS)[6]. El esquema en bloques de un sistema automático de autenticación de la huella digital se representa en la figura 8.

La entrada del sistema AFAS es la imagen de la huella digital y la identidad el individuo correspondiente. La salida es la respuesta Si o No. El sistema compara la imagen en la entrada con la imagen de referencia almacenada en la base de datos correspondiente al individuo. Otro tipo de sistema desarrollado es el AFIS[7], donde la entrada es únicamente la huella digital y la salida es la identidad de una persona de quien se tiene registrada la imagen de la huella digital y es similar a la imagen de la huella introducida.

En estos sistemas resulta muy importante la interfaz hardware encargada de escanear la huella digital y el software encargado de procesar la imagen para que puedan ser claramente analizados sus rasgos característicos.

[6] AFAS: Automatic Fingerprint Autentication System
[7] AFIS: Automatic Fingerprint Identification System. Sistema automático de identificación de huellas digitales.

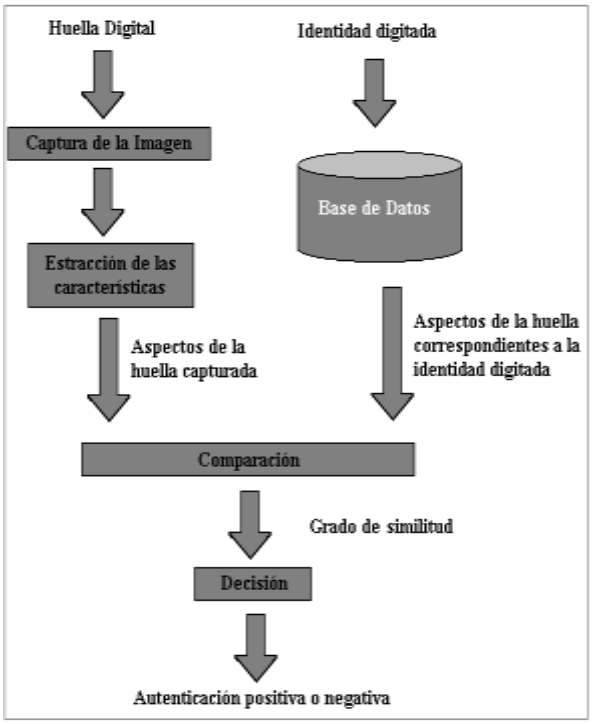


Figura 8. Diagrama en bloques de un sistema automático de autenticación de huellas digitales.

3.4.1.2. Reconocimiento facial

El reconocimiento facial es el método innato de identificación biométrica utilizado para reconocer personas. Esta técnica de reconocimiento biométrico, respecto a otras técnicas, tiene la ventaja de ser no invasiva, de manera que no requiere cooperación por parte de la persona sometida a reconocimiento.

La desventaja de esta técnica es que el rostro no es permanente, es decir que cambia con el tiempo, además de que puede ser sometido a constantes cambios como cabello, barba, bigote, cirugías plásticas; haciendo difícil el reconocimiento facial e implicando mayores complicaciones técnicas en los sistemas automáticos.

Con el uso de técnicas de preproceso y esquemas de representación de características locales, se han desarrollado diversas aplicaciones para la identificación de rostros humanos. La tarea de reconocimiento de rostros se divide en tres etapas bien diferenciadas: preproceso de la imagen original, extracción de vectores de características y clasificación. [Toselli].

3.4.1.3. Reconocimiento del iris y de la retina

El reconocimiento de Iris se realiza a través del análisis de las características del tejido coloreado que se encuentra alrededor de la pupila mientras que el reconocimiento de la retina analiza los capilares que están situados en el fondo del globo ocular. El iris humano, al igual que la vasculatura retinal, es una estructura única por individuo e inalterable durante toda la vida de la persona.

En el reconocimiento de la retina, se analiza la forma de los vasos sanguíneos de la retina humana, que representa un elemento característico de cada individuo. En los sistemas de autenticación basados en el reconocimiento de patrones retinales el usuario a identificar debe mirar a través de unos binoculares, acomodarse adecuadamente, mirar a un punto determinado y pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En este momento se escanea la retina con una radiación infrarroja de baja intensidad, detectando los nodos y ramas del área retinal, para luego compararlos con los almacenados en una base de datos. La compañía EyeDentify[8] posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología.

La identificación basada en el reconocimiento del iris es más moderna que la basada en patrones retinales. El procedimiento consiste en capturar una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos funciones matemáticas hasta obtener una cantidad de datos suficiente para los propósitos de autenticación. Esta muestra, denominada iriscode, es comparada con otra tomada con anterioridad y almacenada en una base de datos. La empresa estadounidense IriScan[9] es la principal desarrolladora de esta tecnología y posee la patente.

Los lectores biométricos de iris y retina, donde el usuario está sometido a una radiación de luz para escanear una imagen, se convierten en intimidantes para algunas personas, haciendo de estos dispositivos, los más impopulares dentro de las tecnologías de reconocimiento biométrico.

3.4.1.4. Reconocimiento de la geometría de la mano

El reconocimiento de la geometría de la mano consiste en la medición de las características físicas de la mano (dedos y palma) del individuo. Un sistema automático cuenta con una cámara digital para capturar la silueta de la mano, tanto en el dorso como en la palma. Las medidas geométricas (dimensión, longitud, distancia, ángulos, etc) de la mano son calculadas por el sistema a través de la imagen adquirida.

[8] EyeDentify: se encuentra en el sitio Web http://www.eyedentify.com/
[9] IriScan: disponible en Internet en: http://www.iriscan.com/

Esta técnica ha sido muy debatida debido por los aspectos de unicidad y permanencia que debe tener toda característica biométrica utilizada con fines de identificación, pues se afirma que la geometría de la mano no es rica en elementos identificativos únicos como si los cuenta la huella digital y el Iris.

Además, el aspecto de permanencia también es discutido porque múltiples situaciones pueden ser causa de inestabilidad y cambios en el tiempo (edad, enfermedad, accidente). Por estas razones, el reconocimiento de la geometría de la mano no es muy utilizado para verificar la identidad de personas. [Geo_mano].

3.4.2. Tecnologías de transporte de datos

En esta sección se encuentran ubicados los dispositivos de almacenamiento electrónico de información. Algunos ejemplos son los códigos de barras, las tarjetas de banda magnética, las tarjetas inteligentes y los dispositivos de almacenamiento que se comunican por radio frecuencia. A pesar de la aceptación que han tenido las tarjetas de banda magnética, ésta cuenta con unos inconvenientes como son la poca seguridad (fácil fraude), sólo pueden almacenar información y tienen poco espacio de memoria, razón por la que no son tenidas en cuenta como dispositivo de transporte de información personal con fines de autenticación. De otra parte, los códigos de barras son mayormente utilizados para etiquetar productos, facilitar la identificación de los mismos dentro de un inventario y para realizar el cobro del producto.
A continuación se hace una ilustración de las tecnologías que permiten una mejor y mayor manipulación de información, estas son, las tarjetas inteligentes y los dispositivos de identificación por radio frecuencia.

3.4.2.1. Tarjetas Inteligentes

Las tarjetas inteligentes son en su forma más general, dispositivos de plástico de dimensiones determinadas, que tienen incrustado un chip capaz de almacenar y en algunos casos, de procesar información de manera segura. Su utilidad es básicamente el almacenamiento y procesamiento de datos confidenciales como pueden ser: números de identificación personal, claves privadas, dinero electrónico, historiales médicos, estado de las cuentas de crédito, entre otras. Las tarjetas inteligentes proporcionan seguridad en el almacenamiento de información y en las operaciones que se realizan con tal información.

La estructura de una tarjeta inteligente se ilustra en la figura 9. Ésta es una tarjeta inteligente de contacto, puesto que cuenta con una placa de contactos además del chip que almacena y procesa la información. En la placa de contactos sólo 6 son utilizados, estos son: polarización (Vcc-5V), tierra (Gnd), reset (Rst), voltaje pico pico (Vpp), reloj (Clk), entrada/salida de datos(I/O). El chip es un microprocesador que cuenta con memoria EEPROM, ROM, RAM y opcionalmente un coprocesador de encriptación (cifrador). Los valores típicos de las tarjetas disponibles son aproximadamente: 32KB de

ROM, 32 KB de EEPROM, 1-4 KB de RAM y un microprocesador de 8 bits con un reloj externo de 1 a 5 MHz. Las tarjetas inteligentes no tienen reloj interno, así es que las señales de reloj deben ser proporcionadas por un reloj externo. Las aplicaciones con tarjetas inteligentes son usualmente almacenadas en la EEPROM, mientras que la mayoría de los sistemas operativos residen en la ROM.

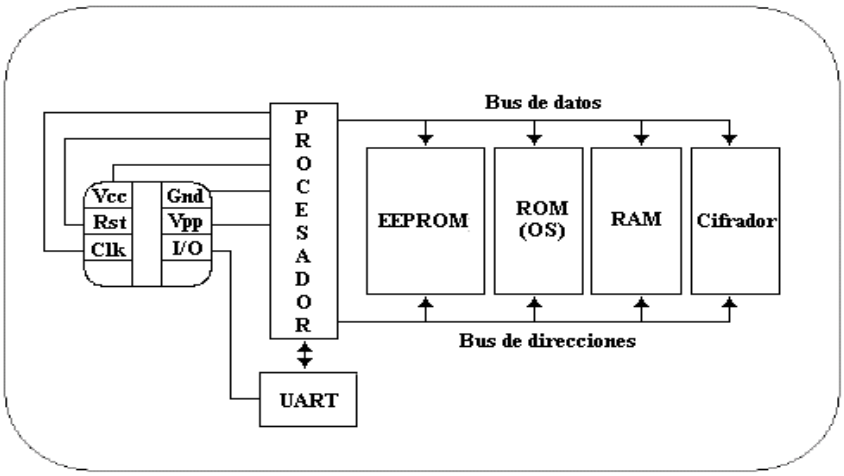


Figura 9. Estructura de una tarjeta inteligente

Las propiedades físicas de las tarjetas inteligentes se encuentran estandarizadas en la norma ISO 7816 (tarjetas con contactos) y ISO 14443 (tarjetas sin contactos). Las tarjetas inteligentes con contactos, requieren de un dispositivo lecto/escritor donde son insertadas y a través del cual se pueden comunicar con el exterior.

Por su parte, las tarjetas inteligentes sin contactos, requieren una antena para transmitir vía radio frecuencia la información. Esto se ampliará en la sección de dispositivos de identificación por radio frecuencia.

Los principales inconvenientes de la utilización de tarjetas inteligentes están relacionados con que los lenguajes de programación de las tarjetas dependen del hardware, la programación se hace generalmente en ensamblador y la mayoría de las aplicaciones son desarrolladas por el proveedor de la tarjeta. Igualmente el protocolo que realiza la comunicación con las tarjetas inteligentes es propietario.

Una solución planteada con el fin de lograr una mayor penetración de las tarjetas inteligentes ha sido la definición de los sistemas OCF[10] en entornos java, PC/SC[11] en entornos Windows y MUSCLE[12] en entornos linux, cuyo objetivo en común es habilitar el desarrollo de aplicaciones con tarjetas inteligentes a través de interfaces de alto nivel, independiente de protocolos de las tarjetas y lectores desarrollados por los diferentes proveedores. Los componentes comunes de estos sistemas son los controladores de los diferentes lectores y tarjetas, API's () y manejadores de recursos.

[10] OCF: OpenCard Framework (Java).
[11] PC/SC: Personal Computer/Smart Card (Windows).
[12] MUSCLE: Movement for the Use of Smart Cards in a Linux Environment (Linux).

3.4.2.2. Dispositivos de Identificación por radiofrecuencia

Los dispositivos de identificación por radiofrecuencia son componentes electrónicos que permiten el almacenamiento de información, pero que a diferencia de las tarjetas inteligentes, tienen un transreceptor radioeléctrico que le permite enviar y recibir señales vía radio. Estos dispositivos trabajan a una frecuencia de operación que se establece en el proceso de fabricación. Cada fabricante diseña los dispositivos para manejar ciertas frecuencias. En el caso de Texas Instruments, maneja dos frecuencias, una baja de 134.2 KHz y una alta de 13.56 MHz.

Dependiendo de la aplicación, se selecciona la frecuencia de operación del sistema RFID y por lo tanto de los dispositivos necesarios para montarlo. Se han estandarizado cuatro bandas de frecuencia primarias para su implementación. Los sistemas de bajas frecuencias (125-134 KHz) son más comúnmente utilizados en aplicaciones de seguridad como controles de acceso y rastreo de productos. Los sistemas de frecuencia media (13.56 MHz) se utilizan en aplicaciones con programas de cliente frecuente donde se requieren rangos de lectura medios. Los sistemas de alta y ultra alta frecuencia (850MHz a 950 MHz y 2.4GHz a 2.5GHz) permiten rangos de lectura más grandes y mayores velocidades de lectura. [Reynolds].

Un sistema de identificación por radiofrecuencia está compuesto esencialmente por los elementos que se ilustran en la figura 10 y que son descritos a continuación:

Figura 10. Elementos de un sistema RFID.

- **Dispositivo de almacenamiento electrónico de información:** dentro de la terminología RFID éstos son denominados transponders. Están compuestos por un chip que permite almacenar información y una antena que transmite a una determinada frecuencia de operación. Se clasifican en dos tipos: pasivos y activos. Los pasivos son aquellos que no requieren de una fuente de alimentación propia para responder a las peticiones del lecto-escritor RFID, pues se alimenta de la misma señal emitida por la antena, de manera que consiguen transmitir

información a cortas distancias. De otra parte, los dispositivos de almacenamiento activos, poseen su propia fuente de alimentación (siendo de gran tamaño), por lo que manejan una mayor potencia de transmisión y se pueden alcanzar mayores distancias de lectura. En consecuencia, los transponders pasivos tienen un costo mínimo, son más pequeños y cuentan con un rango mas bajo de lectura.

En cuanto a los chips de los transponders, éstos pueden ser de sólo lectura (memoria ROM) cuya capacidad no supera los 128 bits, o de lectura y escritura (memoria EEPROM no volátil) con mayor capacidad, de 512 bits hasta 1MB. Durante la fabricación, cada transponder es marcado con un código de identificación único denominado UID.

Los transponders vienen en diferentes presentaciones dependiendo de si son activos o pasivos y su capacidad de almacenamiento de información, encontrando desde diminutas y livianas etiquetas, hasta llaveros, tarjetas y discos.

- **Antena que se conecta al lecto-escritor:** es la encargada de transmitir y recibir las señales vía radio que se intercambian entre los transponders y el lecto-escritor RFID. Cuando una señal es emitida, activan los transponders que se hallen en su campo de lectura y provocan que éstos devuelvan la información solicitada por el comando de lectura al lector RFID. Esta operación tarda menos de 100 ms, y la potencia de emisión debe estar alrededor de los 100 mW, y por norma, nunca puede superar 1 Watio. Las antenas pueden ubicarse en sitios fijos, por ejemplo, para leer los elementos que pasen a través de una cinta transportadora, o pueden ser portátiles, para leer transponders que pueden estar ubicados en cualquier lugar. Cuando las antenas se conectan a lectores fijos, la polarización de la antena suele ser linear, mientras que en lectores portátiles, lo más adecuado es una polarización circular. [Huidrobo].

- **Lecto-escritor RFID:** está compuesto por dos módulos, un módulo RF y un módulo de control. El primero es la interfaz entre el transponder y el módulo de control. Se encarga de la emisión de señales vía radio, esto es, emitir la energía necesaria para cargar al transponder, emite y recibe las señales hacia y desde el transponder. El segundo se encarga de manejar la comunicación con el PC, en él se construyen los mensajes a enviar hacia el transponder. Estos mensajes se componen inicialmente por un comando (que hace parte del protocolo de lectura y escritura RFID) y una información adicional. Así, el PC envía esta información al módulo de control y éste hacia el módulo RF, donde finalmente se emite el mensaje vía radio.

3.4.2.3. Aplicativos de las tecnologías de identificación y captura automática de datos

En esta sección se presenta un cuadro comparativo (ver tabla 3) donde se relacionan las tecnologías de identificación y captura automática de datos, con las aplicaciones más comunes. El propósito de esta sección es dar a conocer los aplicativos más usuales y adecuados de estas tecnologías, de manera que se tenga un referente a la hora de seleccionar una de estas tecnologías en la implementación de un sistema que las requiera.

Aplicación	**Reconocimiento biométrico**	**Transporte de datos**	
		T.I.	**RFID**
Identificación de personas	X	X	X
Control de accesos a lugares restringidos	X	X	X
Etiquetado y rastreo de productos			X
Identificación de productos			X
Identificación de personas, animales u objetos a distancia			X
Control automático de inventarios			X
Almacenamiento y actualización de información referente al sujeto u objeto identificado		X	X
Ruteo de productos en procesos de producción			X
Identificación de animales, personas u objetos sin sistemas de bases de datos centrales.		X	X
Identificación de varios sujetos u objetos al mismo tiempo			X
Pagos automáticos (prepago-postpago)		X	X
Sistemas de pago masivo (buses, trenes)			X
Cronometraje de tiempos en actividades deportivas			X
Expedición de tiquetes para la entradas en eventos			X

Tabla 3. Tecnologías de identificación y transporte de datos y aplicaciones.

Estas son, a grandes rasgos, las aplicaciones de estas tecnologías estudiadas en este capítulo. Como se puede apreciar RFID es la tecnología más flexible y se ajusta a todo tipo de aplicaciones, entre las que actualmente se destacan las relacionadas con automatización de procesos de producción y distribución en las cadenas de abastecimiento donde se busca reemplazar los actuales códigos de barras, los sistemas de pago masivos en buses, trenes que agilizan la movilidad de los transeúntes, la integración con la telefonía móvil, cronometraje de tiempos de actuación en actividades deportivas de alta competencia, entre otros. [Auto ID Center], [FusionConsulting], [Huidrobo]. Esta es una tecnología relativamente nueva y por lo tanto aún cuenta con los problemas típicos de estandarización de protocolos por parte de los diferentes proveedores de dispositivos, y aún no han sido adicionadas funciones de encriptación para proteger la información almacenada. Pero quizás la dificultad más grande de esta

tecnología ha sido la protección ante la lectura y de la información contenida en los dispositivos RFID. Precisamente por tratarse de una comunicación inalámbrica, un lecto-escritor portátil RFID podría capturar la información almacenada en un transponder. Esto problemas representan un reto para los entusiastas de la tecnología RFID, pues a pesar de su flexibilidad y amplio espectro de posibles aplicaciones, aún debe superar estos inconvenientes para conseguir una mejor penetración.

Las tarjetas inteligentes han sido mayormente utilizadas en aplicaciones que requieren identificación de personas y almacenamiento de datos personales o financieros. Los avances en seguridad de las tarjetas inteligentes, donde algunas ya cuentan con microprocesadores para encriptar la información contenida, las convierten en un mecanismo muy apropiado para almacenar datos sensibles. Sumado a los esfuerzos en materia de estandarización de protocolos y construcción de APIs[13] en diferentes entornos para facilitar su programación, se está logrando una mejor penetración y aceptación de las tarjetas inteligentes.

Finalmente, los dispositivos de reconocimiento biométrico son muy útiles en la autenticación de usuarios, su principal ventaja sobre las otras tecnologías es que la información de identificación es portada por cada persona a través de sus características biométricas, sin necesitad de dispositivos físicos externos, eliminando las posibilidades de suplantación.

[13] API: Aplication Program Interface - Interfaz de programación de Aplicaciones.

4. CAPITULO IV. MODELO PARA LA AUTOMATIZACIÓN DE PROCESOS DE IDENTIFICACIÓN PERSONAL EN APLICACIONES Y SERVICIOS TELEMATICOS

4.1. Introducción

El presente trabajo de grado, denominado modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos, pretende brindar un referente teórico útil para contextualizar la necesidad y la importancia que está tomando el tema de identificar usuarios de servicios y aplicaciones telemáticas. A partir de esto, brindar ciertas condiciones básicas de seguridad para proteger la información que se transmite a través de medios abiertos como Internet y de esta manera aumentar el grado de confianza por parte de los usuarios de éstos servicios, constituye el problema central a solucionar con el presente proyecto.

En este sentido, el aspecto tecnológico cobra mucha relevancia, razón por la que se hace énfasis en las tecnologías de la información y las telecomunicaciones asociadas a la seguridad (TIC_S), lógicas (SW) y físicas (HW) como soporte para viabilizar el cumplimiento de los principios básicos de una comunicación segura (privacidad, confidencialidad, integridad y no repudio), y como mecanismo generador de confianza para los usuarios.

Con el ánimo de compartir con el lector un punto de referencia respecto al concepto de modelo, los autores citan el concepto de [Coronado y Pino]: "un modelo es una abstracción que se realiza de un objeto o fenómeno, escogiendo algunos elementos que se consideran representativos y relacionándolos de una forma que tenga sentido, con el propósito de lograr una mejor comprensión de ese objeto o fenómeno", de ahí que se derivan dos anotaciones fundamentales: 1) todo modelo es una representación subjetiva, y por lo tanto, un objeto o fenómeno puede tener tantos modelos como personas quieran observarlo y 2) todo modelo está en continua construcción en la medida en que se adquieran nuevos elementos constitutivos y se realice una mayor experimentación con el objeto de estudio.

El modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos pretende proporcionar una visión del problema abordado analizándolo desde el impacto de las TIC en la sociedad, convirtiéndolo en el dominio de aplicación, y ofrecer desde la ingeniería una base conceptual útil para diseñar y construir un sistema de acuerdo a las características del problema planteado. El modelo comprende cuatro componentes constitutivos, que posteriormente se describen uno a uno (ver figura 11).

En el componente denominado "dominio" se hace un cubrimiento amplio de temáticas asociadas a las tecnologías de información y telecomunicaciones, desde el impacto social y económico que éstas producen en las sociedades, la penetración actual y visionaria de las TIC, los diferentes procesos productivos que se apoyan en su

utilización, y los principios básicos de transacciones y comunicaciones seguras como instrumentos tecnológicos que pueden promover la utilización de las TIC.

El segundo componente dedicado a las tecnologías y sistemas que contribuyen en la automatización de procesos de identificación personal, presenta un estudio tecnológico alrededor de los mecanismos electrónicos de control de accesos, cubriendo tecnologías físicas y lógicas que apoyan los procesos de identificación y autenticación de usuarios. Complementariamente expone algunas posibilidades de combinación de éstas tecnologías para construir sistemas automatizados de identificación.

