UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA

MAESTRÍA Y DOCTORADO EN CIENCIAS E INGENIERÍA

"DISEÑO DE UN SISTEMA PARA EL ALMACENAMIENTO Y RECUPERACIÓN DE EXPEDIENTES CURRICULARES ELECTRÓNICOS UTILIZANDO TARJETAS INTELIGENTES"

TESIS

QUE PARA OBTENER EL GRADO DE
Maestro en Ciencias

PRESENTA
Julio César Castillo Ramírez

DIRECTOR
M.C. Jorge Eduardo Ibarra Esquer

CODIRECTOR
M.C. Brenda Leticia Flores Ríos

Mexicali, Baja California, Mayo de 2007

Agradecimientos

A Dios
Por darme la vida y permitirme estar rodeado de gente maravillosa. Gracias por todos los mensajes y los milagros que veo a diario.

A mis padres
Por traerme al mundo en un ambiente lleno de amor incondicional. Son las personas que más admiro y pido a Dios poder llegar a formar una familia como ustedes lo han hecho.

A mi sobrina: Frida Alejandra
Por ser mi alegría, el renacimiento del amor en mi familia y porque a pesar de mis ocupaciones, siempre tienes esa invitación para estar conmigo y jugar.

A mis hermanos: Félix y Oscar
Por todo lo que hemos vivido juntos y por ser la mejor compañía en este camino de vida. Gracias por estar conmigo en todo momento.

A mis abuelos, tíos y primos
Por todo el cariño y apoyo que caracterizan a esta hermosa familia.

A mis cuñadas: Alejandra y Claudia
Por formar parte de esta familia y estar al pendiente de nosotros en cada momento.

A mi compañera de trabajo y amiga: Lupita Figueroa
Por reconocer mi potencial, motivarme y convencerme para estudiar esta maestría. Gracias a ti logré este gran paso en mi vida.

A mi novia: Alejandra Cárdenas
Por todo tu cariño, consejos, paciencia y comprensión. Gracias por todo lo que reconoces en mí y porque a pesar de la distancia física, me has acompañado en esto.

A todos mis amigos:
Por estar en los mejores momentos y hacer que los malos se pasen rápido. En especial a Luis, Edgar, Fer, Ticho, Rubén E., Rubén L., Adrián, César, Pedro, Ricardo y Paco. Fueron muchas las veces que falté a las reuniones por estar dedicándome a lograr este objetivo, pero siempre siguen conmigo. Gracias por no borrarme de la lista y seguir siendo esos verdaderos amigos.

Al Dr. Gabriel López
Por su enseñanza y sobre todo por los valiosos consejos que me brindó cuando sentí que dejaba este objetivo.

A la Dra. Larisa Burtseva
Por compartir su gran conocimiento, por la asesoría brindada y sus valiosos consejos.

A la M.C. Conchita Mendoza Díaz
Por sus valiosa colaboración en la revision del documento de tesis, lo cual fue de gran ayuda para completar este trabajo.

A mis maestros: Rafael Villa, Martín Olguín y Marcela Rodríguez:
Por compartir su conocimiento y por la buena disposición de llevarnos por este camino.

A mis varios compañeros: Victor, Silvia, Miguel, Samuel, Julia, Mónica, Ulises, Alejandro, Ricardo, Angélica, Luz María, Leonel y Rainier.
Porque aprendimos cosas juntos y compartimos experiencias. Sé que cada uno va tomando diferentes caminos por esta vida. Les deseo mucha suerte.

A todos los compañeros que participaron en el Grupo de Investigación en Tarjetas Inteligentes (GRINTAIN). Por ese gran apoyo para que este proyecto se llevara a cabo.

Y muy en especial, para mis directores de tesis: Brenda Flores y Jorge Ibarra. Quienes pusieron su confianza en mí para formar parte de este proyecto. Por compartir su conocimiento valioso, por sus consejos, por la paciencia que me tuvieron y por ir caminando siempre a mi lado para realizar este trabajo. Sin ustedes no hubiera podido lograrlo.

Muchas gracias a todos. Mil bendiciones.