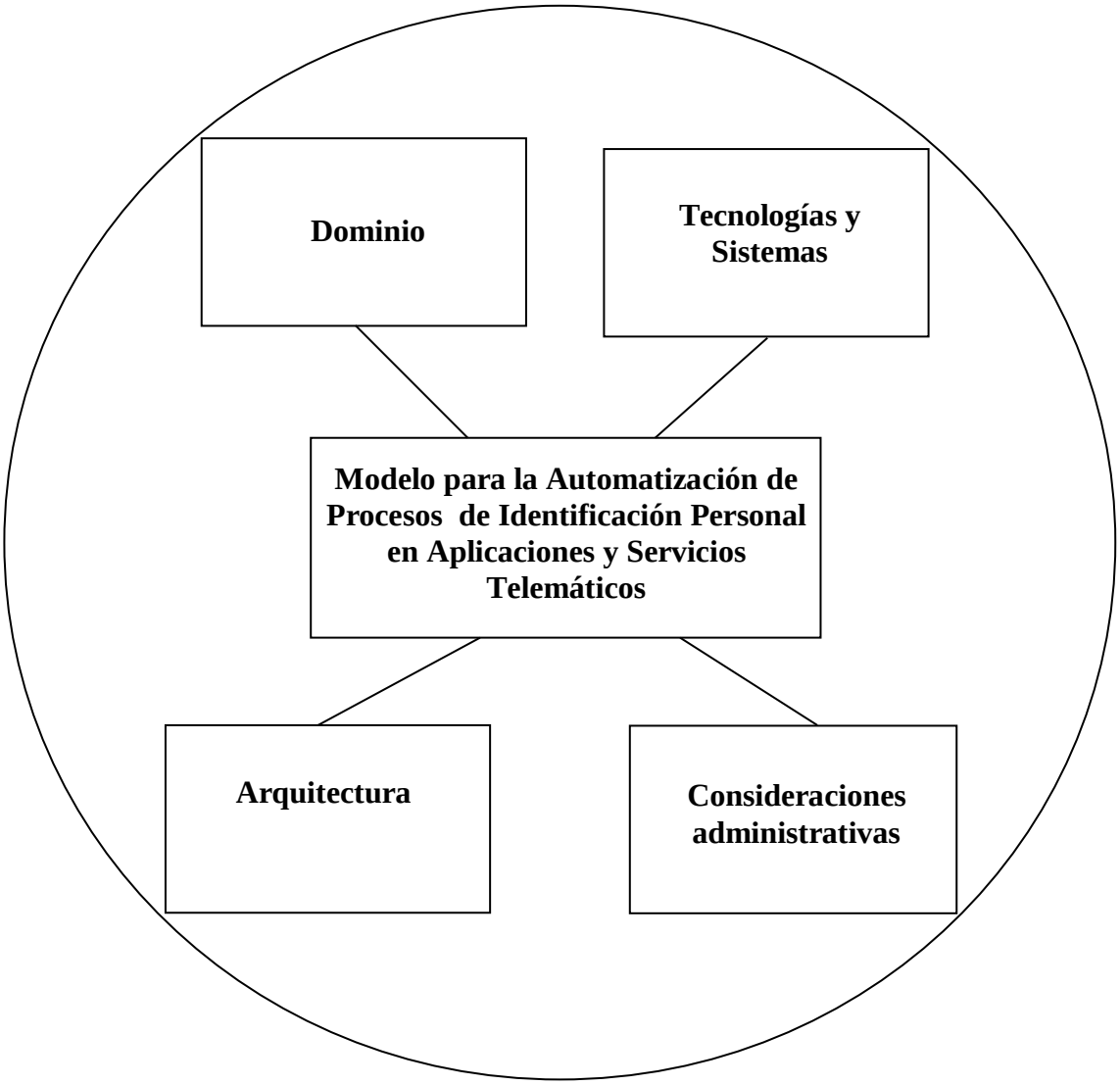


Figura 11. Componentes del Modelo para la Automatización de Procesos de Identificación Personal en Aplicaciones y Servicios Telemáticos.

El tercer componente presenta una arquitectura para la automatización de procesos de identificación, que recoge elementos tanto del marco tecnológico desarrollado en el capítulo dedicado a las tecnologías de información y comunicación asociadas a la

seguridad (capítulo 3), como del segundo componente del modelo relacionado con tecnologías y sistemas para la automatización de procesos de identificación personal. De esta manera, la arquitectura propuesta facilita la visualización de un esquema que contiene los elementos básicos a tener en cuenta a la hora de diseñar un sistema que automatice los procesos en cuestión.

Finalmente, el cuarto denominado "consideraciones administrativas" hace referencia a algunos elementos de gestión para los mecanismos y la información que permiten identificar de manera automática a un usuario de una aplicación o servicio telemático.

4.2. Dominio de aplicación del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos

Este primer componente del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos tiene como finalidad contextualizar ampliamente los campos donde puede ejercer especial influencia el presente trabajo de grado.

Como eje central y transversal a los temas asociados al dominio de aplicación se analizan las tecnologías de la información y las telecomunicaciones, cuyo análisis, no tanto desde el punto de vista técnico sino desde el impacto social y económico que están ejerciendo en las sociedades mas desarrolladas, permiten vislumbrar las repercusiones que puede originar su penetración en nuestro país.

El objetivo es ilustrar desde que punto de vista se hace necesario que el país impulse el sector de aplicaciones y servicios telemáticos y cómo éstos se convierten en un nuevo renglón prometedor de la economía al servir como soporte de nuevos dominios de negocios abiertos a la libre competencia, como los que se esperan venir con la firma de los tratados de libre comercio del momento, (ALCA y TLC)[14].

Adicionalmente se presenta la situación actual del grado de penetración de las TIC en nuestro país y se hace énfasis en un factor del cual se opina que ha frenado su utilización; éste es la inseguridad en las redes de transporte de la información. Para vislumbrar la magnitud de este problema, se presenta un estudio sobre los climas de cultura en materia de seguridad en las organizaciones de nuestro país.

Finalmente, como respuesta a una de las necesidades detectadas al abordar el presente proyecto, para proveer seguridad en los servicios a los que se puede acceder a través de la red de redes y de esta manera incrementar los niveles de confianza por parte de los usuarios, se ilustran los fundamentos básicos de una comunicación segura y la forma cómo tecnológicamente se puede concebir una comunicación que sólo puedan entender las partes involucradas.

[14] **ALCA:** Área de libre comercio de las Américas.
TLC: Tratado de libre comercio con Estados Unidos.

En la figura 12 se detalla la conformación de este primer componente del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos. A continuación se despliegan cada uno de los elementos constitutivos.

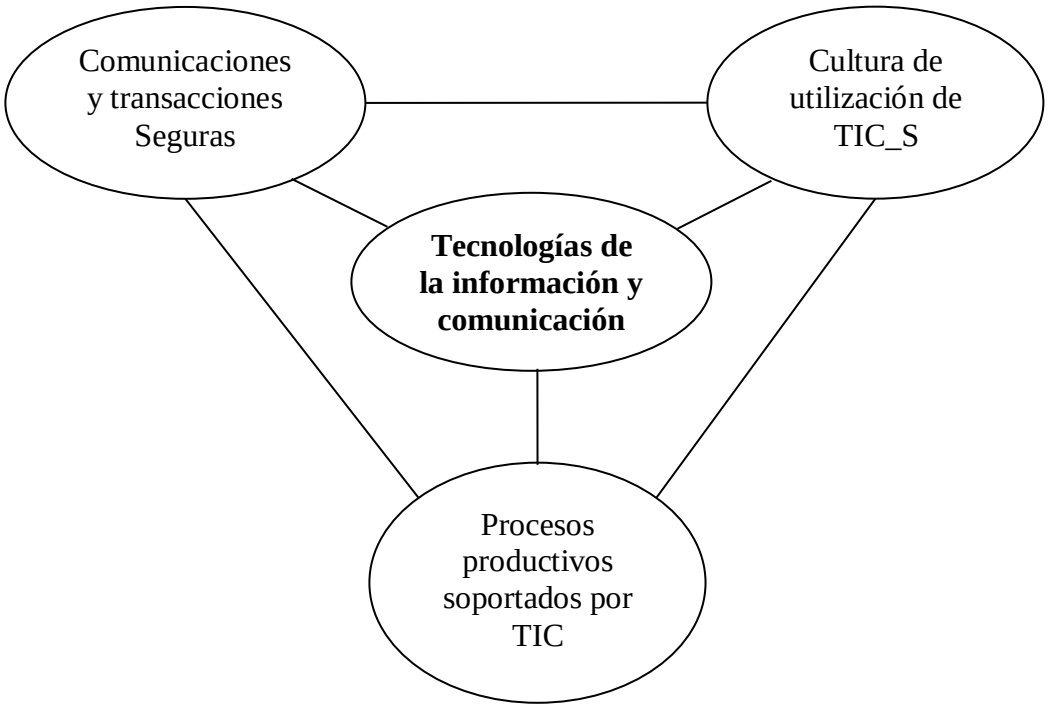


Figura 12. Componente "Dominio de aplicación del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos".

4.2.1. Tecnologías de la información y comunicación

Gran cantidad de literatura encontrada hoy día, relaciona las tecnologías de la información y de las telecomunicaciones con un nuevo modo de desarrollo, una nueva economía y hasta con el surgimiento de una nueva sociedad denominada la sociedad de la información. En este subcomponente, que resulta ser el eje central de los temas abordados posteriormente, se formula un desarrollo teórico tendiente a esclarecer estos conceptos y su relación con las TIC.

La sociedad de la información (SI) representa un esquema de sociedad donde la información se convierte en insumo y factor que revoluciona los procesos productivos. Así como en tiempos pasados, toda revolución tecnológica provocaba una reorganización de la economía y de la sociedad, tal como ocurrió con la invención de la máquina de vapor, el ferrocarril y la electricidad que desencadenaron la revolución industrial, en el momento actual con la fuerza, importancia y utilidad que ha tomado el manejo, almacenamiento y distribución de toda clase de información a través de las TIC,

nos encontramos ante una revolución donde la información es el punto crítico de la transformación de las actividades económicas y sociales.

Los orígenes de lo que hoy se conoce como sociedad de la información datan del año 1993 cuando surge en los Estados Unidos el proyecto de Infraestructura Global de Información[15], promesa del crecimiento económico para las economías nacionales e internacionales. La respuesta europea fue la construcción del informe Europa y la sociedad de la información (1994), conocido también como informe Bangeman[16], construido por la Comisión Europea, según el cual: "La presencia extendida de nuevos instrumentos y servicios de información ofrecería interesantes oportunidades para construir una sociedad más justa, equilibrada y de favorecer las realizaciones personales. La sociedad de la información cuenta con el potencial de mejorar la calidad de vida de los ciudadanos y aumentar la eficacia de las organizaciones"[17].

Así, a la filosofía del proyecto de Sociedad de la información está íntimamente relacionada la idea que es posible lograr un mayor bienestar conforme el progreso se materialice, cualidad que resulta común a otros saltos tecnológicos.

Además el informe describía el plano económico sobre el cual debía desarrollarse la sociedad de la información argumentando: "El mercado llevaría la dirección de los procesos de penetración y sería una primera tarea de los gobiernos, proteger las fuerzas competitivas y garantizar una acogida duradera de la sociedad de la información, de modo que el impulso de la demanda pueda financiar el crecimiento, tal como ocurre en otros sectores"[18].

De esta manera, el proyecto de la sociedad de la información debería abrirse campo a través de la apertura de los mercados; el rol colaborador por parte de los actores públicos sería el de promoción de la puesta en marcha de la iniciativa. Este aspecto debe tenerse muy en cuenta al analizar el grado de penetración que han logrado las TIC, puesto que este enfoque condiciona la política de promoción al servicio universal y replantea el estatuto de servicio público de los bienes y servicios de la información y comunicación, pues al depender del mercado, se limitan las posibilidades reales de acceso para la gente y se cambia el concepto de participación por el de consumo.

Continuando con la visión de la Comisión Europea, las ventajas del proyecto de sociedad de la información en los ámbitos económico, social y político, se expresan así:

[15] Infraestructura Global de información: GII-Global Information Infraestructure.

[16] **Informe Bangeman:** es el principal documento que la unión Europea ha tomado como referencia para la adopción de una filosofía y una legislación en su proyecto de Sociedad de la Información y para incentivar, en el plano industrial, la convergencia de las industrias de telecomunicaciones, informática y audiovisual cuya unificación debería engendrar aplicaciones clave que inviten a los consumidores a expandir el mercado de la SI. Disponible en: http://osi.conselldemallorca.net/pdf/bangemancat.pdf

[17] Idea de un Fragmento del Informe Bangeman, capítulo I: el reto social.

[18] Idea de un Fragmento del Informe Bangeman, capítulo I: plan de acción

- **En lo económico:** permite expandir el mercado, incrementar beneficios, realizar un salto en la productividad y, consecuentemente, aprovechar la convergencia tecnológica protagonizada por las industrias info-comunicacionales.
- **En lo Social:** permite un acceso directo a las fuentes de conocimiento, incrementa el bienestar alcanzado durante la fase denominada, justamente, Estado de Bienestar[19], viabiliza la participación democrática gracias a las facilidades tecnológicas, implica un mejor aprovechamiento del tiempo productivo y mejora la calidad de vida.
- **En lo político:** Permite nuevas oportunidades de participación en una democracia de tipo asambleario, mediante la conformación paulatina de una nueva esfera pública con Internet.

A partir de estos supuestos y la justificación presentada por la comisión europea, nace en los noventas el proyecto de la sociedad de la información, como respuesta de las grandes organizaciones estatales y privadas de los países desarrollados a la crisis iniciada a finales de los años setenta, causada por el agotamiento de las potencialidades del modo de desarrollo industrial, y convirtiéndose en una estrategia de recomposición para el crecimiento y expansión de la economía. Las ideas sobre las cuales se sienta el proyecto son la liberalización (apertura de mercados), la desregulación, y la competitividad internacional. Allí, la información aparece no sólo como recurso ideológico (diversidad de la oferta de información y democratización del acceso) sino como un insumo de productividad ya que contribuye a la lógica del procesamiento de la producción y la circulación de bienes y servicios.

El impacto de este proyecto fue la formulación de un nuevo modo de desarrollo que tuvo como característica fundamental la centralidad de los procesos info-comunicacionales en la estructura productiva de los países altamente industrializados[20].

El nuevo modo de desarrollo, denominado informacional, reforzó los márgenes de ganancia e incrementó la productividad, al tiempo que produjo una alteración de los hábitos de consumo, especialmente en los bienes y servicios info-comunicacionales, generó además una mudanza ocupacional de escala desde la industria hacia el sector servicios. El efecto negativo es la cristalización de nuevas brechas socioeconómicas y culturales con el consecuente efecto montaje sobre las ya existentes.

Según [Becerra], "el modo de desarrollo industrial está determinado por la introducción de nuevas fuentes de energía y por la tendencia a la automatización de la producción y la distribución, mientras que en el modo de desarrollo informacional la fuente de la

[19] **Estado de Bienestar:** son aquellos estados en los que el gasto en bienestar (salud, educación, seguridad social) se convierte en la mayor parte del gasto público total. El modelo de Estado de Bienestar fue un modelo de crecimiento y expansión de la economía. Se correspondió, entonces, con una política de acumulación basada en la edad de oro de la difusión de fuerzas productivas cimentadas en el modo de desarrollo industrial. Este modelo empezó a dar inicios de agotamiento a fines de los años sesenta y se expresó con crudeza en los setenta.

[20] En este contexto, el modelo de desarrollo denominado informacional tendría unas limitaciones muy claras, pues éste sólo se refería a los países con las economías mas avanzadas.

productividad, en cuantía y calidad, es la utilización de conocimiento (su producción, tratamiento, almacenamiento, ordenación, disponibilidad y reproducción) y de las tecnologías y, por tanto, su impacto mayor se advierte en la trasformación de los procesos productivos y en la generación de una nueva tecnología organizacional".

Haciendo un paréntesis a todas estas ideas que han sido presentadas en ráfaga, en la actualidad podemos ver que, aunque con ciertas dificultades, algunos sectores del país han entrado en la era marcada por el nuevo modo de desarrollo, en el que la información es el eje de una gran cantidad de transformaciones que se ven reflejadas en el aumento de la productividad, y a través del cual se busca hacer competencia a las organizaciones internacionales.

Resumiendo algunas ideas de [Becerra], el impacto del modo de desarrollo informacional está orientado a viabilizar las siguientes transformaciones:

- Revolucionar, mediante la aplicación de las nuevas tecnologías de la información, las fuerzas y los procesos productivos, de organización, almacenamiento y gestión.
- Generar una fase de expansión del capital basada en una mayor productividad. Este objetivo está asentado en la innovación tecnológica así como en la creciente desigualdad en la distribución de los beneficios, por lo que en rigor se trata de un incremento de la plusvalía relativa[21] que aparece como fórmula del incremento del excedente, es decir, de la ganancia.
- Lograr la descentralización de la producción y distribución de los bienes y servicios.
- Garantizar la conexión mundial en redes de datos, cuya aplicación prioritaria es la de transportar los flujos financieros de datos.
- Impulsar la privatización de las empresas y entes públicos que, notablemente en el área de actividades info-comunicacionales, originaron, desarrollaron y financiaron estas actividades en régimen de monopolio durante casi todo el siglo XX.
- Vigorizar el cambio de roles del Estado: de planificador, gestor, distribuidor y protector en la época del Estado de Bienestar, desde el fin de la segunda guerra mundial hasta mediados de la década de los setenta, al ejercicio prioritario de las funciones de control, regulación, liberalización, ajuste y acumulación.

El proyecto sociedad de la información también tiene un fuerte impacto sobre la educación toda vez que el desarrollo de nuevas habilidades y capacidades, constituye una función elemental desde un doble propósito: económico, puesto que se configura la fuerza laboral adecuada para lidiar con los retos de un mercado sustancialmente distinto al de hace treinta años; e ideológico, porque contribuye a aprehender los cambios en términos que faciliten la adaptación a estos mismos.

[21] **Plusvalía relativa:** Mientras que la plusvalía absoluta resulta del aumento del monto del trabajo humano empleado durante un tiempo X, sin aumentar la remuneración de ese trabajo, la plusvalía relativa aumenta la productividad mediante el progreso tecnológico que permite producir la misma cantidad de bienes en menos horas de trabajo.

Existe otro término relacionado con TIC que ya cuenta con cierto reconocimiento en nuestro país, y es el de la economía digital, el cual relaciona el surgimiento de la sociedad de la información y otro esquema de desarrollo. Así, según la revista colombiana [SISTEMAS_79], "se trata de un concepto que viene transformando el ambiente de negocios, que no se limita a la simple fusión de las comunicaciones, la computación y la información en un nuevo entorno tecnológico. Abarca mucho más. Por esa razón, es necesario asimilarlo como la evolución de nuestra sociedad, basada en una economía industrial, hacia otro esquema de desarrollo. Es decir, en aquella en la que primaba la productividad de bienes en fábricas organizadas, dentro de un modelo orientado a la especialización de la mano de obra (producción en escala), a una organización distinta. Un entorno, caracterizado por la "producción" de servicios, en un modelo orientado a la manipulación de la información".

Esto indica que en nuestro país se han adoptado los principios de la sociedad de la información y se persiguen los mismos objetivos que alineaba en sus orígenes la Comisión Europea. En otro aparte de [SISTEMAS_79], hace referencia a la competitividad y a la apertura de mercados, así: "economía digital se asocia con el aprovechamiento de las tecnologías de la información, con las infraestructuras abiertas y con las posibilidades que el mercado le está brindando a las compañías de cualquier tamaño, en el sentido de tener una presencia global y herramientas competitivas que las puedan ubicar a la altura de cualquier otra dentro y fuera del país".

Otra referencia a este tema, la realiza la contraloría general de la nación en la revista Economía Colombiana [Economía], donde menciona que: "desde el punto de vista económico, no sólo se han abierto las puertas a otra manera de hacer negocios-compra y venta de bienes y servicios y transacciones financieras en mercados virtuales, sino que han convertido la fabricación de equipos, el diseño de programas y la prestación de servicios en una de las más grandes áreas de inversión y de comercio en la actualidad". Atribuye a las TIC la agilización del proceso de globalización, y advierte el riesgo que trae el carácter transnacional de las inversiones del sector privado en sus campos principales, lo que hace posible que las autoridades nacionales pierdan, en la práctica, el control en buena parte de la estrategia futura en esta actividad. Además, hace mención a que como reflejo de las desigualdades en los aspectos sociales, existe una brecha significativa entre naciones, regiones y sectores de la población, "la brecha digital", la cual paradójicamente se hace cada vez más profunda por estos avances tecnológicos, dada la riqueza desigual de las naciones.

En Colombia la construcción de la sociedad de la información ha correspondido a la iniciativa privada, mientras que al estado le han correspondido dos responsabilidades fundamentales: establecer la regulación adecuada y adelantar acciones que garanticen que se cierre la brecha digital, para que la exclusión social por cuenta de ella no sea mayor, en tanto que el mercado por si mismo no contribuye a su disminución.

El sector privado se ha encargado de la dotación de infraestructura en televisión y telefonía móvil, promoción y mercadeo de equipos de diferente escala, para uso personal, profesional y empresarial, El sector público empresarial (Telecom, ETB y

EPM, en particular) ha aprovisionado la prestación de servicios de conexión a Internet, producción y emisión de programas televisivos y telefonía móvil celular, mientras que las universidades han ofrecido en las últimas décadas programas de formación en Ingeniería Electrónica y de Sistemas, además de las carreras intermedias en computación y materias afines.

De otra parte, para cumplir con sus responsabilidades, el Estado ha adelantado acciones específicas; en materia de regulación: la legislación para reglamentar los servicios de telecomunicaciones (Decreto de ley 1900 de 1990), la regulación de la telefonía móvil celular (ley 37 de 1993), la apertura de la competencia privada en la telefonía de larga distancia (ley 142 de 1994), la reglamentación de la telefonía PCS (ley 550 de 200), el establecimiento de la tarifa plana en la prestación del servicio de Internet (Resolución 307 de la Comisión de Regulación de Telecomunicaciones); y con el objetivo de cerrar la brecha tecnológica se adopta la Agenda de Conectividad.

Con este recorrido a través de la historia de creación de la sociedad de la información, sus principios y objetivos, su influencia en el nacimiento de un nuevo modo de desarrollo y la manera como se ha adoptado en nuestro país, se espera haber provisto de suficiente información para comprender el impacto de las TIC en las sociedades y en caso contrario, se hayan propiciado muchos interrogantes para continuar investigando sobre el tema.

Para introducir el siguiente subcomponente vale la pena reflexionar con el siguiente razonamiento de [Becerra], quien se presenta muy crítico y analítico sobre las repercusiones del proyecto de sociedad de la información: “Cuando la información, que como recurso está potencialmente al alcance de todos, se transforma además en un insumo y en un producto económico primordial, el espacio de intervención comunicativa se va transformando en espacio de mercado”.

4.2.2. Procesos productivos soportados por TIC

Uno de los objetivos mencionados en la visión presentada de la sociedad de la información y que ha empezado a tener rápido efecto, es aquel relacionado con la revolución de las fuerzas y los procesos productivos, de organización, almacenamiento y gestión, a través del soporte que brindan las tecnologías de información y comunicación.

En el subcomponente dedicado a las TIC se hacía una importante referencia citada por la revista Economía Colombiana donde se afirma que con el advenimiento de la sociedad de la información, desde el punto de vista económico, no sólo se han abierto las puertas a otra manera de hacer negocios, compra-venta de bienes y servicios, y transacciones financieras en mercados virtuales, sino que se ha convertido a la fabricación de equipos, el diseño de programas y la prestación de servicios en unas de las más grandes áreas de inversión y de comercio en la actualidad. En este sentido, el comercio electrónico, que podría definirse como uno de los proyectos cumbres de la sociedad de la información,

cobra mucha fuerza y se convierte en una herramienta muy importante en el marco de los tratados de libre comercio.

Así, teniendo en cuenta que una de las actividades productivas que mejor responden al soporte de las TIC es precisamente el comercio electrónico, es importante analizar el origen del macroproyecto de comercio electrónico en el marco de las negociaciones del ALCA y cómo ha sido abordado este tema en nuestro país.

Como es conocido, los países latinoamericanos han iniciado negociaciones para establecer en el 2005 el Área de Libre Comercio de las Américas (ALCA) para lo cual se han establecido varios grupos de negociación y comités expertos. Tal como lo describe [Cárdenas], considerando que para el 2005 el comercio electrónico sería uno de los principales medios para realizar transacciones comerciales, en 1998 se crea un comité conjunto de expertos del gobierno y del sector privado sobre comercio electrónico para que hiciera recomendaciones sobre la manera de aumentar y ampliar sus beneficios y en particular, sobre cómo debería tratarse el tema en las negociaciones del ALCA.

En el primer informe presentado por el comité a los ministros de comercio en 1999[22], se hacían unas recomendaciones sobre los potenciales beneficios del comercio electrónico y los desafíos que tienen los países de la región para su pleno aprovechamiento. Las recomendaciones estaban orientadas a fortalecer la infraestructura de la información, ampliar la participación de los usuarios de Internet, aclarar las normas del mercado y construir confianza en el mismo. Igualmente, para construir confianza en el mercado se formularon recomendaciones sobre seguridad y fiabilidad, autenticación de firmas electrónicas y constancias, privacidad y protección al consumidor.

En agosto de 1999, con el fin de apoyar el desarrollo de los negocios electrónicos y para crear un marco jurídico que genere seguridad entre los usuarios del sector empresarial, el congreso colombiano expidió la ley 527, conocida como la ley del comercio electrónico, por medio de la cual se define y reglamenta el uso de mensajes de datos, el comercio electrónico, las firmas digitales y se establecen las entidades de certificación. Por medio de esta ley, se brinda reconocimiento jurídico y prueba a las operaciones que se realicen electrónicamente y se establecen unos mecanismos de seguridad que se encargan de regular y proteger las transacciones electrónicas, esto es: firma digital, entidades certificadoras y certificados digitales. Igualmente establece que la Superintendencia de Industria y Comercio es el órgano encargado del control y vigilancia de las operaciones electrónicas.

Para consolidar los objetivos de la ley 527, nace Certicamara como una iniciativa de las Cámaras de Comercio por fomentar el uso del comercio seguro entre empresarios, y se crea la primera entidad de certificación digital abierta, sometida al control y vigilancia

[22]ALCA. Documento: FTAA.ecom/01, 4 noviembre de 1999.

Disponible en internet: http://www.ftaa-alca.org/spcomm/derdoc/ec1d_s.asp

de la Superintendencia de Industria y Comercio, que cumple con los más altos estándares tecnológicos y de seguridad.

Certicámara brinda seguridad y garantía en Colombia a las transacciones, comunicaciones y operaciones electrónicas realizadas a través de Internet, con validez y respaldo jurídico en las leyes nacionales mediante la expedición de certificados digitales que facilitan el desarrollo del comercio electrónico en forma segura.

Estando montado todo este aparato político, jurídico y tecnológico, el país se encuentra en condiciones de incursionar en los negocios electrónicos como una oportunidad para incrementar la eficiencia de los procesos productivos, reducir tiempos y costos de operación, agilizar la cadena de distribución, reducir la distancia entre productores y consumidores, facilitar la comparación de precios en los comercios, entre otros beneficios.

En la revista [Economía] se define al comercio electrónico como "un servicio de valor agregado que se presta a través de las telecomunicaciones con fines mercantiles y comerciales, su principal ventaja radica en eliminar restricciones geográficas, fronterizas y de tiempo. Cualquier persona desde su PC, puede acceder a productos y servicios en cualquier lugar del mundo, gracias a las facilidades que ofrecen las TIC, lo cual incrementa las posibilidades del comercio internacional de bienes y servicios."

De acuerdo a los estudios de la firma Boston Consulting Group, las transacciones de comercio electrónico en Internet en América Latina en el año 2001 alcanzaron US$1.280 millones, de los cuales el 71% fue por cuenta de Brasil, el 9.3% por México, 9.3% Argentina, 3.5% Chile y el restante 5.9% por los otros países, incluido Colombia. En consecuencia, la cifra de este renglón aún es muy modesta en Colombia. Sin embargo, vale mencionar, tal como aparece en [Economía], de las 5.922 empresas industriales que fueron entrevistadas en 2001 por el Dane, el 70% manifestó que estaba conectado a Internet y, de este total, el 25.67% tiene sitio Web, que lo utilizan de la siguiente manera: el 51.78% para la comercialización de productos de la industria, el 10.88% para pagos en línea, procesamiento de órdenes y envío en línea y capacidad de ofrecer transacciones seguras; y el 46.06% lo utiliza en otros servicios.

También es relevante el dato que informa que cerca de un millón de microempresas que existen en Colombia, el 4.1% dice disponer de computador y de éste el 37.2% está conectado a Internet. Si esto concuerda con la realidad, existen en Colombia 15.252 microempresas conectadas a Internet y que representan un buen potencial para innovar sus procesos productivos a través de un modelo de negocio soportado por TIC e incursionar en el comercio electrónico.

Como se pudo haber visualizado, es muy grande el campo de acción donde resulta propicio el soporte de las tecnologías de información y telecomunicaciones para agilizar procesos productivos, razón que ha llevado a analizar la necesidad de propiciar ambientes seguros para el intercambio de la información que se comparte a través de las redes de comunicación, y que suplen los contratos escritos o presenciales. Igualmente

en los casos donde la información se convierte en un insumo o mercancía, es necesario proveer mecanismos seguros de entrega. De esta manera, la seguridad de la información empieza a adquirir un rol protagónico en el auge de los procesos productivos que se apoyan en TIC, además de ser un mecanismo generador de confianza para los usuarios de servicios soportados por TIC.

4.2.3. Cultura de utilización de las TIC_S

El objetivo de este subcomponente es ilustrar el grado de penetración que han logrado las TIC e indagar acerca de la importancia que las organizaciones le otorgan al tema de seguridad informática. Para dar respuesta a estos cuestionamientos se recurrirá a las estadísticas de penetración de Internet y a las encuestas en materia de seguridad realizadas por revistas especializadas en el tema. A partir de los resultados de estas encuestas se busca conocer la cultura que existe alrededor de la utilización tecnologías de información y telecomunicaciones asociadas a la seguridad, TIC_S, y establecer una relación de estos resultados con el grado de confianza que tienen los usuarios de TIC a la hora de transmitir información confidencial a través de la red o información sensible para realizar transacciones de tipo comercial.

A nivel mundial, uno de los países con mayor penetración de Internet es Estados Unidos, donde más de un 53% de la población ha accedido alguna vez a Internet. En Europa, Irlanda cuenta con un 69% de navegantes, seguido por Suecia con 64%, Holanda con 58%, Gran Bretaña con 55%, Noruega con 54%. En Francia o Italia, dos de los siete países mas ricos del mundo, la población con acceso a Internet no llega al 34% (En Francia no llega al 30%). En Alemania, es del 36%, en España del 19% y en Rusia 6%.

En el resto del mundo la situación es mucho más precaria. Según la consultora Merrill Lynch[23], en América Latina a pesar de que el porcentaje de navegantes crece muy rápidamente, la audiencia sigue siendo muy pequeña. Con 445 millones de habitantes, al finalizar 1999, sólo el 1.4% de la población latinoamericana había accedido alguna vez a Internet y menos del 20% de las computadoras se había conectado a la red.

Para ver más claramente el fenómeno de penetración en América Latina se presenta la figura 13.

Según esta gráfica, el índice de penetración de Internet en Colombia se encuentra por debajo de la media de América Latina y es ampliamente superado por países como Chile con 20.61%, Uruguay con 11.83%, Argentina con 11.20%, Perú con 7.48% y Venezuela con 5.04%.

A pesar de la baja penetración de Internet en Colombia (4.58%), las TIC asociadas al uso de Internet han permitido dinamizar procesos en algunos sectores de la economía, están siendo adoptadas para soportar procesos educativos, han permitido el acceso de toda clase de comunidades a la información global reduciendo los tiempos y espacios

[23] Consultora Merrill Lynch: http://www.ml.com

geográficos, se ha hecho posible desplazar la realización de algunas operaciones financieras, que anteriormente requerían de la presencia física en determinados horarios y lugares, hacia las transacciones electrónicas, favoreciendo la comodidad de los ciudadanos, entre otros beneficios.

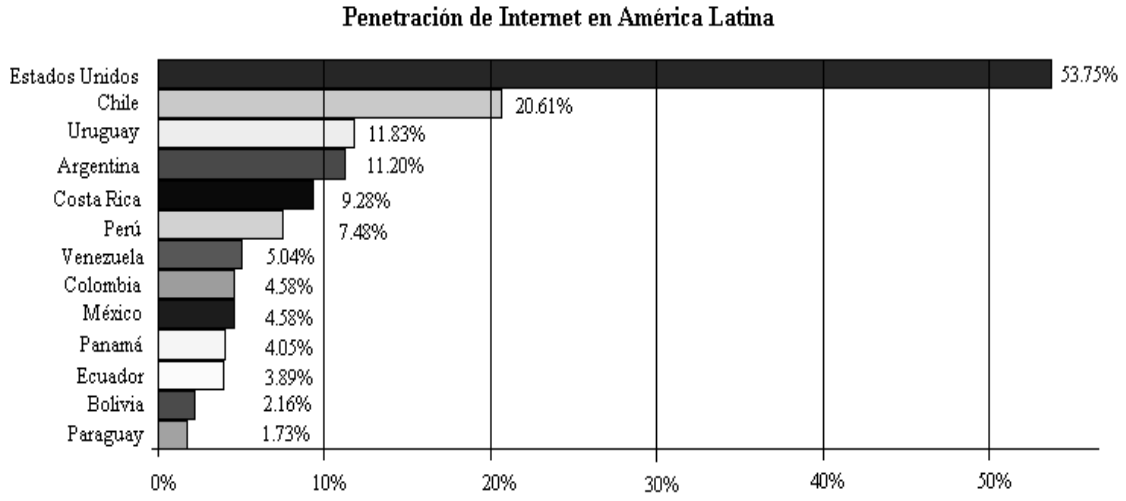


Figura 13. Estadística de penetración de Internet en América Latina. [Economia].

En relación al tema del comercio electrónico, aunque podría pensarse que a mayor penetración, mayor cantidad de usuarios, y por lo tanto mayor participación de ventas, el patrón no funciona así. Este es el caso de Chile, que a pesar de tener la penetración de Internet más alta en América latina, su participación en ventas por comercio electrónico está por debajo de países como Argentina y México, que han alcanzado respectivamente la mitad y la cuarta parte de la penetración de Internet de Chile. Mientras que entre Argentina y México, el porcentaje de participación en ventas es similar, la penetración no lo es.

Estos resultados sugieren un análisis acerca de la cultura de utilización de las TIC que se supone, interviene directamente en la confianza de los usuarios a la hora de realizar una transacción electrónica.

Así, para el caso colombiano, la revista [SISTEMAS_85] en un artículo titulado “el fantasma de la inseguridad”, argumenta que al parecer las dificultades alrededor de las transacciones y del comercio electrónico en el país, obedecen a la ausencia de una cultura que genere confianza, más que a un problema técnico o de infraestructura.

En Colombia, según entrevista realizada a personajes representativos de las instituciones bancarias mas grandes del país (Mastercard, Redeban Multicolor, Credibanco Visa, Bancafé, entre otros) (SISTEMAS_85), existe la infraestructura y la adecuada seguridad para efectuar transacciones electrónicas, la mayoría de éstas se realizan utilizando el

protocolo SSL[24], que brinda la protección adecuada para la información sensible que viaja a través de la red. Luego, el la inseguridad en las transacciones no es más que un fantasma al que los usuarios le temen por desconocimiento de los mecanismos de seguridad que son implementados.

La carencia de confianza por parte de los usuarios, ha entorpecido el crecimiento del comercio electrónico, haciendo que aún la mayoría de transacciones no se realice a través de Internet. El fantasma de la inseguridad que acompaña a los procesos de venta y compra virtuales hace que los consumidores tengan cierta aversión a suministrar el número de sus tarjetas de crédito o de sus tarjetas débito, pues temen que personas inescrupulosas los capturen a través de la red para efectos de suplantación, que representa precisamente el mayor riesgo para el caso electrónico.

La desconfianza por parte de los usuarios a la hora de realizar transferencias electrónicas y sus repercusiones en la utilización del comercio electrónico ha empezado a preocupar a los sectores entusiastas de la iniciativa en el país, el sector bancario y empresarial. Estos, han detectado la ausencia de cultura para realizar transacciones electrónicas tanto en el usuario final como en las compañías. El problema se evidencia desde los mismos empresarios dueños o gerentes de empresas quienes no conocen acerca de la seguridad básica para proteger la información. En consecuencia, si la cultura sobre seguridad no parte de los mismos empresarios, será muy difícil que se vea reflejada en otras instancias de las organizaciones.

Alrededor del tema de la seguridad ya se está empezando a crear conciencia y justamente la Asociación Colombiana de Ingenieros de Sistemas, desde el año 2001 viene realizando anualmente una encuesta nacional tendiente a analizar las tendencias sobre seguridad informática en el país. A continuación se comentarán algunas conclusiones de los resultados de la encuesta realizada en el 2004 [Sistemas_89].

- Existe una importante participación de la pequeña y mediana industria, que poco a poco ha ido tomando conciencia del tema de seguridad. No solo con el propósito de aumentar los niveles de seguridad de sus infraestructuras, sino de generar confianza en sus clientes a través de servicios personalizados y productos diferenciados.
- Los directivos de las organizaciones, los profesionales del área de tecnología y las personas involucradas con el tema de seguridad, se están involucrando con los temas asociados a la seguridad informática, pero no con el impacto requerido ni el entendimiento de la misma. Este tema continua mostrando un matiz técnico, representando un reto para los profesionales de la tecnología, en el sentido de hacer de esta disciplina un proceso transversal en toda organización.
- Se ha incrementado la inversión en la concienciación y formación del usuario final, así como en la generación de negocios electrónicos.
- Se ha dado un aumento en la inversión en materia de seguridad informática por parte de la mediana industria que ha visto el potencial de los negocios

[24] SSL: Secure Socket Layer. Protocolo de sockets seguros.

electrónicos, y ha empezado a tratar a la seguridad informática no sólo como un requisito técnico sino como parte de la estrategia de negocio.

Estos resultados son muy positivos para el propósito de incrementar la oferta de aplicaciones y servicios a través de una estrategia relacionada con generar procesos de cultura hacia el uso de las transacciones electrónicas y el montaje de esquemas seguros.

Los esfuerzos desarrollados en estos dos sentidos podrían mejorar el nivel de confianza de los usuarios hacia la utilización de medios electrónicos para realizar compras, ventas, pagar servicios públicos, realizar transferencias bancarias y e incluso pagar por acceder a nuevas aplicaciones y servicios telemáticos.

4.2.4. Comunicaciones y transacciones seguras

En este subcomponente se hace referencia a los principios básicos de seguridad que fueron ilustrados ampliamente en el capítulo relacionado con tecnologías de información y comunicaciones asociadas a la seguridad (capítulo 3), que garantizan el establecimiento de una comunicación segura.

A manera de resumen, para garantizar la seguridad de la información, se deben cumplir las siguientes condiciones: confidencialidad, integridad, autenticidad y no repudio.

- **Confidencialidad:** consiste en mantener una comunicación por completo privada, protegiendo la información de ser leída por actores externos.
- **Integridad:** Consiste en verificar que la información no ha sido alterada en el transcurso recorrido a través del medio de comunicación.
- **Autenticidad:** Consiste en verificar que el usuario es quien dice ser.
- **No repudio:** Consiste en asegurar que un usuario no pueda negar una acción que ha ejecutado

Gráficamente el esquema básico de una comunicación segura se ilustra en le figura 14.

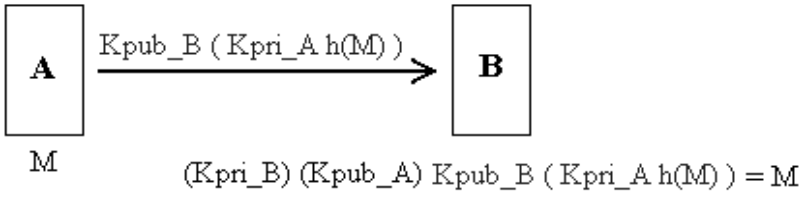


Figura 14. Esquema básico de una comunicación segura.

En la figura 14 se puede observar que al mensaje enviado por el usuario A se le ha calculado el hashing con el fin de verificar la **integridad** del mensaje, h(M). Cuando el mensaje se ha firmado con la clave privada de A (KpriA h(M)), se que comprueba efectivamente que A lo envió -**autenticación**- y se logra que no pueda negar el haberlo firmado -**no repudio**-, pues la clave privada es de exclusivo conocimiento del usuario A. Además el mensaje se cifra con la clave pública de B para que sólo él pueda descifrarlo con su clave privada, consiguiendo la **confidencialidad**.

A manera de conclusión se presenta a continuación en la tabla 4, los principios básicos de una comunicación segura y los métodos que se utilizan para implementarlos.

Principios	Método utilizado
Confidencialidad	Encriptación de la información. Firmar el mensaje a enviar con la clave pública de quien lo debe recibir.
Integridad	Utilización de las funciones de message digest o de hashing. Se compara el hashing del mensaje enviado y firmado con la clave privada del emisor (utilizando la clave pública del emisor), con el hashing del mensaje que llega.
Autenticidad	Cuando el emisor firma con su clave privada un mensaje, este no puede negar que él fue quien lo creó, pues la clave privada es de su exclusivo conocimiento. Utilización de la firma digital, aplicada sobre la información contenida en un certificado digital asociada a una clave privada de conocimiento exclusivo del usuario.
No repudio	Cuando se desencripta un mensaje con la clave pública del emisor, este no pede negar su autoría ya que el mensaje fue firmado con su correspondiente clave privada. Utilización de la firma digital.

Tabla 4. Principios y métodos para establecer una comunicación segura.

Estos conocimientos básicos deben ser conocidos por los usuarios de TIC para que tengan confianza en los sistemas que presten los servicios básicos de seguridad y protejan su información, y eliminen el temor de realizar transacciones electrónicas.

4.3. Tecnologías y sistemas para la automatización de procesos de Identificación personal y protección de la información

El segundo componente del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos se encarga de relacionar las tecnologías de identificación y captura automática de datos con las herramientas de identificación de actores en red (infraestructura de claves públicas, entidades certificadoras), ambas ampliamente desplegadas en el capitulo dedicado a las TIC_S (capitulo 3), para construir sistemas que automaticen los procesos de identificación personal a través de sistemas abiertos como el Internet.

La necesidad de autenticación de los usuarios en aplicaciones y servicios telemáticos se deriva de diferentes razones, entre ellas, salvaguardar la confidencialidad de las comunicaciones que se realizan a través de la red, proteger la información que comparten los usuarios, garantizar la seguridad de las transacciones electrónicas, proteger los niveles de acceso de acuerdo con el perfil de los usuarios, entre otras.

Tal como se ilustró en el primer componente, existe desconfianza por parte de las personas que se conectan a redes abiertas para realizar transacciones comerciales, además temor por que información confidencial pueda ser interceptada por personas malintencionadas. Una posible solución a este problema, que propone este trabajo de grado, es emplear las tecnologías de identificación y captura automática de datos, y las potencialidades de las tecnologías para la identificación de actores en red para autenticar todas las entidades (personas, sitios Web, bancos) involucradas en una transacción comercial electrónica o en una comunicación, y cifrar la información que viaja a través de los medios de transmisión, de tal manera que sólo los destinatarios apropiados puedan descifrarla. En este sentido es importante considerar las diferentes opciones tecnológicas que facilitan la autenticación de los actores que participan en una transacción o comunicación electrónica, y de acuerdo a la participación e influencia de cada actor, seleccionar la más adecuada para su identificación.

Este componente esta conformado por cuatro subcomponentes a saber: un subcomponente central relacionado con los mecanismos electrónicos de control de accesos donde se brinda una introducción a la creciente necesidad de identificar y autenticar a las personas que acceden a los servicios telemáticos y las diferentes TIC_S[25] empleadas para tal fin, otros dos subcomponenetes dedicados respectivamente a las tecnologías de identificación y captura automática de datos, y herramientas de identificación de actores en red, (ilustrados en el capitulo 3 de TIC_S), donde se amplía información sobre herramientas, mecanismos y estándares relacionados con las diferentes tecnologías. Finalmente, el subcomponente dedicado a los sistemas de automatización de procesos de identificación y protección de información, relaciona los otros tres subcomponentes para construir sistemas que automaticen el proceso de identificación de usuarios en aplicaciones y servicios telemáticos y garanticen el cumplimiento de los principios básicos de seguridad en las comunicaciones.

En la figura 15 se ilustran los cuatro subcomponetes del componente número dos del Modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos, denominado tecnologías y sistemas para la automatización de procesos de identificación personal y protección de información. Cada subcomponente se detalla a continuación.

[25] TIC_S: Tecnologías de información y comunicación asociadas a la seguridad.

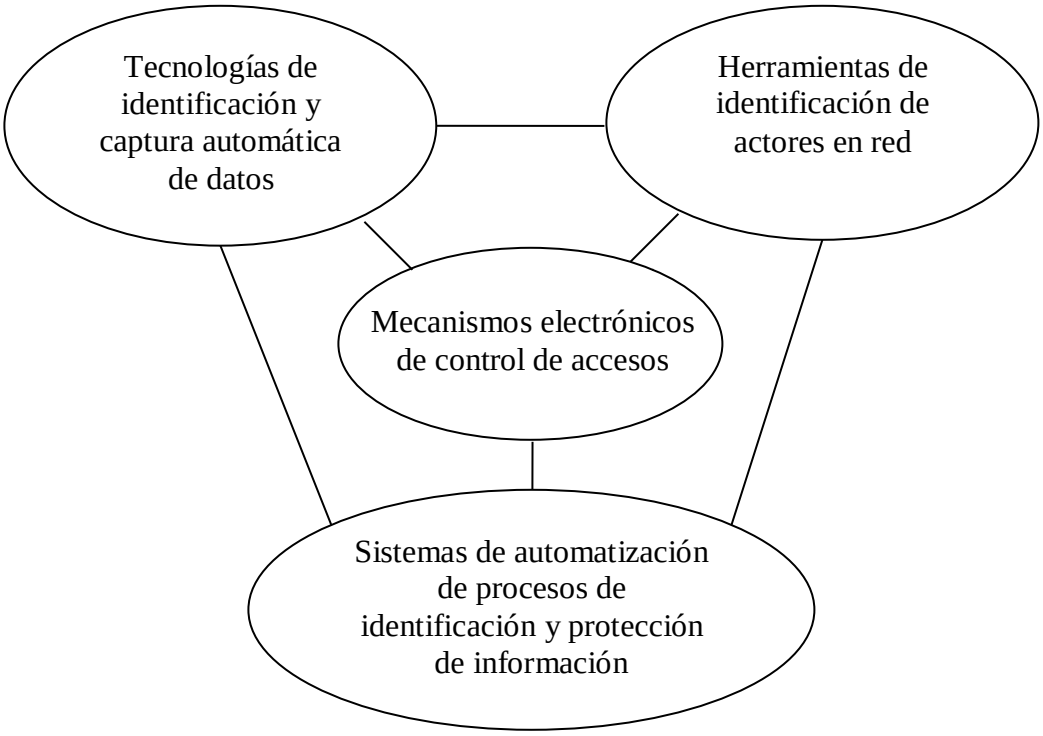


Figura 15. Componente "Tecnologías y sistemas para la automatización de procesos de Identificación personal y protección de la información".

4.3.1. Mecanismos electrónicos de control de accesos

La necesidad de controlar el acceso de personas a ciertas áreas o lugares, ha trascendido los espacios físicos para trasladarse a los espacios virtuales. En este sentido, las tecnologías de la información y comunicación, han permitido traspasar las fronteras físicas y han abierto otra clase de espacios que un usuario puede acceder desde cualquier lugar del mundo, con la ayuda de un computador conectado a la red de redes.

Estos espacios virtuales pueden ser centros de investigación, periódicos, revistas, universidades, concesionarios de autos, centros comerciales, tiendas, video tiendas, casas de discos, en fin, todo lo que pueda existir físicamente, puede tener un espacio virtual y algunas experiencias que requieren de desplazamiento físico y disponibilidad de tiempo, están siendo exitosamente reemplazadas por las transacciones electrónicas, mejorando la calidad de vida de las personas. Un ejemplo simple puede ser el pago de servicios públicos desde la casa, evitando las prolongadas colas.

Esta facilidad que se presta a los usuarios de acceder desde cualquier parte a un espacio virtual representa un reto adicional en materia de identificación de usuarios. Teniendo en cuenta que los mecanismos tradicionales de autenticación de personas, requieren de la presencia física de la persona y la posesión de un documento que demuestre su identidad, los diferentes mecanismos electrónicos de control de accesos suplen estos

requisitos y se pueden complementar en un sistema que automatice el proceso de identificación, haciendo posible que un usuario de servicios a través de un sistema abierto como Internet, pueda probar su identidad y validar su acceso a él. A partir de las diversas experiencias que indican que los sistemas convencionales que validan la identidad de los usuarios a través de un identificador y una contraseña son insuficientes, se presentan a continuación una breve descripción de los distintos mecanismos que pueden ser empleados complementariamente para autenticar a un usuario a través de la red.