Índice

Lista de Figuras

Lista de Tablas

Capítulo I. Introducción

Actualmente, la educación superior es una entidad flexible, en donde los programas de estudio, metodologías y estructuras se han puesto al servicio de la sociedad como elemento clave de integración al mundo globalizado (Erlwein, 2003). Una vez que una persona cumple con los requisitos establecidos en un plan de estudios de una carrera en cierta institución, se le entrega un comprobante de estudios, el cual hace constar que esa persona cursó debidamente las asignaturas requeridas y, por lo tanto, posee conocimientos en cierta área específica y, además, cuenta con cierto grado de seriedad, compromiso y habilidades que, en conjunto, le permiten desempeñarse de manera adecuada dentro del ámbito que le compete.

Sin embargo, no todas las personas que desean obtener un grado académico en una institución educativa, optan por cumplir con todos los requisitos establecidos para adquirir tal comprobante de estudios. Para solventar su necesidad, algunas personas recurren a técnicas de falsificación de comprobantes de estudios, entre los que se incluyen títulos, diplomas y reconocimientos, para lograr pertenecer a un status o campo laboral donde se requiere demostrar habilidades y conocimientos del área a desempeñar. Tal acción se lleva a cabo debido a varios factores, entre ellos, el escaso recurso económico de la persona para solventar el pago de los estudios, el bajo nivel de aprovechamiento de la misma para cursar las asignaturas o la necesidad de resolver en corto plazo, la problemática de no contar con los estudios requeridos que exige el rol que quiere desempeñar en el campo laboral. La falta de ética por parte de la persona interesada en los comprobantes de estudios y por parte de las personas participantes en la falsificación de los mismos, aunado a la disponibilidad actual de mecanismos y tecnologías para su elaboración, ha dado pie al surgimiento de las llamadas “Fábricas de Diplomas” (García de Fanelli, 2002), un problema que actualmente ha sido difícil de atacar.

Motivado por la problemática que ha surgido debido a la falsificación de comprobantes de estudios, se presenta una alternativa de validación de la autenticidad de los mismos, por medio de un sistema que utiliza una tecnología que ha demostrado ser muy segura en cuanto al manejo y transporte de información sensible, ya que actualmente se utiliza en distintos tipos de aplicaciones que varían desde transacciones financieras, hasta el control de acceso físico y de información en instituciones gubernamentales de varios países. Tal tecnología mencionada es la de tarjetas inteligentes, la cual consta de dispositivos que tienen las mismas dimensiones físicas que las tarjetas de crédito convencionales y que se les ha incrustado un circuito integrado (chip) con capacidades que van desde el almacenamiento de información, hasta el procesamiento de la misma para brindar seguridad, portabilidad, facilidad de uso y confiabilidad (Cardlogix, 2004; Jurgensen & Guthery, 2002).

En este trabajo se propone el diseño de un sistema que permite almacenar y recuperar expedientes curriculares electrónicos en forma segura y eficiente, utilizando la tecnología de tarjetas inteligentes. El resultado esperado es que el sistema propuesto sirva de base para que en un futuro cercano se desarrolle una arquitectura que permita dar certeza a la sociedad de que, quienes se ostenten como profesionistas cumplen con la formación académica necesaria y los requisitos legales para ejercer una profesión. De la misma forma, brindar la certeza sobre el capital humano con que cuenta nuestra sociedad y lograr así, un mejoramiento en nuestra capacidad productiva.

1.1 Definición del problema

La evolución constante de las tecnologías de la información (TI) ha permitido que, en la actualidad, se cuente con herramientas especializadas para la gestión de documentación electrónica. Sin embargo, esta misma evolución de las TI ha facilitado la reciente proliferación de un fenómeno sociocultural y académico al que se le denomina “Fábrica de Diplomas” (García de Fanelli, 2002), el cual afecta la calidad de los procesos que

dependen de la formación académica de quien los realiza y, consecuentemente, el crecimiento económico, cultural y de valores de las organizaciones y de la sociedad.