Los diferentes mecanismos electrónicos de control de accesos son: la identificación del usuario, la autenticación del usuario, la verificación de la autenticación y la re-autenticación, que se ilustran (figura 16) y describen a continuación:

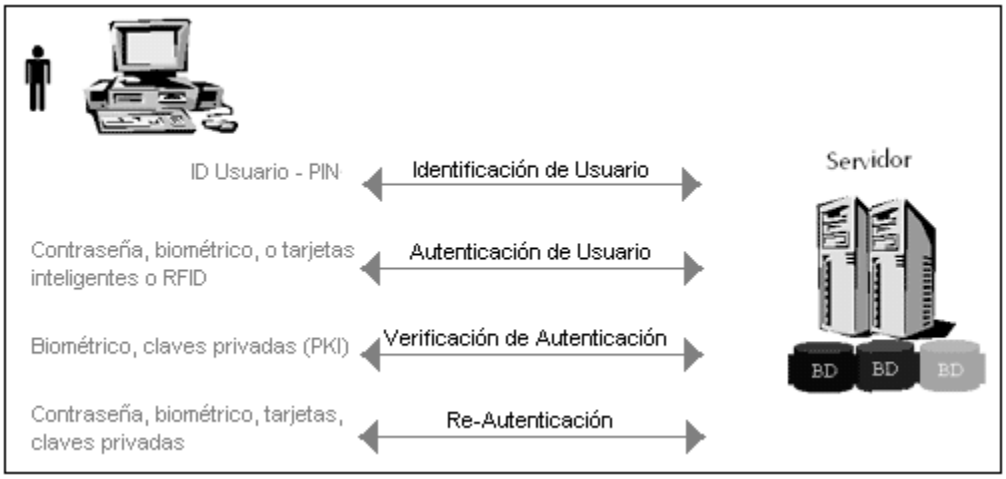


Figura 16. Mecanismos complementarios de un sistema de control de acceso

- **Identificación del usuario:** es el proceso que unitariamente identifica las características pertenecientes a un usuario y que ninguno otro tiene. El propósito de la identificación es permitir a ciertos usuarios acceder y utilizar un sistema en particular. Tecnológicamente este mecanismo se implanta mediante la asignación de un "nombre de usuario", "User ID" o el PIN[26] (Personal Identification Number). Normalmente, existen en las organizaciones parámetros o estándares para construcción de los nombres e identificadores de usuarios (User ID) basados en nomenclaturas.

- **Autenticación del usuario:** la autenticación se define como "el proceso que confirma la identidad del usuario. Este mecanismo se apoya en la utilización de un elemento confidencial que tiene estrechos vínculos con la identificación de usuario (User ID). Este elemento puede tomar diferentes formas, por ejemplo, algo que el usuario posee, tal como una tarjeta inteligente, o algo que el usuario conoce, como un PIN o contraseña, o algo que el usuario es, por medio de

[26] PIN: personal identification number. Número de identificación personal.

medidas biométricas. Por tanto, este mecanismo se basa en la confidencialidad y carácter secreto de estos elementos, lo que hace que en teoría, ningún otro usuario pueda utilizarlos.

- **Verificación de la autenticación:** es "el proceso mediante el cual se prueba la autenticidad del usuario", sin lugar a duda. Las tecnologías que se utilizan para este fin, son las de reconocimiento biométrico y las basadas en esquemas de claves públicas. En el caso de la biometría, este mecanismo se está haciendo más popular y práctico en la actualidad, debido a que sus precios se están reduciendo y comienzan a ser más asequibles. Y para el caso de los esquemas de claves públicas, existen aplicaciones libres que generan las claves públicas y privadas, y facilitan servidores públicos para publicar las claves públicas y así, permitir el intercambio de documentos firmados a través de la red.

- **La re-autenticación:** es "el proceso por medio del cual se reconfirma, en un momento dado, la autenticidad del usuario". Este mecanismo tiene que ver con el hecho de mantener la autenticación del usuario, mediante el monitoreo constante de las sesiones abiertas por éste en un sistema. El propósito primario de la re-autenticación de usuario es garantizar que sea el mismo usuario quien continúa trabajando en el tiempo en una determinada sesión del sistema. Por lo tanto, en determinados intervalos de tiempo vuelve a solicitar al usuario su identificación (User ID) y contraseña, o en caso de contar con biométricos, solicita que vuelva a utilizar el biométrico para autenticarse, de lo contrario el sistema hará que se cierre la sesión.

Estos cuatro mecanismos de control de acceso pueden ser implantados en un sistema, con la posibilidad de ser utilizados mediante la combinación de ellos. Un uso eficiente de estos mecanismos requiere de un estudio de las características de seguridad que debe tener el sistema a ser protegido para determinar la combinación mas adecuada y luego identificar la tecnología que más se adecue en un esquema costo/beneficio.

4.3.2. Herramientas de identificación de actores en red

En este subcomponente se ilustran algunas alternativas tecnológicas existentes para identificar los diferentes actores que participan de una transacción o comunicación electrónica, estas son, la infraestructura de claves públicas y los sistemas PGP y MIME. Estas tecnologías tienen un elemento común, que consiste en la utilización de la criptografía de claves públicas (vista en el capítulo 3) que como se ha mencionado a lo largo del documento, facilita el cumplimento de los principios básicos de una comunicación segura (confidencialidad, integridad, autenticidad y no repudio) entre actores telemáticos.

4.3.2.1. Infraestructura de claves públicas (PKI)

Una solución fuerte y robusta al problema de identificación de actores en red, es la utilización de certificados digitales y de la criptografía de claves públicas, que son elementos constitutivos de una infraestructura de claves públicas. Los servicios básicos prestados por una PKI tienen que ver con la gestión del ciclo de vida de los certificados digitales, es decir, la expedición, validación, publicación, renovación y revocación de certificados [Johner]. Para prestar tales servicios, la infraestructura cuenta con un conjunto de entidades administrativas que cumplen diversas funciones, las más comunes son:

- **Autoridad de registro (RA):** su función principal es identificar y autenticar a los usuarios que solicitan alguno de los servicios que ofrece la infraestructura para luego remitir la solicitud a la entidad certificadora (CA). La cantidad de información del solicitante que es requerida para tramitar la solicitud, depende de la clase de certificado. Así, por ejemplo, a las organizaciones que manejan información o transacciones muy sensibles (ej. bancos, instituciones de gobierno, sitios Web), se requiere suficiente información que acredite a la entidad. Cuando la CA expide el certificado, lo envía a la RA para que ésta lo distribuya a las personas o entidades que lo solicitan.
- **Servidor de solicitudes:** Se encarga de almacenar todas las solicitudes de servicios realizadas tanto por la autoridad de registro como por los usuarios del sistema. Dichas solicitudes son recuperadas posteriormente por la Autoridad de Certificación para tramitarlas.
- **Autoridad de certificación (CA):** es la entidad encargada de tramitar las solicitudes de servicio realizadas por ciertas entidades del sistema. En general está facultada para expedir, renovar y revocar los certificados, firmar las políticas de certificación, y publicar la información en los repositorios de datos tanto internos como públicos. Estas operaciones realizadas por la CA se describen brevemente a continuación.
    - **Expedición de certificados:** es quizás el elemento más importante de los servicios de la PKI. Antes de expedir un certificado, la CA requiere información con la cual se pueda comprobar la identidad del solicitante. Cuando la solicitud es enviada por la RA, la CA no hace la validación de ésta información. Después de la verificación de la veracidad de la información suministrada por el solicitante, la parte más delicada es la generación de las claves pública y privada que se asociarán al certificado. Algunas CAs generan estas claves, pero esto puede convertirse en un hueco se seguridad, así es que lo más adecuado es que el cliente genere por su propia cuenta estas claves, presente su clave pública a la CA y almacene en un lugar muy seguro su clave privada.
    - **Renovación de certificados:** todo certificado tiene un periodo de validez asociado a una fecha de expiración. Cuando un certificado expira, el usuario o la entidad debe acudir a un proceso de renovación, presentándose nuevamente ante la RA y acreditando su identidad.
    - **Revocación de certificados:** en ciertas condiciones como la pérdida o robo de la tarjeta inteligente o token USB, los certificados digitales deben

dejar de ser válidos antes de que se agote su periodo de validez. Cuando esto sucede, la CA debe colocar el certificado en la lista de certificados revocados, esto es, coloca el número serial del certificado y alguna otra información asociada en la lista de certificados revocados. Algunas PKI ofrecen la posibilidad de que sea el propio usuario quien revoque su certificado haciendo uso de su navegador y el certificado en cuestión. Esta última opción sólo es posible en el caso de que el usuario siga teniendo acceso a su clave privada.

- **Repositorio público:** Dicha entidad almacena los certificados digitales (tanto de usuarios como de las propias entidades que componen el núcleo de la PKI) y las listas de certificados revocados emitidas por las CA.
- **Base de datos interna:** Almacena cada una de las solicitudes y documentos emitidos por la infraestructura.
- **Administrador:** es la entidad encargada de la configuración de los parámetros de funcionamiento de la infraestructura. Entre dichos parámetros se encuentra la política de la PKI, que es el reflejo digital de las prácticas de certificación del sistema, y que constituye el elemento clave que guía a gran parte de procesos a la hora de gestionar el ciclo de vida de los certificados.

4.3.2.2. PGP (Pretty Goog Privacy)

PGP[27] que en su versión de libre distribución se denomina GnuPG[28], es una aplicación popular desarrollada para asegurar mensajes y archivos. Es quizás la aplicación para correo electrónico en Internet más usada. Emplea una variedad de estándares de encriptamiento y permite generar las claves públicas y privadas. Las aplicaciones para encriptamiento/desencriptamiento PGP están disponibles de manera gratuita para la mayoría de los sistemas operativos. Las claves privadas son protegidas con frases de paso, siendo más fáciles de recordar por parte de los usuarios. La característica principal de estos sistemas es que cada usuario cuenta con un llavero de claves públicas y uno para la clave privada. En el llavero de claves públicas, cada usuario puede almacenar las claves públicas de los usuarios con los cuales se relaciona y está firmado por su correspondiente clave privada. De esta manera, PGP y GnuPG no cuentan con entidades de certificación para autenticar a los usuarios y su filosofía de confianza se basa en un esquema directo, donde cada usuario confía en las claves públicas de las personas que conoce personalmente y las introduce en su llavero de claves públicas. Otra característica importante es que estas herramientas cuentan con servidores públicos donde almacenan todas las claves públicas de una comunidad de usuarios. Así, cuando un usuario desea agregar la clave pública de una persona conocida en su llavero, debe buscarla en éstos servidores y almacenar la llave pública de su conocido en su propio llavero.

[27] PGP: Pretty Good Privacy. Muy buena privacidad.

[28] GnuPG: GNU Privacy Guard. Es un reemplazo completo y libre de PGP (Pretty Good Privacy). No utiliza el algoritmo patentado IDEA por lo que puede ser utilizado sin restricciones. GnuPG cumple con las especificaciones del OpenPGP descrito en el RFC 2440.

4.3.2.3. S/MIME (Secure/Multipurpose Internet Mail Extensions)

S/MIME[29] es uno de los protocolos de seguridad para el correo electrónico, que especifica no solamente cómo encriptar y firmar mensajes, sino cómo manejar llaves, certificados y algoritmos criptográficos. S/MIME encripta y firma mensajes de Internet MIME[30] que es el estándar propuesto para los mensajes de correo electrónico de multipartes. El formato MIME permite al correo electrónico anexar textos pesados, gráficos, audio y más, pero MIME en sí, no provee ningún servicio de seguridad. El propósito de S/MIME es definir tales servicios siguiendo la sintaxis proporcionada por el PKCS#7[31] sobre encriptación y firmas digitales. S/MIME utiliza certificados digitales, por lo tanto, emplea algún tipo de autoridad de certificación, ya sea corporativa o global, para asegurar la autenticación. S/MIME ha sido adoptado por un buen número de vendedores de productos de mensajería y networking (trabajos en red), entre ellos: ConnectSoft, Frontier, FTP Software, Qualcomm, Microsoft, Lotus, Wollongong, Banyan, NCD, SecureWare, VeriSign, Netscape, and Novell.

4.3.2.4. Estándares para la criptografía de claves públicas

Como se puede apreciar la utilización de las claves pública y privada para cifrar información e identificar de esta manera al portador de la clave privada, es un elemento común de estas tecnologías de identificación de actores en red, que además permiten cumplir con los principios básicos de una comunicación segura. La diferencia esencial de estas tecnologías radica en el esquema de confianza que utilizan, pues de acuerdo al tipo de entidad o de usuario que se desee identificar, de la importancia de la información a ser compartida entre actores y el tipo de actividad (comercial, académica, social), se analiza la necesidad de una entidad certificadora que se encargue de verificar la identidad del actor y proporcionarle un certificado que de fe que el actor es quien dice ser.

Como se ha ilustrado hasta el momento, la criptografía de claves públicas es un elemento indispensable en la identificación de actores en red, razón por la que existen estándares para generar las claves públicas y privadas, encriptar y desencriptar información sensible, encriptar un documento con una frase de paso, protocolos para el intercambio de certificados, y otras operaciones relacionadas con el uso de las claves públicas y privadas. Estos estándares para la criptografía de claves públicas (PKCS[32]) son especificaciones que fueron desarrolladas por los laboratorios RSA[33] en cooperación con los desarrolladores de sistemas seguros de todo el mundo, con el propósito de acelerar el desarrollo de la criptografía de claves públicas. A continuación se presenta la tabla 5 con una descripción breve de éstos estándares. (**PKCS_RSA**).

[29] S/MIME: Secure/Multipurpose Internet Mail Extensions. Seguras / Extensiones de correo multipropósito para Internet.
[30] MIME: Multipurpose Internet Mail Extensions.
[31] PKCS#7: Public Key Cryptography Standard #7.
[32] PKCS: Public Key Cryptography Standard. Estándares para la criptografía de claves públicas.
[33] RSA Laboratorios: Laboratorios RSA. Disponible en internet en: http://www.rsasecurity.com/rsalabs

Estándar	Descripción
PKCS#1	Define los mecanismos para encriptar y firmar datos utilizando los sistemas criptográficos de clave pública de RSA.
PKCS#3	Define el protocolo de intercambio de claves Diffie-Hellman.
PKCS#5	Define el método para encriptar una cadena con una clave privada derivada de una frase de paso o contraseña.
PKCS#7	Define la sintaxis general para mensajes que tienen tratamientos como firmas digitales o encriptación.
PKCS#8	Describe el formato de información de una clave privada. Esta información incluye una clave privada para algunos algoritmos de clave pública y opcionalmente un conjunto de atributos.
PKCS#9	Define los tipos de atributos a utilizar en los estándares PKCS.
PKCS#10	Define la sintaxis para el intercambio de certificados.
PKCS#11	Define una interfaz de programación tecnológicamente independiente denominada Cryptoki, para dispositivos criptográficos como tarjetas inteligentes y tarjetas PCMCIA.
PKCS#12	Especifica un formato para el almacenamiento o transporte de las claves públicas, certificados o demás información confidencial de los usuarios.
PKCS#13	Define los mecanismos para encriptar y firmar datos utilizando criptografía de curvas elípticas.
PKCS#14	Está actualmente en desarrollo y se relaciona con la generación de números seudo aleatorios.
PKCS#15	Es un complemento para el PKCS#11, que proporciona un estándar para el formato de la información criptográfica almacenada en los tokens criptográficos.

Tabla 5. Estándares para la criptografía de claves públicas desarrollados por los laboratorios RSA.

4.3.3. Tecnologías de identificación y captura automática de datos

Cuando se mencionaba que entre los servicios de la PKI se encuentra la autenticación de usuarios, se hace referencia a la utilización de la clave privada del usuario para firmar documentos o realizar transacciones. Así, retomando el proceso de solicitud de un certificado digital, una autoridad de registro se encarga de comprobar la información proporcionada por el usuario para acreditar su identidad, y luego se realiza la solicitud a la autoridad de certificación para que expida el certificado digital al usuario en cuestión. Este asocia la información del usuario a una clave pública y una privada que es de su conocimiento exclusivo. Luego, cuando un usuario firma un documento con su clave privada, el mensaje queda cifrado y para descifrarlo el receptor del mensaje utiliza la clave pública del emisor. De esta manera, puede comprobar que el mensaje fue enviado por la persona a la que se le ha asociado esa clave pública. Este es el mecanismo de autenticación que ofrece la criptografía de claves públicas.

De la misma manera, en el capítulo dedicado a las TIC_S se ilustraron las diferentes tecnologías de identificación y captura automática de datos que podrían ser utilizadas en procesos de autenticación de usuarios o verificación de la autenticación de usuarios dada su utilidad en el almacenamiento de certificados digitales o claves privadas.

El objetivo de tocar nuevamente este tema en el presente subcomponente es ampliar la información relacionada con el estándar PKCS#11 desarrollado para promover el uso de la criptografía de claves públicas, su relación con dispositivos criptográficos como herramienta fundamental en los procesos de autenticación de usuarios de servicios telemáticos y las diferentes interfaces de programación que facilitan el desarrollo de aplicaciones sobre dispositivos criptográficos. Igualmente se realiza una descripción básica de los diferentes mecanismos que han integrado las tecnologías de reconocimiento biométrico con las tecnologías de transporte de datos para construir sistemas de autenticación de usuarios.

4.3.3.1. Estándar PKCS#11, dispositivos criptográficos e interfaces de programación de aplicaciones.

En el subcomponente anterior se ilustraron los diferentes estándares desarrollados por los laboratorios RSA para promover la utilización de la criptografía de claves públicas en todo tipo de aplicaciones de seguridad. En este subcomponente, se amplia el PKCS#11 que define una interfaz de programación tecnológicamente independiente denominada Cryptoki [Cryptoki], para dispositivos criptográficos.

En primer lugar, un dispositivo criptográfico es un dispositivo electrónico utilizado para almacenar información criptográfica y posiblemente para desarrollar funciones criptográficas. Este puede ser una tarjeta inteligente, un token USB, un disco inteligente, o alguna otra tecnología que incluya software únicamente o algún proceso en un servidor.

El estándar PKCS#11 especifica una interfaz de programación a nivel de aplicación (API) llamada Cryptoki, para dispositivos que almacenan información criptográfica y desarrollan alguna función criptográfica. Se aproxima a la programación orientada a objetos, sigue los objetivos de independencia de la tecnología (soporta cualquier tipo de dispositivo) y permite compartir recursos (muchas aplicaciones accediendo a muchos dispositivos), presentando a las aplicaciones una vista lógica y común de los dispositivos criptográficos. Cryptoki aísla la aplicación de los detalles del dispositivo criptográfico y la aplicación no tiene que cambiar para comunicarse con otro tipo de dispositivo o correr en un ambiente diferente, por lo tanto, la aplicación es portable.

Las tecnologías de identificación y captura automática de datos son herramientas ideales para realizar implementaciones de criptografía de clave pública, ya que pueden almacenar una llave privada o una pareja de llaves pública/privada de manera segura y bajo el control de un solo usuario. Una aplicación criptográfica programa los

dispositivos para que desarrollen operaciones, de tal forma que la información sensible, como llaves privadas, nunca abandonan el dispositivo.

Para logar que la interfaz de la aplicación sea independiente del dispositivo, Cryptoki ofrece una interfaz de bajo nivel de programación que abstrae los detalles de los dispositivos y presenta a la aplicación un modelo común del dispositivo criptográfico.

El modelo general de Cryptoki se ilustra en la figura 17. El modelo empieza con una o más aplicaciones que necesitan desarrollar ciertas aplicaciones criptográficas y termina con un dispositivo criptográfico, sobre el cual se realizan algunas o todas las operaciones criptográficas. Un usuario debe estar asociado a una aplicación.

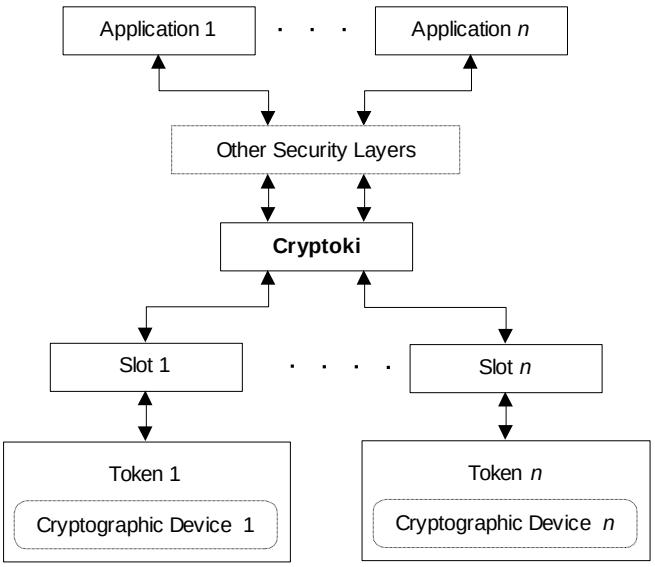


Figura 17. Modelo General de Cryptoki.

Cryptoki provee una interfaz para uno o más dispositivos criptográficos que están activos en el sistema a través de lectores (slots). Cada lector permite leer uno o varios dispositivos criptográficos. Cada dispositivo criptográfico se vé lógicamente igual a cualquier otro, independiente de la implementación tecnológica.

Otra interfaz para la construcción de aplicaciones criptográficas muy empleada es JavaCard, en esencia es una tecnología que combina el lenguaje de programación Java con el ambiente de ejecución optimizado para tarjetas inteligentes u otros dispositivos similares, tiene capacidad de procesamiento y memoria muy limitados. Su objetivo es proporcionar los beneficios de la programación en Java a los a los recursos limitados de las tarjetas inteligentes. La interfaz de programación de aplicaciones (API) de JavaCard es compatible con estándares internacionales como ISO7816, y algunos específicos de la industria para aplicaciones de comercio o banca electrónica. Las aplicaciones desarrolladas a partir del API JavaCard se denominan applets; éstas al emplear la tecnología Java son provistas de una plataforma de ejecución segura e interoperable.

4.3.3.2. Mecanismos de autenticación de usuarios utilizando dispositivos de reconocimiento biométrico y tecnologías de transporte de datos

Entre los dispositivos criptográficos, las tarjetas inteligentes han tenido un mayor desarrollo en materia de estandarización, razón por la que se ha facilitado la creación de estándares verticales relacionados con la tecnología de las tarjetas (ISO 7816 para tarjetas con contactos, ISO 10536 para tarjetas sin contactos, protocolo T=0 que define la estructura y procesamiento de los comandos enviados a la tarjeta), y horizontales relacionados con aplicaciones en que han sido empleadas las tarjetas inteligentes (técnicas de seguridad, firmas digitales, transacciones electrónicas seguras, banca electrónica)[34].

De la misma manera en que las tarjetas inteligentes han sido ampliamente utilizadas para interactuar con sistemas PKI, los token USB se están popularizando por que además de ofrecer las mismas facilidades de la tarjeta inteligente para portar y procesar (encriptar-desencriptar) información criptográfica, evitan la compra de lecto-escritores de tarjetas inteligentes para cada terminal de usuario. Como mecanismo de seguridad para proteger la información almacenada en estas tarjetas inteligentes y/o token USB, se implementa un sistema de autenticación del portador que consiste en solicitar un número de identificación personal (PIN) para acceder al certificado o claves almacenadas en él.

Por otro lado, los dispositivos de reconocimiento biométrico han empezado a tener gran aceptación pues su utilización fortalece la seguridad en las autenticaciones de usuarios y controles de acceso. La principal ventaja del reconocimiento biométrico es que la información necesaria para la autenticación es portada por cada usuario en sus propios rasgos biométricos, de manera que no hay lugar a las suplantaciones de identidad y se evitan los inconvenientes resultado de la pérdida o extravío de un dispositivo de almacenamiento electrónico de datos, o el olvido de un número de identificación personal, contraseña o frase de paso.

Obedeciendo a la necesidad de generar confianza en los usuarios de aplicaciones y servicios telemáticos, los sistemas modernos de autenticación combinan los diferentes mecanismos electrónicos de control de accesos (identificación, autenticación, verificación de autenticación y re-autenticación), empleando tecnologías de reconocimiento biométrico apoyadas por tecnologías de transporte de datos como tarjetas inteligentes o token USB.

Uno de los procesos de autenticación más tradicionales se realiza a través de la comparación de huellas digitales. (ver figura 18).

La figura ilustra un proceso en el que un dispositivo biométrico captura la imagen de huellas digitales para luego someterlas a un procesamiento digital mediante el cual se extraen las minucias que son sus puntos característicos y únicos. La distribución de las minucias es la información que permite el reconocimiento de los usuarios y es la

[34] Estándares verticales y horizontales para tarjetas inteligentes: disponible en Internet en: http://www.eurociber.es/index.php?mostrar=tarjetasinteligentes2

información que se almacena en una plantilla en las bases de datos para realizar las posteriores validaciones de identidad. Así, en el momento de la autenticación del usuario, las características de la huella capturada por el escáner son comparadas con la plantilla almacenada en la base de datos y el resultado de la comparación indica si el usuario es aceptado o rechazado por el sistema.

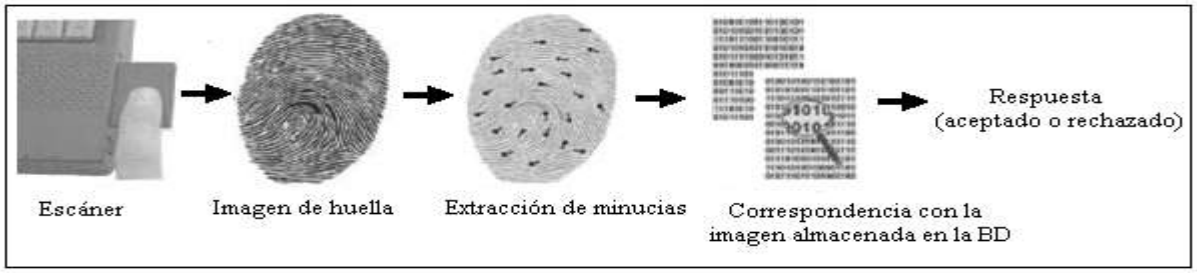


Figura 18. Proceso de autenticación de usuarios con dispositivos biométricos.

Este proceso que en sus inicios se realizaba con una base de datos centralizada, tenía muchas limitaciones en cuanto a velocidad de la respuesta de la validación y el depender de una base de datos se constituía en un limitante para la escalabilidad del sistema. Por esta razón, los sistemas de autenticación de usuarios empezaron a apoyarse en las tecnologías de transporte de datos, tarjetas inteligentes o token USB, en los que es posible almacenar información relacionada con los rasgos biométricos necesarios para realizar la validación, de manera que en lugar de acudir a la comparación por medio de una base de datos centralizada, se consulte la información almacenada en el dispositivo de almacenamiento electrónico.

En esta aplicación las tarjetas inteligentes han sido la tecnología de transporte electrónico de datos más empleada. Gracias a las capacidades de procesamiento de la tarjeta inteligente, el proceso de comparación es realizado dentro de las tarjetas inteligentes, aliviando la carga de tareas de un sistema tradicional de autenticación de usuarios y agilizando el proceso de validación. A continuación se presentan algunos sistemas que hacen uso de la biometría y de las tarjetas inteligentes para validar la autenticidad de los usuarios. [**Bechelli et al]**. Los sistemas que se describen a continuación utilizan diferentes tecnologías para comparar las huellas digitales obtenidas por un escáner biométrico con las plantillas de las huellas que se encuentran almacenadas.

- Plantilla en la tarjeta[35]: en este tipo de sistemas la plantilla con información biométrica es almacenada en un módulo hardware de seguridad (tarjeta inteligente o token USB). En este caso la plantilla tiene que ser recuperada y transmitida a un sistema diferente donde se comparan las huellas digitales capturadas por el escáner. Para ese propósito se utilizan tarjetas con memoria y aplicaciones software.

[35] En inglés: Template on Card = TOC.

- Comparación en la tarjeta[36] : agrupa aplicaciones y sistemas donde la comparación entre la plantilla biométrica y la huella digital capturada por el escáner se realiza dentro del módulo hardware de seguridad. Se consigue con el uso de tarjetas con microprocesador, provistas con un sistema operativo y una aplicación adecuada. La plantilla biométrica es almacenada de manera segura en la tarjeta.
- Sistema en la tarjeta: Esta es una evolución de las dos tecnologías explicadas anteriormente y es la mejor solución en términos de seguridad porque incluye el uso de hardware de seguridad que posee escáneres biométricos. La adquisición, el procesamiento, la selección de la plantilla y las operaciones de comparación se realizan en un solo sistema. Este tipo de tecnología utiliza tarjetas inteligentes o token USB equipados con lectores especiales de huellas digitales. Es más común el uso de sistemas basados en token USB puesto que ellos no necesitan un lector (como si lo requieren las tarjetas inteligentes).

El funcionamiento general de estos sistemas se ilustra en la figura 19 y se describe a continuación:

a. El lector de huellas digitales (escáner) detecta una huella.
b. La aplicación que se encuentra en la máquina del usuario recibe la huella digital capturada, la procesa y la envía a la tarjeta inteligente.
c. La tarjeta inteligente hace a comparación de la huella capturada con la plantilla almacenada previamente en ella y responde a la aplicación del usuario que la invocó indicando si el usuario ha sido autenticado correctamente.

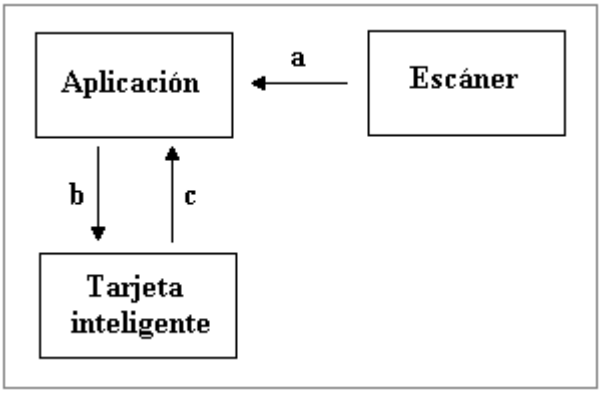


Figura 19. Descripción de los sistemas con tarjetas inteligentes y lectores biométricos.

4.3.4. Sistemas de automatización de procesos de identificación y protección de información

Este subcomponente tiene como finalidad exponer algunos sistemas alternativos que se pueden implementar para identificar y autenticar a los usuarios de aplicaciones y servicios telemáticos, y viabilizar el cumplimiento de los principios básicos de seguridad en la transmisión de información a través de redes abiertas.

[36] En inglés: Match on Card = MOC.

En la tabla 6 se ilustra un cuadro con las diferentes tecnologías que se han mencionado en el despliegue de este componente, relacionadas con los diferentes sistemas que se pueden construir para cumplir los objetivos mencionados.

TIC_S / Sistema	PKI con entidad certificadora	PGP, GnuPG, S/MIME	Reconocimiento biométrico	Transporte de datos TTD	PIN o frase de paso
Sistema 1	X			X	X
Sistema 2	X		X	X	X
Sistema 3		X			X
Sistema 4		X		X	X
Sistema 5		X	X	X	

Tabla 6. Sistemas para automatizar procesos de identificación personal y proteger la información.

A continuación se realiza una descripción de los sistemas de acuerdo con la combinación de tecnologías que utiliza:

Sistema 1: Este sistema es uno de los mayormente empleados en los ambientes de negocios electrónicos (e-business), pues por un lado, la utilización de la infraestructura de claves públicas (PKI -Public Key Infrastructure) habilita el cumplimiento de los principios básicos de seguridad en la transmisión de la información, además de facilitar la comprobación de la autenticidad de los actores involucrados en una transacción (banco, vendedor, comprador). Como un elemento que genera confianza en los usuarios se utiliza una tecnología de transporte de datos (tarjeta inteligente o token USB, más adecuados), que almacena de manera segura certificados digitales o claves privadas pertenecientes a los usuarios. Por lo general, el acceso a esta información contenida en la TTD[37], se encuentra protegida por un PIN (numero de identificación personal) o una frase de paso de conocimiento exclusivo del usuario, para que en caso de pérdida o robo, no haya lugar a suplantaciones de identidad. [Cánovas] y [Mueller] exponen sistemas de pago a través de la red que implementan algunos servicios soportados por la PKI y utilizan tarjetas inteligentes para almacenar información sensible, generando de esta manera, un ambiente de acceso seguro.

A nivel de autenticación de usuarios este sistema ofrece varias garantías: Algo que él porta (tecnología de transporte de datos - tarjeta inteligente, token USB) en donde almacena el certificado digital o la clave privada y algo que él sabe (PIN) que es de su conocimiento exclusivo y permite acceder a la información contenida en el dispositivo de almacenamiento.

Sistema 2: Este sistema se diferencia del sistema 1, en el empleo de una tecnología adicional para el reconocimiento del usuario final, en este caso es alguna tecnología de reconocimiento biométrico. Tal como se ilustraba en la sección “mecanismos de autenticación de usuarios utilizando dispositivos de reconocimiento biométrico y tecnologías de transporte de datos”, emplea alguna de las alternativas mencionadas

[37] TTD: Tecnología de transporte de datos: dispositivos electrónicos que permiten almacenar y en algunos casos, procesar información.

(plantilla en la tarjeta, comparación en la tarjeta o sistema en la tarjeta) para fortalecer el sistema de autenticación de usuarios en aplicaciones y servicios telemáticos. Este es quizás el sistema que ofrece mayor seguridad, pues la información que identifica al usuario parte de dos componentes esenciales: algo que porta (tarjeta o token USB) y algo que tiene intrínsecamente (rasgos biométricos), representando una ventaja ante los tradicionales PIN que pueden ser olvidados por el usuario. Adicionalmente, éstos sistemas han logrado integrar la PKI, para identificar las partes que componen el sistema de autenticación (tarjeta o token, escáner y la aplicación), de manera que no haya lugar a situaciones fraudulentas. Igualmente, una vez autenticado a través de la PKI se ofrecen servicios de protección de la información que él transmite a través de la red.

Este sistema ofrece además un buen rendimiento y es muy escalable pues no requiere de una base de datos centralizada para almacenar ya sean los certificados, las claves públicas o los rasgos biométricos para realizar la autenticación de la identidad del usuario. [Mueller] expone algunas características del comportamiento de un sistema donde se comparan los rasgos biométricos capturados por un lector de rasgos biométricos al instante de la verificación de identidad del usuario, con los datos almacenados en una tarjeta inteligente (plantilla en la tarjeta). En la tabla 7 se hace una comparación de algunas características propias de los rasgos de reconocimiento más utilizados: huellas digitales, el rostro, el iris y la geometría de la mano.

	Rostro	**Huella digital**	**Iris**	**Geometría de la mano**
Costo de los dispositivos	Moderado	Bajo	Alto	Moderado
Tamaño (bytes)	84-1300	250-1000	512	9
Tiempo (seg)	10	9 - 19	12	6 - 10
FRR	3.3 – 70 %	0.2 – 56 %	2 - 6 %	0 - 5 %
FAR	0.3 – 5 %	0 - 8 %	< 1 %	0 – 2 %

Tabla 7. Rasgos biométricos y propiedades básicas. [Mueller].

En la primera fila se ilustran los precios de los sensores requeridos para cada caso de reconocimiento biométrico. La segunda y tercera fila muestran el tamaño en bytes de la información de los rasgos biométricos que son almacenados en la tarjeta y el tiempo total de procesamiento. En la cuarta fila se ilustra la tasa de falsas lecturas - FRR (False Rejection Rate) - que mide el número de veces que el sistema no reconoce correctamente a una persona. Y finalmente en la quinta fila se ilustra la rata de falsos reconocimientos - FAR (False Aceptance Rate) - que mide el número de aceptaciones incorrectas del sistema. La FRR puede ser el resultado de una iluminación insuficiente, pero en la mayoría de los casos puede resolverse con un segundo intento. Mientras que la FAR es más crítica. Para reducir las aceptaciones falsas, es necesario adicionar métodos como contraseñas o números de identificación personal (PIN) que deben ser introducidos por el usuario.

Sistema 3: Este sistema hace uso de una tecnología (PGP o GnuPG) que utiliza los principios de la criptografía de claves públicas para garantizar el cumplimiento de los principios básicos de seguridad en la información transmitida, pero sin un tercero de confianza como lo es la entidad certificadora en los sistemas 1 y 2. Este sistema es ideal

para el trasporte de información sensible entre personas conocidas, como es el caso del correo electrónico. La información a transmitir es cifrada con una frase de paso que se relaciona con la clave privada del emisor, y quien recibe el mensaje debe tener almacenado en su llavero de llaves públicas, la de la persona que le envía el mensaje para poderlo descifrar. El esquema de confianza que se maneja en PGP es directo, así, un usuario almacena en su llavero privado las llaves de las personas en que confía. Como se puede observar a nivel de autenticación de la identidad del usuario, este sistema sólo cuenta con un mecanismo que consiste en algo que él sabe, en este caso es la frase de paso.

Sistema 4: Este sistema es similar al sistema 3, con la diferencia que utiliza un dispositivo criptográfico (token o tarjeta inteligente) para almacenar la palabra de paso con la cual se encripta la información que va a ser transmitida. Adicionalmente, la palabra de paso almacenada en el dispositivo criptográfico puede ser protegida con un PIN que es conocido únicamente por el usuario portador de la tarjeta. El dispositivo criptográfico agrega al sistema un nivel de seguridad importante al evitar que la frase de paso (con la que se cifra la información) sea digitada desde el teclado, desde donde podría ser capturada por un programa espía, generando un hueco a la seguridad de los sistemas PGP o GnuPG. Como mecanismos de autenticación de la identidad del usuario este sistema cuenta con algo que posee (dispositivo criptográfico -tarjeta inteligente o token) y algo que sabe, la frase de paso.

Sistema 5: Este sistema es similar al sistema 2 en lo relacionado a los mecanismos de autenticación de usuarios. Se cuenta con algo que posee (tarjeta inteligente o token), algo que sabe (frase de paso), y algo que tiene intrínsecamente (rasgos biométricos). Este sistema se diferencia del sistema 2 en el nivel de seguridad en la transmisión de información a través de la red, pues en este caso no se cuenta con un tercero de confianza que certifique a las partes que comparten una comunicación, dado que al utilizar un sistema como PGP, la relación de confianza entre las partes es directa.

4.4. Arquitectura para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos

Teniendo en cuenta los conceptos desplegados en el capítulo III y la fundamentación tecnológica ofrecida por el segundo componente del modelo "Tecnologías y sistemas para la automatización de procesos de identificación personal y protección de la información", el componente actual tiene como finalidad recoger todos los elementos teóricos desarrollados y proponer una arquitectura para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos, que ofrezca altos niveles de seguridad en la autenticación de usuarios y buena protección a la información transmitida. De esta manera, se busca que el presente Modelo sea tenido en cuenta tanto en los diseños como en las implementaciones de aplicaciones y servicios telemáticos. La figura 20 ilustra las partes constitutivas de la arquitectura propuesta.

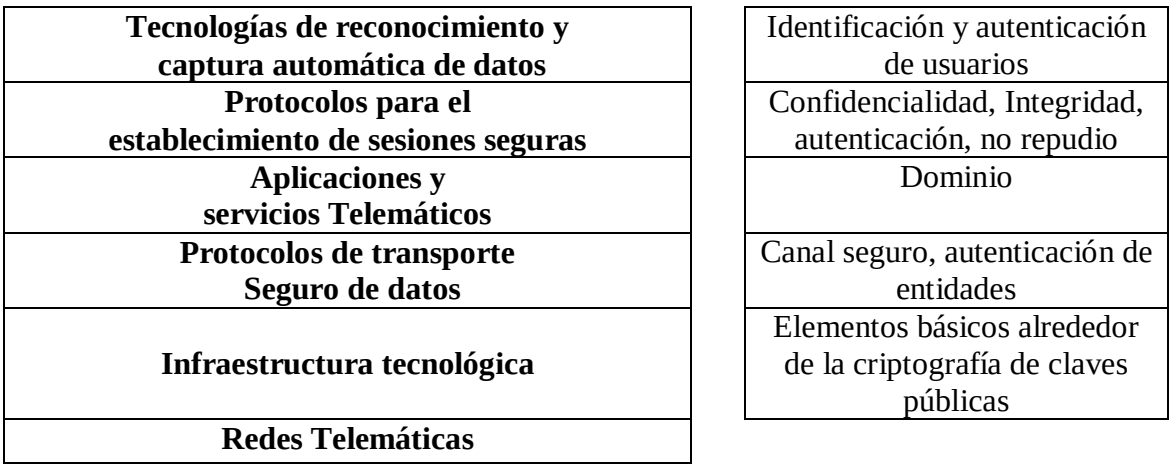


Figura 20. Arquitectura para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos.

- **Redes Telemáticas**

Tal como se ha venido tratando desde el planteamiento del problema, las redes telemáticas han dado espacio a una gran cantidad de nuevas aplicaciones y servicios a los que un usuario puede acceder a través de su computador personal y contando con una red de comunicación.

Una red telemática es un conjunto de equipos terminales y dispositivos de interconexión a través de los cuales se puede establecer una comunicación e intercambiar información. En la construcción de una red telemática intervienen esencialmente los siguientes elementos:

a. Medios de transmisión: son todos aquellos materiales que se utilizan para transportar la información, en las diferentes formas en que se hace posible, es decir, a través de señales eléctricas, de luz o electromagnéticas. Entre los medios de transmisión más utilizados se tiene el cable de cobre, el cable coaxial, el par trenzado (señales eléctricas), la fibra óptica (señales de luz) y el aire (señales electromagnéticas). En el diseño de una red telemáticas, la selección del medio de transmisión depende de los servicios y aplicaciones que se van a implementar, la velocidad de transmisión requerida, las características físicas o geográficas del lugar donde se va a instalar, el presupuesto, entre otras consideraciones.
b. Dispositivos de interconexión: son dispositivos que facilitan el intercambio de información entre diferentes equipos terminales que se conectan a una red. Son concentradores, switches, enrutadores, modems, entre otros.
c. Equipos terminales: estos se pueden clasificar en dos tipos: estaciones de trabajo y los servidores. Las estaciones de trabajo son los computadores personales que utilizan los usuarios, mientras que los servidores son equipos destinados exclusivamente a ofrecer servicios de red, ya sea en una intranet o en Internet.

- **Infraestructura tecnológica**

Como se ilustró en el capítulo dedicado a TIC_S, todos los conceptos básicos de seguridad giran alrededor de la criptografía de claves públicas que habilita el cumplimiento de los principios básicos (confidencialidad, integridad, autenticidad, no repudio) de seguridad en las comunicaciones que se realizan a través de medios abiertos como Internet. A continuación se presentan algunos elementos que resultan fundamentales a la hora de proveer una infraestructura para la prestación de estos servicios.

- **Esquema de Confianza:** en el desarrollo de este documento se ha hecho mención a dos esquemas de confianza: el que incluye una tercera parte que da fé que alguien es quien dice ser (propio de las PKI) y los esquemas directos. En cualquiera de los dos casos, debe darse la autenticación veraz de las personas o entidades a través de certificados o de llaves públicas y privadas. En un esquema de tercero de confianza la autenticación la realiza generalmente una autoridad certificadora en colaboración con una autoridad de registro, tal como sucede en la PKI. En un esquema de confianza directo, la autenticación de los usuarios la debe realizar directamente la entidad o persona interesada en utilizar el esquema. El esquema de confianza es el eje central de todo proceso de autenticación de usuarios porque de la veracidad de la información que ofrecen estos esquemas depende la validación del resto de servicios básicos de seguridad que sean habilitados (confidencialidad, integridad y no repudio).

- **Directorios de Claves Públicas y/o Certificados:** en cualquiera de los esquemas de confianza se requiere de un directorio que almacene las claves y/o certificados que pueda ser accedido en el momento de una verificación de autenticidad de la persona o entidad en cuestión. En el caso de certificados es importante contar con la lista de certificados digitales vigentes y la lista de certificado digitales revocados para facilitar la autenticación de las entidades que intervienen en la comunicación. La PKI no especifica cómo, en la práctica, deben publicarse estas listas de certificados. Existen diversas soluciones, la más recomendada es a través de un directorio LDAP[38]. Éste es un protocolo de acceso a directorios que corre sobre TCP/IP. En el caso de tecnologías con esquemas de confianza directos, se requiere de una especie de llaveros que se comportan de manera similar al directorio y son utilizados para almacenar las llaves públicas de las personas en quienes se confía.

- **Bases de datos**: a nivel de control de accesos, identificación de usuarios, control de privilegios de acuerdo a un perfil, etc; las bases de datos constituyen un elemento básico que contribuye en la gestión de todo servicio u aplicación telemática, dado que la información almacenada allí y que relaciona a un usuario, determina el nivel de interacción que puede alcanzar con el sistema telemático. Existe gran cantidad de motores de bases de datos, unos más robustos que otros,

[38] LDAP: Lightweignt Directory Access Protocol. Protocolo ligero de acceso a directorios.

que pueden ser utilizados de acuerdo a las necesidades del sistema o al presupuesto que se disponga. Existen motores de bases de datos de libre distribución como es el caso de MySQL o FireBird, y otros de utilización empresarial como ORACLE.

- **Gestión de Claves Públicas y Privadas:** es un aspecto fundamental en cualquier sistema que haga uso de la criptografía de claves públicas dado que constituyen el elemento central para el cumplimiento de los principios básicos de una comunicación segura (confidencialidad, integridad, autenticidad y no repudio). Comprende tres áreas fundamentales:
  - Generación y distribución de claves: para lograr un nivel alto de seguridad en las claves, se requiere un procedimiento de generación de claves muy bueno. Como se ha mencionado, la creación de claves públicas y privadas utiliza procedimientos matemáticos relacionados con la generación de números aleatorios. Así, las claves robustas utilizan un generador de números aleatorios de alta calidad. Las longitudes de claves mas utilizadas son las de 512, 768 y 1024 bits. Para la selección de la longitud de la clave hay que tener en cuenta el tipo de aplicación en la que se va a utilizar y las capacidades que tienen los equipos de cómputo para descifrar las claves. En la actualidad se ha descubierto que es posible romper una clave de 512 bits pero con una gran cantidad de recursos computacionales que hasta el momento no poseen la mayoría de organizaciones. Otra consideración importante a tener en cuenta en la generación de claves es quien debe realizar esta función, es decir, si debe ser el mismo usuario o una autoridad central. En muchos casos, el hecho que las claves sean generadas por los usuarios adiciona un nivel de seguridad. En otros, la generación de claves por una autoridad central brinda la ventaja de ofrecer un mejor control sobre los algoritmos utilizados. Si una organización pretende generar claves privadas a sus usuarios, necesita una manera segura de distribuir las claves a sus propietarios y alojarlas en sus computadores personales o en un una tecnología de almacenamiento de datos. Además, debe asegurar que no se realicen copias no autorizadas en el lugar donde se generen.
  - Uso, actualización y destrucción de claves: Las claves tienen un ciclo de vida limitado, por esta razón las organizaciones deben definir una política que establezca los tiempos en que los usuarios deben renovar su par de claves, al igual los mecanismos para destruir las claves antiguas en caso de renovación.
  - Almacenamiento, copia de seguridad y recuperación de claves: estos son tres aspectos muy importantes a tener en cuenta ante la posibilidad de ocurrencia de situaciones extremas, como la pérdida de las claves. Así, las copias de seguridad en un soporte seguro (tarjetas inteligentes, tokenUSB) se convierten en una herramienta importante que contribuye en su gestión.