Cuando una persona va a solicitar empleo o quiere continuar sus estudios en alguna institución educativa, debe presentar documentos que comprueben que tiene los estudios o experiencia laboral requeridos. La forma más común de verificación de la validez de estos comprobantes es por medio de la inspección visual de los mismos, por parte de la persona que les da trámite. Esto ha facilitado a los falsificadores recurrir a nuevas técnicas para falsificar los documentos, cumpliendo cada vez más con las nuevas exigencias en las características que determinan si el documento es válido. En algunos casos, como parte de una verificación más segura, se contacta a las instituciones o empresas que expiden los documentos probatorios para comprobar si la información contenida en ellos es válida. Este proceso resulta sencillo para los casos en que se validan documentos que provienen de empresas e instituciones que son conocidas por la entidad que está realizando la verificación, ya que generalmente se tienen los datos de contacto de los departamentos responsables de expedir tales documentos. Sin embargo, el proceso se vuelve complicado conforme se requiere validar documentos probatorios de instituciones y empresas que no son conocidas por la entidad en cuestión. Además, no se cuenta con un mecanismo seguro para validar en forma inmediata si las instituciones educativas y empresas se encuentran registradas legalmente con los organismos correspondientes. Debido a lo anterior, el proceso para determinar la validez de documentos probatorios requiere de tiempo, herramientas de comunicación y otros factores que, aunados a la cantidad de documentos por verificar, incrementan la complejidad del mismo.

En México existe la cédula profesional, la cual es una credencial que sirve para dar certeza que una persona cumple con la formación académica necesaria y ha cumplido con los requisitos legales para ejercer una profesión, ya sea de nivel licenciatura, maestría, doctorado, nivel técnico o nivel técnico superior. Para solicitarla, la Secretaría de Profesiones valida todos los documentos probatorios requeridos incluyendo, para el caso de licenciatura, los certificados de estudios de secundaria, bachillerato y profesional, así

como el acta de examen profesional y título profesional. El trámite de una cédula para nivel licenciatura tiene un costo de $712 pesos mexicanos y contiene catorce mecanismos de seguridad para que no se pueda falsificar. Entre estos mecanismos se encuentran el uso de tinta ultravioleta, impresión en grabado láser con foto y firma, fondo de seguridad e impresión de cambio de color. Sin embargo, se han dado reportes sobre la falsificación de cédulas profesionales de este tipo, por lo que se inició un plan para aumentar la seguridad de éstas que consiste en incrustarles un circuito integrado o chip (Notimex, 2004).

La implementación del chip en la cédula profesional hará mucho más difícil su falsificación y podrá ser un medio seguro para que una persona demuestre que puede desempeñarse en el ámbito profesional. Sin embargo, este documento solamente muestra el grado de estudios de la persona sin mencionar más detalle sobre la misma y por lo tanto, tiene la desventaja de que no puede ser utilizada como documento probatorio de otros estudios como diplomados, cursos, publicaciones, ni de experiencia laboral.

Por otro lado, algunas instituciones educativas almacenan información de la trayectoria académica de sus alumnos en formato digital. Este proceso consiste en obtener una imagen digital del documento probatorio para posteriormente almacenarlo e incluirlo en el historial académico del alumno en caso de ser requerida su consulta. Esto les brinda la ventaja de tener un mejor control de los documentos, así como contar con acceso rápido a los mismos para cuestiones internas de la institución. Sin embargo, este método no constituye una estrategia adecuada para la consulta de datos específicos contenidos en los documentos, por no contarse con un estándar para el almacenamiento y presentación de los expedientes curriculares. Además, sus expedientes no pueden ser consultados desde otras instituciones o empresas que requieran validar comprobantes de estudios de una persona. Lo anterior, en términos del problema que aquí se plantea, no proporciona ventajas adicionales a las propias del almacenamiento físico de la información.

Existe la necesidad de resolver los graves inconvenientes asociados a la gestión tradicional de los expedientes curriculares en papel, tales como la realización de procesos repetitivos, la falta de control, la acumulación o pérdida de expedientes, dificultad para

transportarlos y sobre todo la vulnerabilidad a su alteración y falsificación. Tales demandas, propias del área de la educación y del sector laboral, han creado la necesidad de contar con sistemas modernos para el procesamiento de información curricular.

Las tecnologías de la información han facilitado los diferentes procesos que contribuyen a la falsificación de comprobantes de estudios y de experiencia laboral. Estos procesos van desde el duplicado o creación del documento falso hasta su proliferación y venta. Actualmente una de las vías más comunes para realizar esta venta es por medio de Internet, ya que es la herramienta que más nos acerca al mundo de la publicidad y del comercio. Lo anterior se refleja en el alto incremento de la fabricación de documentos probatorios falsos, así como en la complejidad para identificarlos. Por lo tanto, es de relevancia que se cuente con un sistema que aproveche las ventajas de los dispositivos de almacenamiento y recuperación de información y las tecnologías de información actuales que permita verificar la validez de la documentación presentada por el portador, y que minimice el esfuerzo y tiempo invertido en el proceso de autenticación.