- **Software Criptográfico:** el uso de claves públicas implica entrar en contacto con aplicaciones que ejecuten funciones criptográficas. **L**as funciones más importantes a tener en cuenta se presentan a continuación:
  - Primitivas criptográficas: estas aplicaciones proveen el acceso a funciones criptográficas de bajo nivel, como: la generación de claves, la aplicación de una

función de hashing, la encriptación y desencriptación de información con una clave privada utilizando algoritmos de claves públicas, entre otras; generalmente se utilizan localmente. Así, las funciones básicas que deben proveer las primitivas criptográficas tienen que ver con: generación de números aleatorios, generación de claves (públicas y privadas), generación de claves secretas compartidas (para criptografía simétrica), aplicación de funciones de hashing, entre otras. Es importante tener en cuenta que las interfaces de acceso a estas aplicaciones están estandarizadas para facilitar la ejecución de las implementaciones de servicios criptográficos. Algunas alternativas son: PKCS#11[39], la interfaz de programación de aplicaciones de Microsoft (CryptoAPI) y el estándar X/OPEN GCS-API.

- Servicios criptográficos: hace referencia a las funciones que habilitan estos servicios básicos de claves públicas como: la importación y exportación de claves, la derivación de claves (permite la generación de claves a partir de contraseñas o frases de paso), aceptación o refutación de claves y el control de utilización de claves. Entre las interfaces de programación de aplicaciones que se utilizan para implementar servicios criptográficos se encuentran: X/Open GCS-API, Microsoft CryptoAPI y Cryptoki.

- **Protocolos para el transporte seguro de datos**

Estos protocolos se incluyen en la arquitectura puesto que contribuyen al logro de dos propósitos fundamentales: la autenticación de las entidades que intervienen en la comunicación (cliente/servidor) y la protección de los datos transmitidos. Además, dada la característica de trabajar en los niveles de red y transporte, contribuyen al establecimiento de canales y/o sesiones seguras independientemente de la aplicación.

La información que es compartida a través de una red telemática debe ser protegida de posibles intromisiones hechas por personas ajenas al proceso de comunicación: esto se traduce en asegurar los canales de intercambio de información. En las aplicaciones y servicios telemáticos, las entidades que generalmente intervienen en un proceso de comunicación se ilustran en la figura 21.

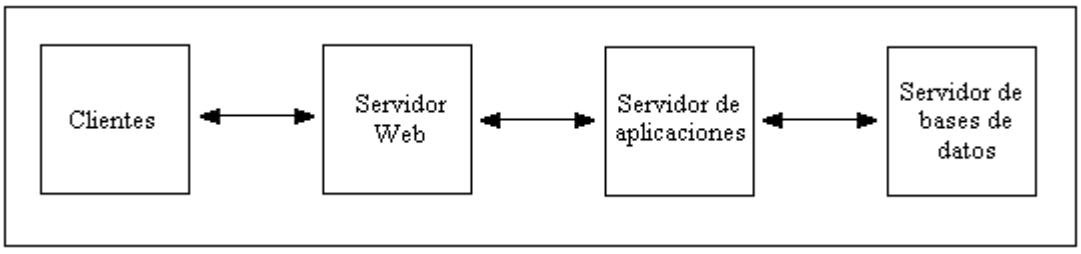


Figura 21. Entidades que intervienen en comunicaciones telemáticas.

[39] PKCS#11: Public Key Cryptography Standard #11. Estándar para la criptografía de claves públicas #11. Ver página 59.

Las flechas hacen referencia a los canales que deben ser protegidos por los protocolos de transporte seguro. Existen diversas alternativas descritas a continuación.

- **SSL (Secure Socket Layer):** tal como se ilustra en el capítulo III, el protocolo de conexión segura a través de Sockets SSL, provee un canal de conexión segura entre clientes y servidores Web que utilizan el protocolo para establecer sus sesiones. SSL utiliza funciones criptográficas complejas para cifrar y descifrar datos, por lo tanto afecta al rendimiento de la aplicación. La mayor disminución del rendimiento se produce durante el protocolo de enlace inicial en el que se realiza cifrado asimétrico, es decir, con claves públicas y privadas. Posteriormente (una vez generada e intercambiada una clave de sesión segura), se utiliza cifrado simétrico que es más rápido para cifrar los datos de la aplicación. SSL es principalmente utilizado en aplicaciones Web.
- **TLS (Transport Layer Security):** TLS es la versión del IETF[40] del protocolo SSL. Al igual que SSL, proporciona seguridad en la capa de transporte. TLS ofrece seguridad entre las partes que establecen una conexión haciendo uso de la criptografía de claves públicas y es transparente a las aplicaciones en que es implementado.
- **IPSEC (Seguridad IP):** es uno de los protocolos comunes utilizados en redes privadas virtuales. Ofrece una solución para comunicaciones seguras a nivel de red que puede utilizarse para proteger la información transmitida entre dos equipos (servidores, enrutadores) que han establecido una asociación de seguridad, esto es, que han preestablecido las claves de sesión y los mecanismos de encriptación. Entre los servicios que provee el protocolo se encuentran la privacidad, integridad, autenticidad y protección ante reenvíos para el tráfico de red en los escenarios: cliente/servidor, servidor/servidor y cliente/cliente con seguridad extremo a extremo. Por ejemplo, entre un servidor de aplicaciones y un servidor de bases de datos. Es transparente para las aplicaciones y, por lo tanto, puede utilizarse con protocolos seguros que se ejecutan sobre Internet como HTTP[41], FTP[42] y SMTP[43].

- **Aplicaciones y Servicios Telemáticos**

Todo este trabajo ha girado en torno a la seguridad en el acceso de usuarios a las aplicaciones y servicios telemáticos (autenticación) y a la protección de la información que se transmite en la utilización de estos servicios. Para contextualizar el dominio de

[40] IETF: Internet Engineering Task Force. Grupo de trabajo de ingeniería del Internet. Es una organización que desarrolla protocolos para la transferencia de información a través de Internet.
[41] HTTP: (HyperText Transfer Protocol). Protocolo de transferencia de hipertexto.
[42] FTP: (File Transfer Protocol). Protocolo de transferencia de archivos.
[43] SMTP: (Simple Mail Transfer Protocol). Protocolo de transferencia simple de mensajes.

los servicios de seguridad que se han presentado, a continuación se presentan las definiciones de aplicaciones y servicios telemáticos. [Coronado y Pino].

- **Servicios telemáticos:** son programas que corren en uno o varios computadores, generalmente de tipo servidor, y ofrecen funcionalidades que pueden ser aprovechadas por otras aplicaciones en redes de área local o de área extensa. Aunque las arquitecturas para el desarrollo de éstas aplicaciones han evolucionado desde la tradicional 2-niveles o Cliente/Servidor, a arquitecturas de n-niveles como las soportadas por J2EE o .NET, los servicios básicos continúan siendo Cliente/Servidor. Los más utilizados son el correo electrónico, la transferencia de archivos, el alojamiento de Sitios Web (Web), las salas de conversación (chats), el disco virtual, transmisión de voz, videoconferencia, entre otros.

- **Aplicaciones telemáticas:** son programas informáticos que corren en uno o varios equipos para ofrecer ciertas funcionalidades a los usuarios, se basan en los servicios disponibles en una red telemática. La acogida de los servicios Web y la universalización del navegador como interfaz para el acceso a la información, son aspectos que se deben tener en cuenta para el desarrollo de éstas aplicaciones. Entre las más utilizadas se tienen: los sistemas de información, facilitan el almacenamiento, administración, búsqueda y visualización de cualquier tipo de información; los sistemas de comunicación, constituyen interfaces que aprovechan algunos servicios básicos en Internet, como el correo electrónico, los foros electrónicos, las salas de conversación, las listas de noticias; los sistemas groupware[44], son aplicaciones para ayudar al trabajo en grupo; y los sistemas de comercio electrónico, facilitan la compra venta de bienes y servicios a través de Internet.

- **Protocolos para el establecimiento de sesiones seguras**

Estos protocolos trabajan a nivel de aplicación (Modelo OSI), son incluidos en esta arquitectura para facilitar el cumplimiento de los principios básicos de una comunicación segura: confidencialidad, integridad, autenticidad y no repudio. La selección de uno u otro protocolo para el establecimiento de sesiones seguras depende entre otras cosas, del tipo de aplicación, el esquema de confianza requerido, la portabilidad y el presupuesto. A continuación se presentan algunas alternativas:

- **S-HTTP (Secure HTTP):** es una extensión segura del protocolo HTTP, utilizado principalmente en las aplicaciones Web, pues provee un medio seguro a los clientes que se comunican con servidores Web. Se ubica en la capa de aplicación, en paralelo con HTTP y otros servicios de red (s/mime, telnet, mail, ftp). Fue diseñado para ser lo suficientemente general, proporciona soporte a un número de diferentes tecnologías de seguridad, incluyendo encriptación

[44] Groupware: hace referencia al trabajo compartido entre usuarios de una aplicación, es decir trabajo en grupo y cooperación entre usuarios.

simétrica para guardar la confidencialidad de los datos, encriptación con llaves públicas para autenticación cliente/servidor, y algoritmos de hash o message digest para proveer integridad a los datos. Estas operaciones pueden ser utilizadas en forma aislada o conjunta durante una transacción.

- **PGP o GnuPG:** Esta es una aplicación para correo electrónico utilizada para asegurar mensajes y archivos. Como se mencionó anteriormente (segundo componente), trabaja bajo el esquema de confianza directo con llaves públicas y privadas con las que puede encriptar y desencriptar la información transmitida.
- **S/MIME:** es un protocolo que provee servicios de seguridad a una amplia gama de tipos de archivos transmitidos a través de correo electrónico. Emplea un esquema de confianza donde se involucra una tercera parte, utiliza certificados digitales.
- **SET:** es un protocolo para brindar seguridad a las transacciones electrónicas, muy utilizado en aplicaciones de comercio electrónico. Se encarga de asegurar la autenticidad de los vendedores y de los clientes, además brinda protección a la información relacionada con la transacción comercial. Emplea entidades certificadoras y por lo tanto hace uso de certificados digitales. En el capítulo III se encuentra más información respecto a este protocolo.

- **Tecnologías de reconocimiento y captura automática de datos**

En el nivel superior de la arquitectura se encuentran los dispositivos de reconocimiento biométrico y las tecnologías para el almacenamiento y procesamiento de datos (tarjetas inteligentes, los token USB) ampliamente ilustradas en el capítulo de TIC_S y en el segundo componente del modelo. Estas se encargan de almacenar la información relevante para realizar los procesos de encriptación y firmado de información, como los certificados digitales y las claves privadas. Igualmente pueden almacenar plantillas con algún rasgo biométrico en los procesos de autenticación de usuarios. La importancia de estas tecnologías radica en la robustez que proporcionan a los mecanismos de control de acceso y autenticación de usuarios, redundando en la generación de una mayor confianza en los usuarios de aplicaciones y servicios telemáticos.

Finalmente, ubicando algunos protocolos, aplicaciones y/o servicios telemáticos y algunos dispositivos de identificación en su lugar correspondiente, la arquitectura para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos puede verse en la figura 22.

Dispositivos de reconocimiento biométrico	Tarjetas inteligentes	Tarjetas RFID	Token USB	
S-HTTP	**PGP**	**S/MIME**	**SET**	
Correo electrónico	Televisión por demanda	Educación virtual	Transferencia electrónica de archivos	Comercio electrónico
SSL	**TLS**	**IPSec**		
Esquema de confianza	Directorios de claves y/o certificados	Bases de datos	Gestión de claves	Software criptográfico
Redes Telemáticas				

Figura 22. Arquitectura para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos.

4.5. Consideraciones administrativas en la automatización de procesos de identificación personal

El último componente del Modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos, hace referencia a algunos elementos que se deben tener en cuenta para el correcto funcionamiento de un sistema que requiera autenticación automática de usuarios. (Figura 23).

Teniendo en cuenta que a menudo los huecos de seguridad son producidos más por errores humanos que por fallas de un sistema, los procesos de capacitación de usuarios constituyen un elemento muy importante dentro de cualquier esquema de seguridad. A continuación se enuncian y describen algunos elementos que influyen en la gestión de sistemas con algún mecanismo de identificación y autenticación de usuarios.

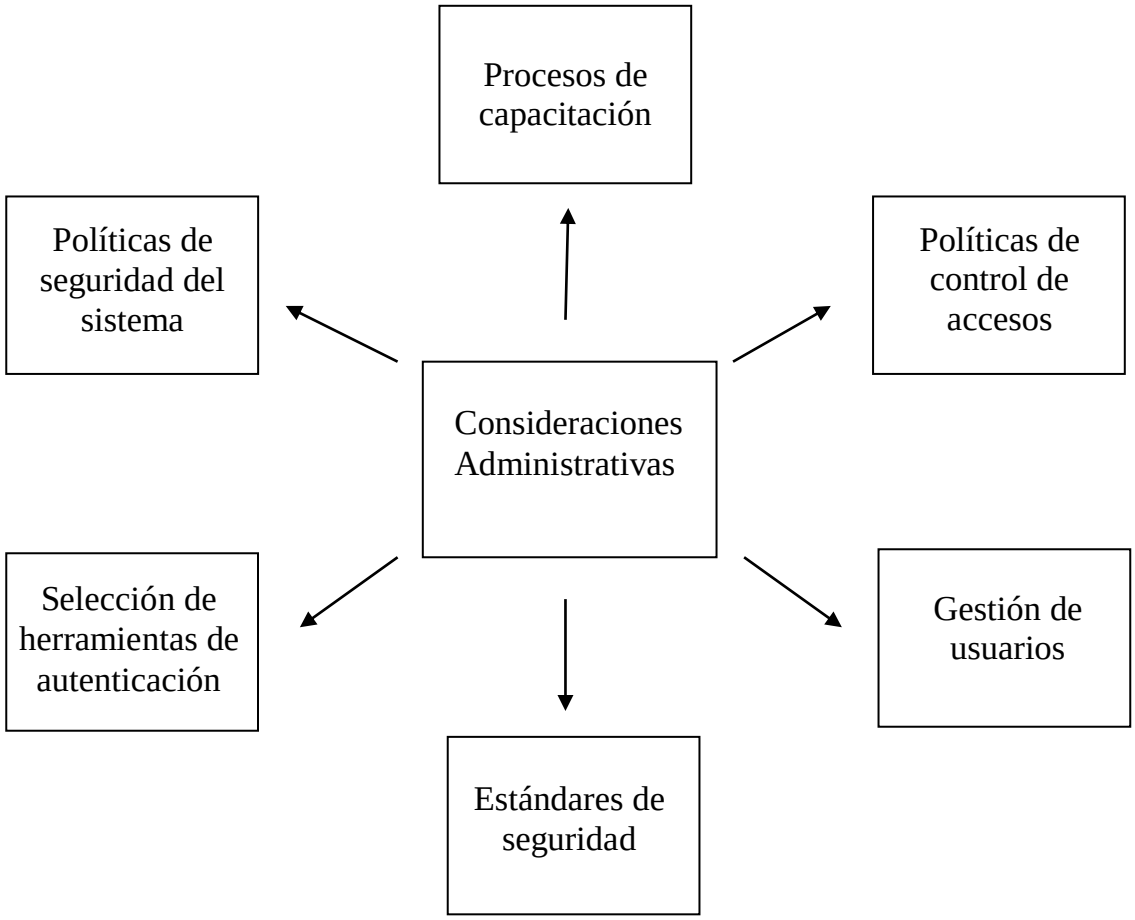


Figura 23. Consideraciones administrativas en la automatización de procesos de identificación personal.

- **Definición de Políticas de seguridad del sistema**

En términos generales, son normas materializadas en documentos que describen la forma adecuada de hacer uso de los recursos computacionales, las responsabilidades y derechos que tienen los usuarios y administradores; además las medidas de contingencia a ser adoptadas para cada inconveniente computacional y en caso de catástrofes, donde en orden de prioridad se busca salvaguardar la integridad de las personas, la integridad de la información y por último las máquinas y equipos. [**Amador et al]**.

Las políticas de seguridad no se limitan a los aspectos tecnológicos (Hw y Sw), sino que también comprende aspectos relacionados con la educación de las personas que tienen a su cargo la responsabilidad de mantener la integridad, confidencialidad, consistencia, disponibilidad, autenticación, control y auditoria de la información.

Ampliando este concepto y relacionándolo con la aplicación del modelo para la automatización de procesos de identificación personal, la educación de los usuarios es un aspecto preponderante dentro de una política de autenticación de usuarios, tal como se ampliará más adelante.

La seguridad computacional se divide en tres grandes áreas a saber: lógica, física y locativa. La primera hace referencia a todos aquellos recursos computacionales lógicos o programas (sistema operativos, programas de desarrollo, bases de datos, editores, entre otros) que intervienen en el manejo de la información, además de los procedimientos realizados en el manejo y administración de programas. La segunda tiene que ver con los mecanismos empleados para asegurar el correcto funcionamiento de los recursos físicos (servidores, enrutadores, switches, estaciones de trabajo), en tanto que la última es aquella que cubre todos los recursos de área local o de espacio físico (oficinas, centros de cómputo, bodegas, parqueaderos, etc) que pertenezcan a la entidad y que intervienen en el manejo de usuarios, datos e información.

La seguridad lógica tiene un papel importante. Los aspectos en que se centra son: disponibilidad, confidencialidad e integridad de la información, autenticación de usuarios (con influencia en la autorización de accesos y privilegios), controles de acceso automatizados y auditoria de programas (procedimientos que permitan conocer las actividades realizadas durante los accesos), cubiertos en gran parte por el modelo.

- **Definición de políticas de control de accesos**

Se orientan hacia el establecimiento de mecanismos electrónicos de control de accesos y hacia la definición del esquema que empleará un determinado sistema.

En el componente dedicado a tecnologías y sistemas para la automatización de procesos de identificación personal, que tuvo como eje central los mecanismos electrónicos de control de accesos, se hizo referencia a cuatro instrumentos básicos: la identificación, la autenticación, la verificación de autenticación y la re-autenticación. Dependiendo del nivel de seguridad requerido, se decide implementar uno u otro mecanismo, pero independientemente del mecanismo y las tecnologías asociadas, se debe buscar el cumplimiento de tres condiciones que permitan identificar y autenticar plenamente al usuario en un acceso a una aplicación servicio telemático, estas son:

- Algo que el usuario conozca: puede ser una clave secreta, una contraseña, o una frase de paso, todas de conocimiento exclusivo por el usuario.
- Algo que el usuario porte: puede tratarse de un dispositivo de almacenamiento electrónico de información como una tarjeta inteligente, una tarjeta RFID o un token USB, debe ser de manejo exclusivo del usuario.
- Algo que el usuario posea intrínsecamente: esto es una característica biométrica que pueda ser comparada y verificada en el momento del acceso.

En la medida en que se combinen estas condiciones como requisitos para acceder a una aplicación o servicio telemático, se fortalece la seguridad en el control de acceso.

Acerca de la definición del esquema de control de accesos que se debe implementar en un sistema, debe estar acorde con las necesidades de seguridad del sistema. Así, si se trata de un ambiente Web, la autenticación de usuarios es el proceso a través del cual un servidor Web verifica la identidad del cliente que solicita un servicio. Por ejemplo, en el

servicio de correo electrónico el mecanismo de autenticación más utilizado hasta ahora es un identificador del usuario y una palabra clave. Pero tal como se ha ilustrado, actualmente se pueden emplear otros mecanismos que ofrecen mayores niveles de seguridad. En todo caso, en el proceso de autenticación de usuarios el servidor debe contar con una base de datos donde se encuentren registrados los usuarios legítimos del sistema, con la información que los identifique y su perfil.

Un aspecto importante acerca de la lista de control de accesos es la sección de contraseñas o claves privadas. Estas palabras clave deben protegerse a través de algoritmos de encriptación antes de ser almacenadas en el servidor. A pesar de que este no es un mecanismo de protección fuerte, representa la protección mínima que se debe proporcionar a la información de autenticación.

En las autenticaciones vía Web, el usuario accede a una página Web donde puede explorar servicios, bienes, o información de su interés. Así cuando aquello que busca el usuario es de acceso sólo para personas autorizadas o que cumplan con algunas condiciones (p.e. crédito, débito), el servidor presenta un panel de autenticación donde el usuario debe registrar los datos que lo identifican ante el sistema. Posteriormente el usuario llena los campos de autenticación y los envía al servidor. Allí, ésta información es comparada con la información almacenada en la lista de control de accesos. En el caso simple de requerir únicamente nombre de usuario y contraseña, estos datos son comparados con los almacenados en la lista de control de accesos del servidor y en caso de que coincidan, el usuario queda autenticado y el servidor le permite concluir la petición al usuario. Este proceso es ilustrado en la figura 24.

Este esquema utilizado como ejemplo emplea una base de datos centralizada que es consultada por el servidor en todos los accesos que se pretendan realizar. Hoy día existen otros esquemas como son, los de autenticación con la combinación de biométricos, tarjeta inteligente y hasta número personal de identificación; no es necesaria una base de datos centralizada pues estos tres mecanismos se apoyan mutuamente, agilizando el proceso de identificación automático. En estos últimos esquemas se necesitan elementos hardware conectados a la estación de trabajo desde donde acceden los clientes.

- **Gestión de los usuarios**

Es fundamental dentro del control de accesos. Esta función puede asimilarse a la que realiza la autoridad de registro de una organización de certificación. Esta tarea distingue cuatro áreas básicas a saber: registro de usuarios, gestión de privilegios, gestión de información sensible y revisión de los derechos de los usuarios.

El registro de usuarios asocia el procedimiento mediante el cual se valida su identidad ante el sistema y es adicionado a la lista de usuarios. La gestión de privilegios comprende la asignación de permisos de acceso a ciertos servicios, aplicaciones o información de carácter restringido para quienes no han gestionado ningún proceso de autorización. La gestión de información sensible tiene que ver con el mantenimiento de

contraseñas, frases de paso, claves públicas y privadas, que permiten autenticar al usuario a través de los mecanismos de control de acceso. Finalmente la revisión de los derechos de los usuarios es un procedimiento que se realiza durante intervalos periódicos de tiempo y tiene que ver con la verificación de los privilegios que posee.

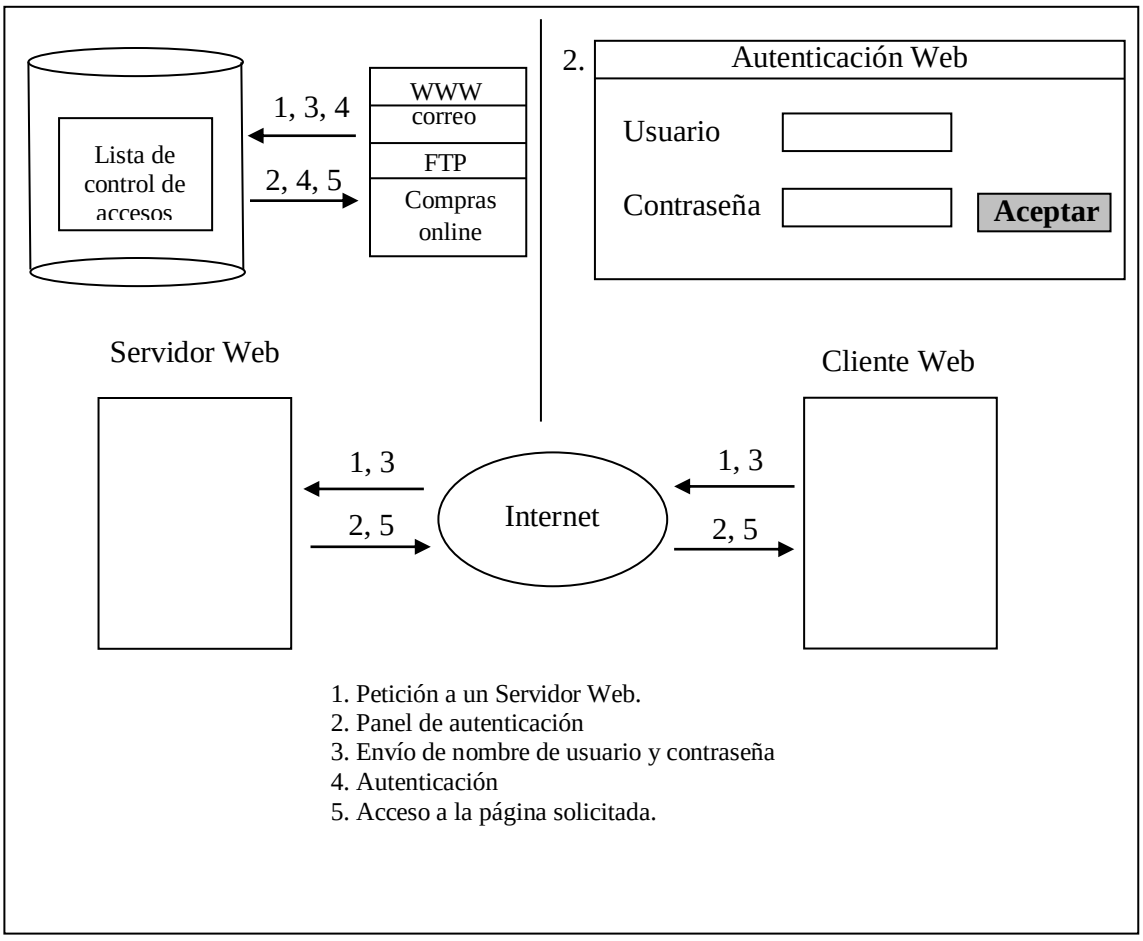


Figura 24. Autenticación básica de usuarios vía Web.