1.2 Antecedentes

En 1950 surgió la idea de utilizar tarjetas de plástico para identificar a clientes que tenían ciertos privilegios, como descuentos y línea de crédito, en establecimientos tales como bancos, restaurantes y otros negocios. Al paso de los años los bancos empezaron a implementar mecanismos de seguridad a estas tarjetas al agregarle una barra magnética que contenía información sobre la cuenta del cliente, hecho motivado principalmente por la necesidad de evitar fraudes o duplicado de la tarjeta. A pesar del éxito en el uso de estas tarjetas con barra magnética, no fue suficiente para evitar los delitos por el mal uso. Los bancos tuvieron que implementar medidas de seguridad más estrictas ante la gran cantidad de fraudes por clonación (eGov, 2006).

La invención del microprocesador en 1971 por la empresa Intel, abrió las puertas a un mundo de aplicaciones donde se requiere el procesamiento de información. Estos

dispositivos han evolucionado en gran escala en cuanto a las capacidades de procesamiento, velocidad y miniaturización. Posterior a la invención del microprocesador se desarrollaron los microcontroladores, los cuales son la integración de las funciones del microprocesador, con componentes adicionales para lograr conformar lo que se conoce como una "computadora en un solo circuito integrado (chip)". En la actualidad existen microcontroladores para todo tipo de aplicación. Castillo & Sosa (2001), en un trabajo de investigación sobre estos dispositivos, mencionan que "cualquier dispositivo que haga mediciones, almacene información, controle procesos, realice cálculos o despliegue información, es candidato para contener un microcontrolador".

En 1974 un inventor francés patentó la primera tarjeta que contenía un circuito integrado con capacidades de realizar transacciones. En aquel entonces era demasiado costosa, pero no fue sino hasta 1978 que, gracias a la miniaturización de los circuitos integrados, se lograron producir estas tarjetas en grandes cantidades. La red de tarjetas de crédito "Carte Bancaire" implementó esta tecnología en sus tarjetas Visa y MasterCard.

La evolución de la tecnología de estos dispositivos permitió el desarrollo de diversas aplicaciones, haciéndolas cada vez más seguras para la transferencias de fondos, monedero electrónico, almacenamiento de valor e información sensible y como medio de autenticación e identificación. Tanto fue el éxito de esta tecnología que en 1986 se encontraban en circulación varios millones de tarjetas inteligentes para uso telefónico en Francia, alcanzando casi 60 millones en 1990 y para 1994 ya todas las tarjetas en bancos franceses contaban con chip integrado. Hoy en día se utilizan tarjetas con chip en más de 90 países (Petri, 1999; eGov, 2006).

Las tarjetas inteligentes se han incorporado también en el ámbito educativo, al ser utilizadas en diversas aplicaciones que van desde monedero electrónico, hasta medio de autenticación para que los estudiantes puedan acceder a información académica. Tal es el caso de la Universidad de Cantabria en España, la cual utiliza tarjetas inteligentes para que sus estudiantes, profesores, investigadores y personal administrativo, puedan realizar diversos pagos en su modalidad de monedero electrónico, obtener descuentos en distintos

establecimientos afiliados a la institución, acceder a edificios del campus que requieren autorización, obtener préstamos de libros de las bibliotecas, acceder a los equipos de cómputo y comercio electrónico, entre otros servicios (UC, 2003). Como otro ejemplo, se encuentra la Universidad Autónoma de Baja California, quien recientemente repartió tarjetas inteligentes a sus estudiantes para que puedan realizar los pagos de colegiatura, identificarse en los servicios de préstamo de libros en las bibliotecas y servir como identificación de estudiante. Esto abre las puertas para desarrollar nuevas aplicaciones y aprovechar así, los beneficios que estos dispositivos brindan.