- **Selección de herramientas de autenticación**

Entre las herramientas de autenticación, hay que tener en cuenta las tecnologías de reconocimiento biométrico y las tecnologías de almacenamiento de información tales como las tarjetas inteligentes, las tarjetas RFID y los token USB. Igualmente, dependiendo de las necesidades de protección de la información transmitida, es necesario considerar las herramientas de encriptación con manejo de claves públicas y privadas.

La selección de tecnologías empleadas debe obedecer a una evaluación de las características de rendimiento y seguridad que requiera el sistema.

- **Procesos de capacitación de usuarios**

Los diferentes mecanismos que controlan accesos son diseñados partiendo de la premisa que las claves privadas, las contraseñas y los dispositivos electrónicos de almacenamiento de datos corresponden al uso exclusivo por parte del respectivo usuario. De lo contrario los mismos usuarios constituirían un hueco de seguridad en los esquemas de autenticación. Por esta razón, es necesaria la generación de procesos educativos alrededor básicamente de tres temas:

- Los principios básicos de una comunicación segura (confidencialidad, integridad, autenticación y no repudio) y cómo funcionan. Igualmente se requiere brindar una capacitación básica acerca de la criptografía de claves públicas y el manejo de las claves pública y privada.
- El funcionamiento de las tecnologías de identificación y almacenamiento electrónico de datos, utilizadas como soporte de la información que identifica y autentica al usuario ante un sistema.
- La importancia y responsabilidad que deben tener los usuarios con respecto a la información que debe ser de su conocimiento exclusivo (contraseñas, frases de paso); y al porte y uso personal de las tecnologías de almacenamiento electrónico de datos.

- **Estándares de seguridad**

En toda organización que haga uso de las tecnologías de la información se recomienda implementar buenas prácticas de seguridad, de manera que sea garantizada en los sistemas y la información manejada. Es así como se encuentra el estándar ISO 17799 que es una norma internacional de alto nivel para la administración de la seguridad de la información. Fue publicado en diciembre del año 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. Se orienta a preservar la confidencialidad, integridad y disponibilidad de la información. La aplicación del marco de referencia proporcionado por él proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información. Las diez áreas de seguridad que abarca el estándar son [**ISO_17799**]:

- **Políticas de seguridad:** define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

- **Seguridad organizacional:** establece el marco formal que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

- **Clasificación y control de activos:** el análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de

clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.
- **Seguridad del personal:** proporciona controles a las acciones del personal que opera con los activos de información. El objetivo de esta área es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer responsabilidades por parte del personal en materia de seguridad de la información.
- **Seguridad física y de entorno:** identifica los perímetros de seguridad de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.
- **Comunicaciones y administración de operaciones:** integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, abarcan desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.
- **Control de acceso:** habilita los mecanismos que permitan monitorear el acceso a los activos de información; incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.
- **Desarrollo de sistemas y mantenimiento:** la organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para sus tareas específicas.
- **Continuidad de las operaciones de la organización:** el sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias. Estos deben ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.
- **Requisitos legales:** son los requerimientos que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

La aplicación de un estándar de seguridad proporciona un marco ordenado de trabajo en el cual deben incluirse todos los miembros de una organización. Aunque no elimina el cien por ciento de los problemas de seguridad, ayuda a establecer una valoración de los riesgos a los que se enfrenta una organización en materia de seguridad de la información. Dicha valoración les permite administrar los riesgos en función de los recursos tecnológicos y humanos con los que cuenta, además establece un entorno que identifica los problemas en tiempos razonables, garantizando que se pueden detectar las violaciones a la seguridad de la información.

5. CAPITULO V. DESCRIPCION, DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO DE VALIDACION

Para validar el modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos se decidió realizar un prototipo de ventas a través de Internet. A través de esta aplicación es posible aplicar la mayoría de conceptos incluidos en el marco teórico proporcionado por el capítulo dedicado a las tecnologías de información y comunicación asociadas a la seguridad, al igual que permite plasmar los componentes tecnológicos del modelo. A continuación se realiza una descripción del prototipo y se presentan su diseño e implementación.

5.1. Descripción del prototipo

El prototipo de validación es una aplicación que permite la compra-venta de bienes por medio de transacciones electrónicas realizadas a través de Internet. Se hace la simulación de un sistema de pagos con débito electrónico (e-cash), para lo cual se crea una entidad bancaria que debe ser consultada para autorizar los pagos. Los otros actores del sistema son básicamente el vendedor y el comprador. El primero tiene un sitio Web a través del cual publica los bienes que tiene en venta, y el segundo accede a la tienda virtual a través de su navegador. El prototipo permite identificar plenamente al comprador en el momento en que se realiza la petición de autorización de compra al banco. Igualmente, permite verificar la autenticidad de los sitios Web de las entidades de negocio (vendedores y banco). La información que viaja a través del medio de transmisión va cifrada de tal forma que se puede conservar la confidencialidad de los datos sensibles. (figura 25)

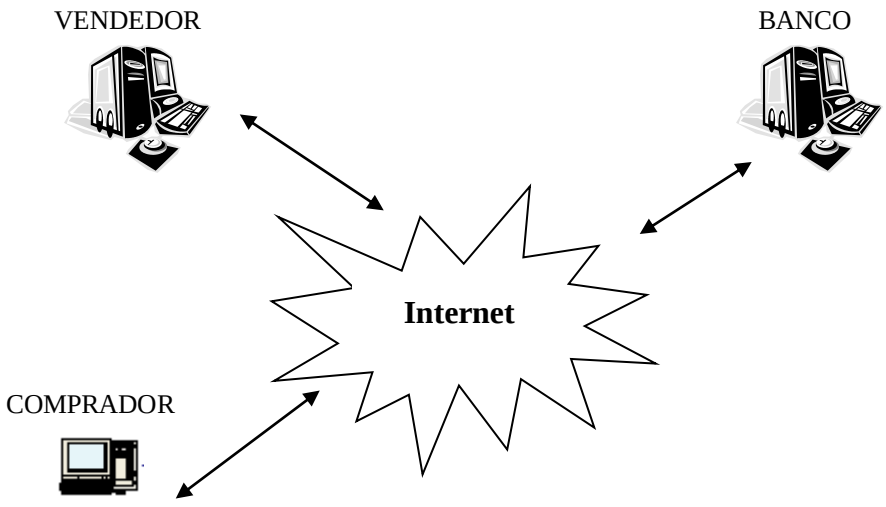


Figura 25. Descripción básica de entidades del prototipo.

Para cumplir con los dos requisitos puntuales que son: la autenticación de las entidades involucradas y la seguridad en la información que es transmitida a través de la Web, se procede como se describe a continuación.

Identificación del banco: Al tratarse de una entidad que recibe información sensible de los usuarios, para autenticarlo y autorizarle la compra de bienes o servicios, y que va a ser accesible vía Web, es necesario que el sitio tenga un certificado emitido por una autoridad competente.

Identificación del vendedor: es una entidad a la que los usuarios acceden para realizar compras de bienes o servicios a través de un sitio Web. Es importante que los sitios Web de los vendedores tengan un certificado digital para que a la hora de comunicarse con el banco, éste los pueda reconocer como una entidad válida.

Identificación de usuarios: dado que los usuarios pueden acceder a un sitio Web de un vendedor desde cualquier parte y pueden adquirir bienes o servicios a través de su estación de trabajo conectada a Internet, es necesario que se identifiquen plenamente ante el banco que va a autorizar la compra. Previamente, los usuarios deben registrarse en el banco para que sean registrados en la base de datos y les sea asignada una etiqueta RFID donde se almacena una parte de la información requerida en el proceso de autenticación. Esta información es: una frase de paso (conocida únicamente por el usuario) y almacenados en la tarjeta RFID, un identificador único y una clave privada.

El proceso de compra-venta de bienes y servicios implementado requiere del cumplimiento de dos condiciones: la autenticación del usuario (comprador) y la autorización de la compra. Así, antes de realizar la compra, el usuario debe autenticarse ante el banco. Para lograrlo, abre la aplicación que se encuentra en su máquina, sigue las instrucciones que se le indican e ingresa la información requerida (cédula y frase privada). La aplicación recoge ésta información y además (con el lector RFID) lee la información almacenada en la tarjeta RFID.

Protección de la información sensible: para el caso de compra de productos en línea, la información sensible abarca la orden de compra (que podría ser capturada por entidades interesadas en conocer perfiles de consumo), datos personales del comprador (nombre, dirección, teléfono) utilizados para realizar la entrega de los pedidos, número de la cuenta bancaria, claves personales, frases privadas, etc. Para proteger este tipo de información, se utiliza el protocolo SSL.

Para cumplir con los objetivos de autenticación de entidades, se cuenta con los siguientes dos elementos:

Entidad certificadora: comprueba por medios tradicionales (documentación legal), la autenticidad de las entidades involucradas y expide certificados digitales. Se implementó una entidad certificadora cerrada, con fines académicos, utilizando herramientas y librerías de seguridad del proyecto Open SSL.

Servicios de GnuPG: Se requiere de una aplicación que permita utilizar las funcionalidades criptográficas de GnuPG, para cifrado y descifrado de información a partir de la utilización de claves públicas y privadas.

5.2. Diseño del prototipo

El prototipo de validación es una aplicación Web a través de la cual se puede realizar compra venta de bienes y servicios, haciendo la validación y ejecución de pagos con una entidad bancaria. En la tabla 8 presentada a continuación, se describen los elementos fundamentales de la aplicación:

Arquitectura a cuatro capas	Implementación
El prototipo posee una arquitectura de cuatro capas. Esto quiere decir que existen 4 niveles de componentes o sistemas que se detallan a continuación: - Interfaz o capa cliente. Se encarga de la presentación y captura de la información de pedidos y autenticación de usuarios, además de contener ciertas reglas de validación de datos. La autenticación por medio del dispositivo RFID se realiza a través de un sw residente en el cliente. - Capa Web. Hacen parte los sitios Web a los que acceden los usuarios. Son accedidos desde los navegadores. - Capa de negocio. Es la encargada de gestionar la información que hace parte de la transferencia electrónica. Siempre se ejecutan en el servidor, y son requeridas por el nivel anterior. También establecen el nexo de comunicación con el siguiente nivel. - Capa de Datos. Gestiona el acceso a datos o a las bases de Datos. Se encarga de almacenar y recuperar los datos. Nunca es accedido por los clientes, y sólo establece comunicación con el servidor o servidores de aplicaciones	La arquitectura de cuatro capas en el prototipo está implementada de la siguiente forma: El nivel Cliente lo forman los navegadores con mayor uso a nivel mundial, es decir, el Internet Explorer o Netscape Comunicator. Igualmente, al nivel de cliente se encuentra el Sw residente en las estaciones de trabajo desde donde acceden los compradores para hacer su autenticación ante el banco. Las reglas de negocio, residen en los servidores del vendedor (compra-venta de bienes y servicios) y del banco (autenticación de usuarios y autorización de pagos), están desarrolladas en Java. Las Bases de Datos, se encuentran en los servidores, se implementaron con MySql (Banco) y FireBird(Tienda-vendedor).

Reglas del negocio	Implementación
Las reglas del negocio se ejecutan en los servidores, éstos se encargan de manejar las transacciones. Para ello establecen enlaces de comunicación tanto con las interfaces de la aplicación, como con los sistemas de acceso a datos. Así mismo, también se relacionan con el resto de los sistemas que componen el prototipo.	Se han desarrollado en Java, necesitando una máquina virtual de Java en su versión 1.4 o superior, y se encargan de gestionar las relaciones con la Base de Datos y las interfaces gráficas. Además, marcan toda la política de validaciones y procesos de la aplicación. Los componentes de Java (cliente, web, de negocio, datos), incorporan desarrollos en JSP, servlets, JavaBeans, entre otros.
Bases de datos	**Implementación**
Son relacionales. Todos los componentes y piezas de código del sistema utilizan sentencias SQL estándar, por lo que es la pieza del sistema con menor resistencia al cambio. Puede implementarse con cualquier base de datos relacional, los únicos requisitos son la existencia de un driver Java para el acceso a los datos.	Es una base de Datos Relacional, en el caso del prototipo es MySql, de tipo software libre.
Funcionalidades y flujo de tareas	**Implementación**
En el prototipo existen unas funcionalidades claras y un flujo de tareas que se encargan de marcar el camino por el que se mueve la información de un cliente. Dichas funcionalidades y flujo de tareas están ligadas con el prototipo a través de API's Java, las cuales deben permitir que las diferentes tareas se ejecuten a través de interfaces y se relacionen con el modelo de datos del prototipo.	El flujo de Tareas, se ha implementado con un conjunto de API's java que facilitan cada una de las funcionalidades del prototipo.
Servidor Web ó servidor de aplicaciones	**Implementación**
El prototipo utiliza un servidor de aplicaciones. Existe un repositorio de componentes (reglas de negocio) que se encuentran en un servidor y que permite que las interfaces clientes "hablen" con dichos componentes.	Se ha utilizado como servidor Web Apache Tomcat, brinda soporte a los desarrollo con JSP y Servlets, y el servidor de aplicaciones JBoss. Las anteriores herramientas también son de tipo software libre, disminuyendo aun más costos de desarrollo.
Seguridad	**Implementación**

La seguridad en el prototipo, está basada en algunas de las TIC_S descritas en el marco teórico. Estas son: - Entidad Certificadora - Software criptográfico (GnuPG) - Tecnologías de transporte electrónico de datos. - Implementación de SSL para el establecimiento de un canal seguro.	La capa de seguridad, que contempla las funciones de firma digital, encriptación, verificación de firmas, no repudio, etc. se ha implementado bajo las especificaciones del modelo para la automatización de procesos de identificación personal en aplicaciones y servicios telemáticos. La autenticación de usuarios tiene soporte de una herramienta hardware (RFID). La información sensible enviada a través del medio de transmisión es protegida con SSL.

Tabla 8. Elementos fundamentales de la aplicación.

La arquitectura en cuatro capas fue escogida por las ventajas que se describen a continuación:

- **Independencia Lógica y Física:** las reglas de negocio (capa de negocio) se implementan de forma independiente al almacenamiento físico de la información (capa de datos).
- **Múltiples interfaces de usuario:** al estar implementadas de forma independiente la interfaz de usuario y las reglas de negocio, es posible crear diferentes interfaces sin necesidad de modificar dichas reglas de negocio.
- **Fácil mantenimiento:** aa existencia de las cuatro capas permite la fácil modificación de cualquiera de ellas. Es sencillo modificar la interfaz gráfica, puesto que reside en una sola capa y no afecta a las reglas de negocio. Del mismo modo se puede modificar cualquier servicio de la capa de negocio sin necesidad de modificar la interfaz que lo utiliza y el almacenamiento físico de los datos que implica. Por último, en la capa de datos (Bases de datos), se pueden reorganizar o redistribuir los datos sin afectar al cliente que los utiliza.
- **Escalabilidad y procesamiento distribuido:** si el número de clientes aumenta, y por tanto sus peticiones a procesar, será posible establecer nuevos recursos en las capas intermedias que cubran dichas peticiones.
- **Seguridad del proceso de negocio**: las capas intermedias permiten establecer un control sobre las transacciones que se realizan, permitiendo optimizar la utilización de los recursos y recuperarse ante posibles errores.

A continuación se despliega la arquitectura final adoptada para implementar una aplicación Web que permite automatizar procesos de identificación personal (compradores ante los bancos) y proteger la información que es transmitida a través de Internet. Ver figura 26.

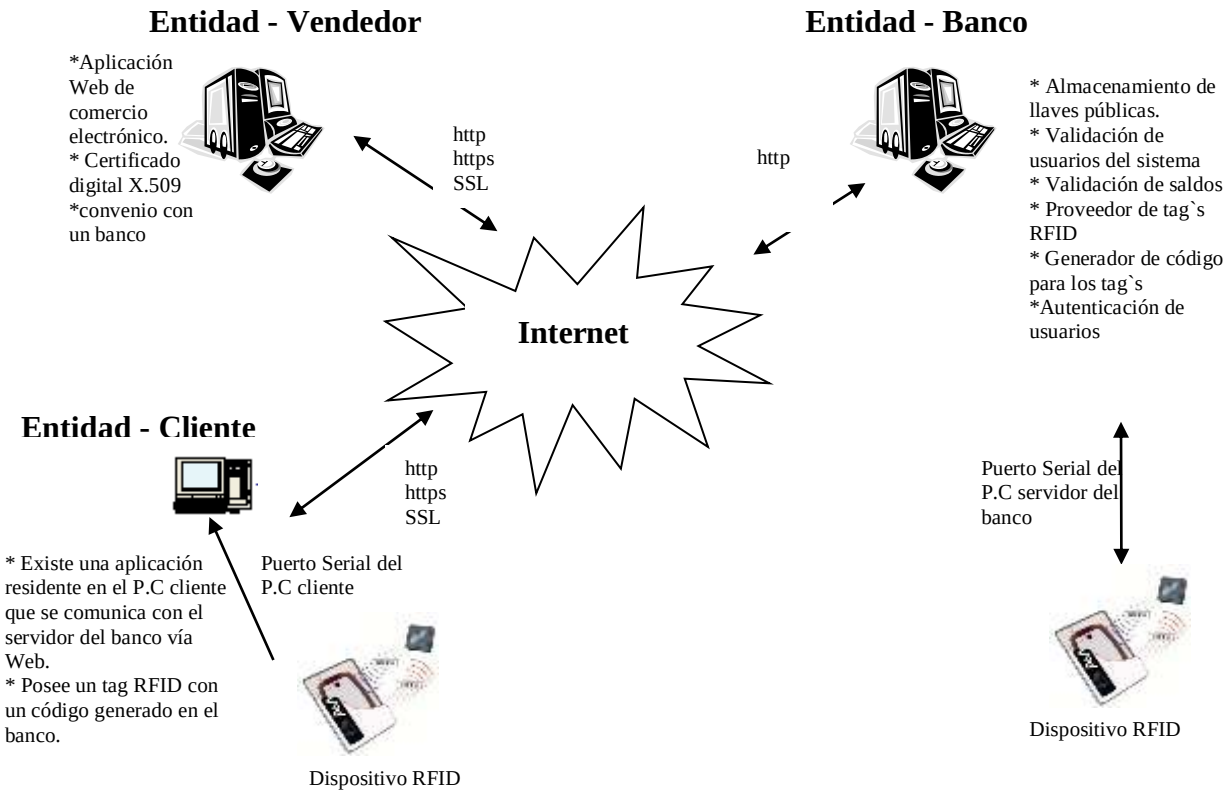


Figura 26. Arquitectura final del prototipo de validación.

- **Descripción de los elementos de la arquitectura:**

Entidad Vendedor: esta entidad reúne todas aquellas empresas que ofrecen venta de bienes o servicios. Para el caso específico del prototipo se trata de una empresa que tiene un sitio Web a través del cual implementa una tienda virtual para vender productos (equipos de cómputo y accesorios). Los clientes acceden a las tiendas virtuales haciendo uso de su navegador. Una vez allí pueden adicionar los productos que deseen adquirir en un carrito de compras que va calculando el valor total de la venta hasta que pasa al proceso de pago. El vendedor posee un certificado digital que permite realizar su autenticación con las otras entidades implicadas en el prototipo. Adicionalmente, el vendedor tiene un convenio con una Entidad Banco, que facilita el pago de los productos a los compradores que tienen cuenta en dicha entidad bancaria. Así, en el momento del pago, la entidad vendedor se comunica con la entidad banco para solicitar la autorización de la compra.

Entidad Cliente: es cualquier persona que accede a un sitio Web desde un Vendedor por medio de su navegador. El cliente realiza el proceso de selección de productos para la compra y debe cumplir con la autenticación ante el banco para que en caso que tenga el saldo suficiente, su compra sea autorizada. Así, en la máquina desde donde se conecta el cliente, se encuentra instalado un dispositivo hardware (lector RFID) que a través de

una aplicación que se ejecuta en la estación de trabajo, permite leer el dispositivo de almacenamiento electrónico de datos (etiqueta RFID) que lo identifica como suscriptor de la entidad bancaria que tiene convenio con el vendedor.

La autenticación del usuario se realiza cumpliendo con dos instrumentos de control: algo que el usuario sabe (frase privada) y algo que el usuario porta. La etiqueta RFID es aquello que el usuario debe portar y almacena la información de dos condiciones de autenticación (identificador único y clave). En el proceso automático de autenticación, la aplicación del usuario envía la información de autenticación al banco a través de la invocación del servicio Web de autenticación.

La autorización de la compra es solicitada por el cliente utilizando al vendedor como pasarela en el momento en que se realiza la confirmación de la compra y se procede a pagar. Así, invoca el servicio Web de autorización del Banco y le envía el número de cédula, el NIT del vendedor y el valor de la compra. Si el cliente (comprador) se encuentra autenticado, el banco procede a verificar su saldo, en caso que tenga suficiente, autoriza la compra. Este proceso se ilustra en la figura 27.

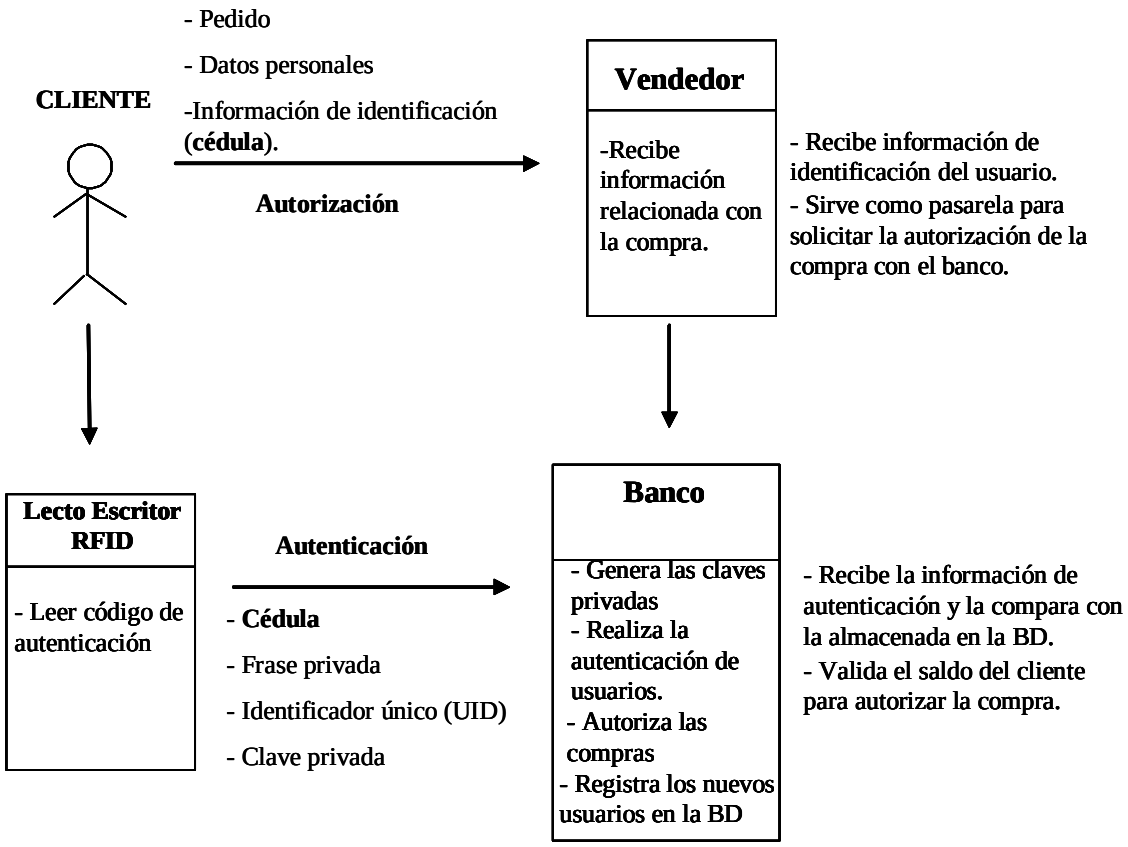


Figura 27. Proceso de identificación automática de usuarios.

Entidad Banco: es la entidad que realiza el registro de usuarios en la BD y ejerce todo el control sobre la autenticación de usuarios vía Web y la autorización de compras.

Dentro del registro de usuarios, el banco se encargada de verificar por medios tradicionales la identidad del cliente y posteriormente lo registra en la base de datos. De esta manera, el banco implementa un tipo de autoridad de registro. Dentro de la información del usuario, la más importante es la utilizada con fines de autenticación, consiste en tres datos:

- Frase Privada: es almacenada en la BD después de aplicarle un algoritmo de hashing a una frase que sea fácilmente recordada por el usuario.
- Identificador único: son 8 números que trae cada una de las etiquetas RFID. Este es asignado a cada etiqueta en el proceso de fabricación. Es único y no se puede alterar.
- Clave: es generada por el banco combinando funciones de hashing con herramientas de cifrado GnuPG. Después de la generación esta clave es almacenada en la tarjeta RFID en unas posiciones de memoria preestablecidas. Esta clave luego es bloqueada para que no se pueda modificar.

Posteriormente el banco entrega al usuario la etiqueta RFID (donde se encuentran consignados el identificador único y la clave), el lecto-escritor RFID y la aplicación que debe instalar en la estación de trabajo para autenticarse ante el banco.

Los servicios de autenticación de usuarios y autorización de compras se implementan como servicios Web [Web Services], de manera que son accesibles desde cualquier lugar por medio de una conexión a Internet. Estos servicios corren sobre el Servidor de aplicaciones JBoss [JBoss] que esta configurado para soportar el servicio SSL.

La autenticación de usuarios se realiza a partir de la información que envía el cliente cuando invoca el servicio, comparándola con la información almacenada en la BD. Deben cumplirse las tres condiciones (identificador único, clave y frase privada) para autenticarlo correctamente. Después de la autenticación, el cliente cuenta con un tiempo entre 20 y 40 segundos para realizar la solicitud de autorización de la compra. Si transcurrido este tiempo no lo ha hecho, el banco desautentica al usuario, teniendo que autenticarse nuevamente.

La autorización de la compra se invoca desde la tienda virtual en el momento de realizar el pago. Cuando se invoca este servicio, se envía la identificación del cliente (cédula), el valor de la compra, y el número que identifica al vendedor (NIT). El banco recibe esta información y procede a validar si el cliente tiene saldo suficiente, en caso afirmativo, autoriza la compra, hace el desembolso del valor en el saldo del cliente y lo adiciona al saldo del vendedor.

El Banco posee un certificado digital X.509 para su autenticación ante las demás entidades involucradas en la arquitectura del prototipo, este certificado digital ha sido entregado por una entidad certificadora. La seguridad en los medios de transmisión está a cargo del protocolo SSL.

- **Procedimiento para realizar la compra de bienes o servicios**

Un procedimiento de compra se puede definir a grandes rasgos como un proceso en el que un consumidor se interesa por adquirir un bien o servicio y procede a intercambiarlo por dinero en efectivo.

En esta aplicación los productos se encuentran exhibidos a en un sitio Web, (entidad vendedor), a través del cual, el usuario puede consultar en catálogos electrónicos las características de los productos, incluyendo el precio, e ir añadiendo los productos deseados a un carrito de compras. Como no existe una interacción física entre el cliente y el vendedor, y por lo tanto no se puede realizar directamente el intercambio de bienes y servicios por dinero efectivo, debe existir un mecanismo automático de pago para que el vendedor proceda a hacer la entrega del bien o servicio adquirido. En los casos en donde aquello que se adquiere no se puede obtener vía electrónica, es necesario que el vendedor provea un servicio de distribución de los productos físicos (se supone que el vendedor cumple con las entregas).

El mecanismo de pago se implementa realizando la conexión con un banco al que se encuentran afiliados tanto el vendedor como el comprador y manejan una cuenta de ahorros o corriente. El comprador debe manejar débito. El control sobre el pago lo realiza la entidad banco, comprobando en primera instancia que el cliente se haya autenticado correctamente y luego que éste cuente con saldo suficiente. En este caso, sustrae el valor de la compra del saldo del cliente y lo adiciona al saldo del vendedor.

Para poder realizar este proceso de pago se deben cumplir las siguientes condiciones iniciales:

- El cliente debe tener una cuenta de ahorros en el Banco.
- El vendedor debe tener una cuenta de ahorros o corriente en el banco.
- El banco debe haber incluido en su base de datos al cliente y al vendedor, previa comprobación de su identidad bajo mecanismos tradicionales.

Con el objetivo de ilustrar claramente el proceso de compras con autenticación de compradores, en la tabla que se presenta a continuación (tabla 9), se presenta un diagrama de secuencia con los casos positivos.

CLIENTE	VENDEDOR	BANCO
1. Accede a un sitio Web de una entidad vendedor. **2.** Revisa el catalogo de productos y selecciona los que desea comprar. **3.** Selecciona la opción de pago. →	**4.** Presenta un formulario que el cliente debe llenar	

	con información personal y datos a cerca del pago.	
5. Llena el formulario. 6. Envía la información de autenticación al banco. (cedula, identificador único, clave y frase privada)		
		7. Compara la información de autenticación recibida con la almacenada en la BD. Si estos datos coinciden coloca el estado de autenticación del usuario en 1.
8. Selecciona la opción de "solicitar autorización". Con la que envía al banco información de identificación y datos relacionados con la transacción. (cédula, valor de la compra, NIT del vendedor).		
		9. Valida el saldo del cliente, y modifica los saldos del cliente y el vendedor. **9.** Autoriza la compra, notificándoselo al vendedor.
	10. Realiza la entrega del bien o servicio adquirido por el cliente.	

Tabla 9. Procedimiento de compra-venta de bienes o servicios vía Web.

5.3. Implementación del prototipo

Para la implementación del prototipo se seleccionó un conjunto de herramientas y tecnologías basadas en software de libre distribución y de código abierto. A continuación se describe cada uno de ellos.

5.3.1. Servidor Web Apache Tomcat

El servidor Web que se instaló para la publicación del sitio de comercio electrónico es Apache Tomcat 4, compatible con las especificaciones de Java: Servlet y JavaServer Pages. Apache Tomcat se desarrolló dentro del proyecto Jakarta, el cual es gratuito y está disponible en http://jakarta.apache.org.
Para la instalación de Apache Tomcat se utilizó una computadora Athlon XP, con sistema operativo Windows 2000 Profesional. Previamente a la instalación del servidor Web se instaló el entorno de programación de Java JDK 1.4 (Java Development Kit) mediante el cual los servlets, las clases y los JavaServer Pages son compilados. Para la configuración del servidor Web se modificó el archivo server.xml. Las características específicas que se modificaron son el puerto de atención de solicitudes y el redireccionamiento de peticiones que utiliza el protocolo de seguridad SSL.

5.3.2. Sistema Administrador de Bases de Datos Mysql

Es un sistema administrador de bases de datos relacionales. La instalación de MySQL se realizó en la misma computadora en la que se instaló el servidor Web. Para la configuración y monitoreo del manejador de bases de datos se instaló WinMySQLadmin ver. 1.4 para Windows.
Las características que se configuraron principalmente fueron las de control de acceso remoto a la base de datos y creación de usuarios.

Las características principales de MySQL, de utilidad para la implementación del prototipo son las siguientes:
a) Velocidad y robustez,
b) Código abierto,
c) Altamente portable,
d) Ofrece todo un conjunto de APIs para C, C++, Eiffel, Java, Perl, PHP, Phyton, Ruby.
f) Soporta multihilos.
g) Provee de un sistema de contraseñas y privilegios flexible y seguro.

5.3.3. APIs De Java

- Servlets. Son programas escritos en lenguaje Java que se ejecutan en un servidor Web. Actúan como una capa intermedia entre una petición proveniente de un navegador Web u otro cliente http. Entre las características que ofrecen los servlets, fueron de utilidad para el desarrollo del prototipo las siguientes:

a) Cuentan con una extensa infraestructura para analizar y decodificar automáticamente los datos de los formularios HTML, administrar las cookies, rastrear las sesiones y muchas otras utilidades.
b) Los servlets pueden comunicarse directamente con el servidor Web. También pueden mantener información de una petición a otra, lo que simplifica las técnicas como el rastreo de sesiones.
c) Son transportables, ya que los servlets están escritos en el lenguaje de programación Java, por lo tanto, pueden utilizarse de manera directa o como complementos en virtualmente cualquier servidor Web.
d) Son económicos. Hay disponibles diversos servidores Web gratuitos o muy económicos. No obstante, con la excepción de Apache, que es gratuito, la mayoría de los servidores Web de calidad comercial son relativamente costosos. Sin embargo, una vez que se cuenta con un servidor Web, sin importar su costo, la adición de características para los servlets cuesta muy poco.

- Java Server Pages (JSP). La tecnología de las Java Server Pages permite mezclar HTML estático con contenido dinámicamente generado a partir de los servlets. JSP no proporciona facultad alguna que en principio no pueda realizarse con un servlet. De hecho, los documentos JSP son automáticamente traducidos a servlets. Sin embargo, es más fácil escribir y modificar el código HTML que tener una gran cantidad de instrucciones println que lo generen.

- JDBC. Es una API que proporciona Java para ejecutar instrucciones SQL. Consiste en una serie de clases e interfaces escritas en Java, para el desarrollo de aplicaciones que acceden a bases de datos de forma homogénea. En otras palabras, con la API JDBC no es necesario escribir un programa para acceder a Sybase, otro programa para acceder a Oracle, y otro programa para acceder a MySQL; con esta API se puede crear un solo programa que sea capaz de enviar instrucciones SQL a la base de datos apropiada.
La aplicación de Java debe tener acceso a un controlador (driver) JDBC adecuado. Este controlador es el que implementa la funcionalidad de todas las clases de acceso de datos y proporciona la comunicación entre el API JDBC y la base de datos real. Los distribuidores de bases de datos suministran los controladores que implementan el API JDBC. De esta forma JDBC proporciona una interfaz de alto nivel que evita el tener que trabajar con detalles de bajo nivel para acceder a bases de datos. En el caso del manejador de bases de datos MySQL, Conector/J es el driver JDBC oficial.

- JavaMail. El API JavaMail es un paquete opcional (extensión estándar) para leer, redactar, y enviar mensajes electrónicos. Su propósito principal no es transportar, enviar, o re-enviar mensajes como sendmail u otros programas de este tipo. En otras palabras, los usuarios interactúan con los programas para leer y escribir e-mails. El API JavaMail está diseñado para proporcionar acceso independiente del protocolo para enviar y recibir mensajes.

5.3.4. Aspectos de Seguridad

En el servidor Web se configuró y habilitó el direccionamiento de las peticiones tipo https (que utilizan el protocolo SSL) para comunicar datos de manera encriptada y segura entre el navegador y las aplicaciones del servidor. Las funciones del prototipo para las cuales se utilizó el protocolo de seguridad SSL son las siguientes:

a) La transmisión de los datos de facturación y envío del formulario de registro y de detalles de compra a la aplicación del servidor del vendedor.
b) La transmisión de los datos del tag de RFID a la aplicación bancaria.
c) La autentificación del cliente a través de su frase de paso y otros datos.

6. CAPITULO VI. CONCLUSIONES Y TRABAJOS FUTUROS

A partir del desarrollo del presente trabajo de grado, surgieron las siguientes conclusiones:

- A través de la combinación de tecnologías de identificación personal, captura automática de datos y aplicaciones de la criptografía es posible automatizar un proceso de identificación personal a través de la red.

- El modelo ofrece una gran cantidad de herramientas y posibilidades de implementación que siendo asimiladas correctamente brindan pautas suficientes para automatizar procesos de identificación de usuarios.

- En los ambientes telemáticos, cada vez se hace más necesario el fortalecimiento de los mecanismos de acceso a la información y los servicios. La misma dinámica del mercado que ha intentado personalizar a los clientes hace que resulte muy útil la implementación de mecanismos de identificación de usuarios con ayuda de herramientas de Hw y SW, de tal forma que se elimine o se reduzca sustancialmente la suplantación de identidades a través de la red.

- Los procesos de capacitación son una parte fundamental para el éxito de los procesos de autenticación de usuarios. La carencia de conocimientos por parte de los usuarios en este aspecto puede generar huecos a la seguridad de los sistemas con procesos automáticos de identificación.

- La utilización de dispositivos de reconocimiento biométrico es muy deseable en la automatización de procesos de identificación personal.

- La selección de herramientas HW y SW dependen de las características de los ambientes donde se requiera implementar un proceso de autenticación de personas.

- Dentro de la validación del Modelo para la Automatización de Procesos de Identificación Personal en Aplicaciones y Servicios Telemáticos se logró construir un prototipo funcional que evidenció muchos de los tópicos descritos en el modelo, como por ejemplo, el uso de tecnologías de información y comunicación asociadas a la seguridad, protocolos de seguridad y tecnologías de identificación personal.

- El prototipo desarrollado, dentro del marco de las transacciones comerciales, fue el de una tienda virtual, enfatizando en el módulo de pagos y de autenticación de clientes, en el que se hizo uso de herramientas de software libre, con lo que se muestra que es factible desarrollar aplicaciones y servicios telemáticos de nivel empresarial a bajo costo, haciendo posible que las pequeñas y medianas empresas puedan acceder al mercado del comercio electrónico global de Internet.

- Se comprobó, de manera particular a través del prototipo de validación, la gran utilidad que tienen herramientas de seguridad como OpenSSL para el establecimiento de conexiones seguras a través de Internet.

El tema de la autenticación de usuarios a través de Internet asociado las tecnologías de identificación y almacenamiento electrónico de datos y a la criptografía de claves públicas abre las puertas a muchos proyectos interesantes como pueden ser:

- Asociar los patrones de huellas digitales a la generación de claves públicas y privadas. Actualmente estas claves se generan a partir de frases de paso conocidas por los correspondientes usuarios. En algunos casos, como PGP, los documentos se cifran con la frase de paso asociada a la clave privada, así que es cuestión de recordar la frase. El problema deviene en caso de olvido. Igualmente, cuando las claves privadas son guardadas en dispositivos de almacenamiento electrónico (tokens o tarjetas), es posible que éstos se extravíen, lo que en caso de no tener un respaldo, el usuario no podría volver a utilizarla para cifrar su información, viéndose obligado a solicitar otro par de claves pública y privada. La idea de utilizar huellas digitales para generar estas claves evitaría estos inconvenientes, dado que el usuario siempre portaría la clave privada consigo mismo en sus rasgos biométricos.

- En aplicaciones de educación virtual sería muy adecuada la autenticación de los estudiantes mediante dispositivos biométricos para evitar las suplantaciones. Igualmente, un mecanismo de re-autenticación sería muy útil para que la aplicación pudiera comprobar a intervalos de tiempo determinados, que el estudiante se encuentra presenta al frente de la aplicación educativa.

- A partir de los principios de las comunicaciones seguras (integridad, autenticidad, confidencialidad y no repudio), sería interesante la construcción de una herramienta didáctica que permitiera a los usuarios comprobar por si mismos el funcionamiento de estos principios. Esto tendría un impacto importante en la capacitación que requieren los usuarios para hacer uso de las herramientas de seguridad informática disponibles para el cuidado de la información.

7. CAPÍTULO VII. BIBLIOGRAFIA

[Amador et al]. Amador, Siler**; Carrascal,** Carolina; **Agredo,** Guefry**.** Políticas de Seguridad Computacional. Universidad del Cauca. Abril 2002. Disponible en Internet en: http://www.criptored.upm.es/guiateoria/gt_m124c.htm

[Auto ID Center]. La nueva red. Identifique automáticamente cualquier objeto, esté donde esté. Disponible en Internet en: http://www.codigo.org.ar/Descargas/EPC.pdf

[Becerra], Martín. Sociedad de la información: proyecto, convergencia, divergencia. Enciclopedia Latinoamericana de Sociocultura y Comunicación. Bogotá. Editorial Norma. 2003.

[Bechelli et al], Bechelli, Luca ; **Bistarelli**, Stefano y **Vaccarelli**, Anna. Biometrics with SmartCard. Instituto de Informática y telemática. Italia. 2002.

[Bella], Giampaolo. Biometrics to enhance SmartCard Security. University of Cambridge. Disponible en Internet en: http://www.sci.unich.it/~bista/papers/papers-download/mocviatocfinal.pdf

[Cánovas], Oscar. PISCIS: Comercio Electrónico basado en Infraestructuras de Certificación Avanzadas y Sistemas de Tarjeta Inteligente. Universidad de Murcia. 2002. Disponible en Internet en: http://ditec.um.es/~ocanovas/papers/piscis.pdf

[Cardenas], Manuel José. La nueva economía del conocimiento. Bogotá D.C. Ediciones Jurídicas Gustavo Ibáñez. 2001.

[Certicamara]. Entidad certificadora abierta en Colombia. Sitio Web: http://www.certicamara.com.co.

[Chaparro], Rolando. Alternativa de Infraestructura de clave pública basada en el uso de DNSSEC. Disponible en internet en: http://www.cnc.una.py/invest/paper2/chaCLEI.pdf

[CORBA]. Descripción de la especificación en:
http://www.corba.org, http://www.omg.org/corba/cichpter.html

[Coronado y Pino]. **Coronado**, Juan Manuel y **Pino**, Ulises. Modelo de Conectividad para redes humanas. Universidad del Cauca. Popayán. 2004.

[COYUNTURA]. Telecomunicaciones en Colombia. Revista Economía Colombiana y Coyuntura Política, publicada por la Contraloría General de la República. Bogotá D.C. Edición N. 288. Febrero-Marzo de 2002.

[Cracking DES]: presentación del libro que presenta la vulnerabilidad de DES. Disponible en internet en: http://www.eff.org//Privacy/Crypto/Crypto_misc/DESCracker/

[Cryptoki]. (PKCS#11) Adaptation Layer. CDSA (Common Data Security Architecture). 2000. Disponible en internet en: http://cvs.sourceforge.net/viewcvs.py/cdsa/cdsa_doc/cal_dev_guide.pdf?rev=1.2

[ECONOMIA]. Colombia en la Sociedad de la Información: cinco dimensiones de la gestión municipal. Revista Economía Colombiana, publicada por la Contraloría General de la República. Bogotá D.C. Edición N. 301. Marzo de 2004.

[FusionConsulting], RFID: The future of contactless payment in Asia. 2005. Disponible en internet en: www.fusionc.com

[**Geo_mano**], the biometric Consortium. Disponible en: http://www.biometrics.org/html/examples/hand_and_finger.html

[Ghosh], Anup K. Jhon Wiley & Sons. E-Commerce Security: weak links, best defenses. USA, 1998. p. 113-104 y 114-118.

[GnuPG]. El GNU Privacy Guard. Disponible en internet en: http://www.gnupg.org/

[Grarfinkel], Simson. Web Security & Commerce. Estados Unidos. O´REILLY. Junio 1997.

[Huidrobo], Jose Manuel. RFID. Etiquetas inteligentes. Disponible en Internet en: http://www.coit.es/publicac/publbit/bit146/quees.pdf

[Internacional Biometric Club], el sistema de clasificación de Henry. Disponible en Internet: http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf

[IPSec]. Protocolo de Seguridad en Internet. RFC 2401. Disponible en Internet en: http://www.faqs.org/rfcs/rfc2401.html

[ISO_17799]. International Organization for Standardization. Disponible en internet en: http://www.iso.org

[JBoss], Servidor de aplicaciones Jboss. Disponible en: http://www.jboss.com/products/jbossas

[JCP], Java Community Process, Comunidad de procesos Java, información disponible en: http://java.sun.com/developer/technicalArticles/jcp/

[Johner], Heinz. Deploying a Public Key Infrastructure. IBM. International Technical support Organization. 2000.

[Johner], Heinz. Deploying a Public Key Infraestructure. IBM. International technical support organization. 2000. Disponible en internet en: http://securitytechnet.com/resource/security/pki/sg245512.pdf

[J2EE]. Detalles de la especificación y descargas disponibles en: http://java.sun.com/j2ee/index.jsp

[Ley 527 de 1999]. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Internet en: http://www.ocyt.org.co/leg/Ley%20527.pdf

[Mueller]. **Mueller**, Wolfgang. Javacard-enabled Smart Cards for collaborative engineering enviroments. Universidad de Paderborn.2003. Disponible en Internet en: http://www.c-lab.de/~wolfgang/cce03b.pdf

[PGP]. Curso introductoria a PGP. Disponible en internet en: http://www.rediris.es/pgp/doc/intro-pgp.es.html

[PKCS_RSA] Labs. ¿Que son los estándares de clave pública (PKCS)? Disponible en Internet en: http://www.rsasecurity.com/rsalabs/pkcs/

[Rajput], Wasim. E-commerce Systems, Architecture and Applications. Artech House. 2000.

[RFC 1321]: Message Digest Algorithm MD5. Disponible en Internet en: http://www.faqs.org/rfcs/rfc1321.html

[RSA_labs]: Algoritmos de Encriptación. Disponible en Internet en: http://www.rsasecurity.com/rsalabs/node.asp?id=2247

[Reynolds], George. RFID: un acercamiento práctico. Factores críticos de éxito en implementaciones RFID. 2004. Disponible en Internet en:

[SISTEMAS_79]. Economía Digital: estrategias disponibles. Revista Sistemas, publicada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS).Bogotá D.C. Colombia. Edición N.79 Mayo-Junio 2001.

[SISTEMAS_85]. Panorámica de la seguridad informática en Colombia. Revista Sistemas, publicada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C. Colombia. Edición N.85 Junio-Julio 2003.

[SISTEMAS_89]. Seguridad informática: Colombia en la mira; IV Encuesta Nacional, tendencias 2002-2004. Revista Sistemas, publicada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS). Bogotá D.C. Colombia. Edición N.89 Mayo-Agosto 2004.

[S/MIME]. Que es S/MIME. Disponible en internet en: http://www.rsasecurity.com/rsalabs/node.asp?id=2292

[Toselli], Alejandro Héctor. Reconocimiento de texto manuscrito continúo. Tesis Doctoral.Universidad Politécnica de Valencia.2004.

[**Web Services**], Tutorial de Servicios Web de Java. Disponible en: http://java.sun.com/webservices/docs/1.0/tutorial/

[.NET]. Características y descargas disponibles en:
http://www.microsoft.com/spanish/msdn/arquitectura/default.asp