El hecho de que las tarjetas inteligentes cuenten con la capacidad para funcionar como mecanismo de autenticación e identificación, hace posible que éstas se puedan integrar a sistemas mayores que cuenten con aplicaciones variadas incluyendo bases de datos, y permitir así, la consulta de información relacionada con el portador de la tarjeta inteligente. Como ejemplo de una aplicación así, se encuentra el de un sistema que permita almacenar y consultar información sobre documentos probatorios que avalen los estudios y la experiencia laboral de una persona. Sin embargo, esto implicaría contar con un sistema donde se almacene de manera estructurada y estandarizada tal información. Actualmente no se cuenta con una estandarización para estructurar información de este tipo, pero existen algunos grupos de personas independientes que se encuentran trabajando en el desarrollo de esquemas para el almacenamiento de documentos académicos. Tal es el caso del proyecto *XMLRésumé Library* que, a finales del 2002, hizo pública la versión 1.5.1 de un programa con licencia de código abierto que permite crear un esquema de un currículum vitae, utilizando una definición de un tipo de documento (DTD) en lenguaje XML. Tal proyecto pretende mostrar una idea de cómo debe ser estructurado un currículum vitae para ser transportado entre diversas plataformas y aprovechar así, las tecnologías de la información para consulta y manejo de información académica entre instituciones educativas y empresas (Kelly, Christensen & Miller, 2002). El hecho de estar elaborado en lenguaje XML brinda varias ventajas, entre las que se encuentran, ser fácil de crear y de interpretar, facilita el intercambio de información entre distintas plataformas, utiliza una estructura jerárquica, permite agregar y eliminar elementos sin que se pierda su estructura y además, la información de los documentos

está etiquetada por su significado de forma precisa, por lo que facilita el desarrollo de aplicaciones donde se requiera presentación y búsqueda de información (McManus & Kinsman, 2002). Sin embargo, existe la limitante de que la estructura del proyecto *XMLRésumé Library* no incluye información a detalle sobre todos los elementos que conforman los documentos probatorios existentes. Tal proyecto permite estructurar solamente un resumen acerca de las habilidades, estudios y experiencia laboral de la persona, sin incluir elementos que sirvan para verificar su validez.

Tomando como referencia el proyecto *XMLRésumé Library*, se presenta en este trabajo el diseño de una estructura de documento en formato XML para almacenar expedientes curriculares en servidores de bases de datos, los cuales podrán ser consultados de manera eficiente y segura, utilizando tarjetas inteligentes.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un sistema basado en tarjetas inteligentes que permita almacenar y recuperar de manera segura y eficiente, expedientes curriculares electrónicos para brindar una alternativa en la verificación de la validez de documentos probatorios de las personas que cuentan con estudios de nivel profesional.

1.3.2 Objetivos específicos

A partir de la definición del objetivo general se plantean los siguientes objetivos específicos:

1. Establecer los requerimientos para el diseño de un sistema que brinde una alternativa eficiente y segura, para la verificación de la validez de documentos

probatorios.

2. Proponer el uso de tarjetas inteligentes como mecanismo seguro de autenticación e identificación para tener acceso al sistema de almacenamiento y consulta de expedientes curriculares electrónicos.

3. Proponer y desarrollar un modelo para el almacenamiento y representación de expedientes curriculares electrónicos, con una estructura bien definida, que sea fácil de interpretar, y que sirva como estándar para su uso por las instituciones educativas y empresas del todo el país.

4. Diseñar y presentar la arquitectura del sistema de almacenamiento y recuperación de expedientes curriculares electrónicos.

1.4 Metodología

La metodología utilizada para la realización de este trabajo se integró por tres etapas, tal como lo muestra la figura 1.1 (Hernández, Fernández & Baptista, 1991). La primera etapa consistió en un estudio exploratorio, debido a que se examinó el tema y la problemática a solucionar, mencionando algunos antecedentes que motivaron la realización de este trabajo. En base a lo anterior, se definió el objetivo general el cual derivó en varios objetivos específicos.

Una vez planteado el problema y definido los objetivos, se realizó una investigación descriptiva la cual consistió de una revisión bibliográfica extensa sobre la tecnología de las tarjetas inteligentes para la documentación de temas que incluyen desde sus antecedentes hasta lo más actual, así como ejemplos de aplicaciones y temas relacionados con el manejo de información en forma segura. De igual forma, se elaboró el marco teórico sobre el tema de la seguridad de la información y los mecanismos para brindarla. Una vez obtenido suficiente información sobre estos dos temas fundamentales para este

trabajo, se procedió a realizar un análisis de la misma y documentar aquello que se consideró relevante para este trabajo.

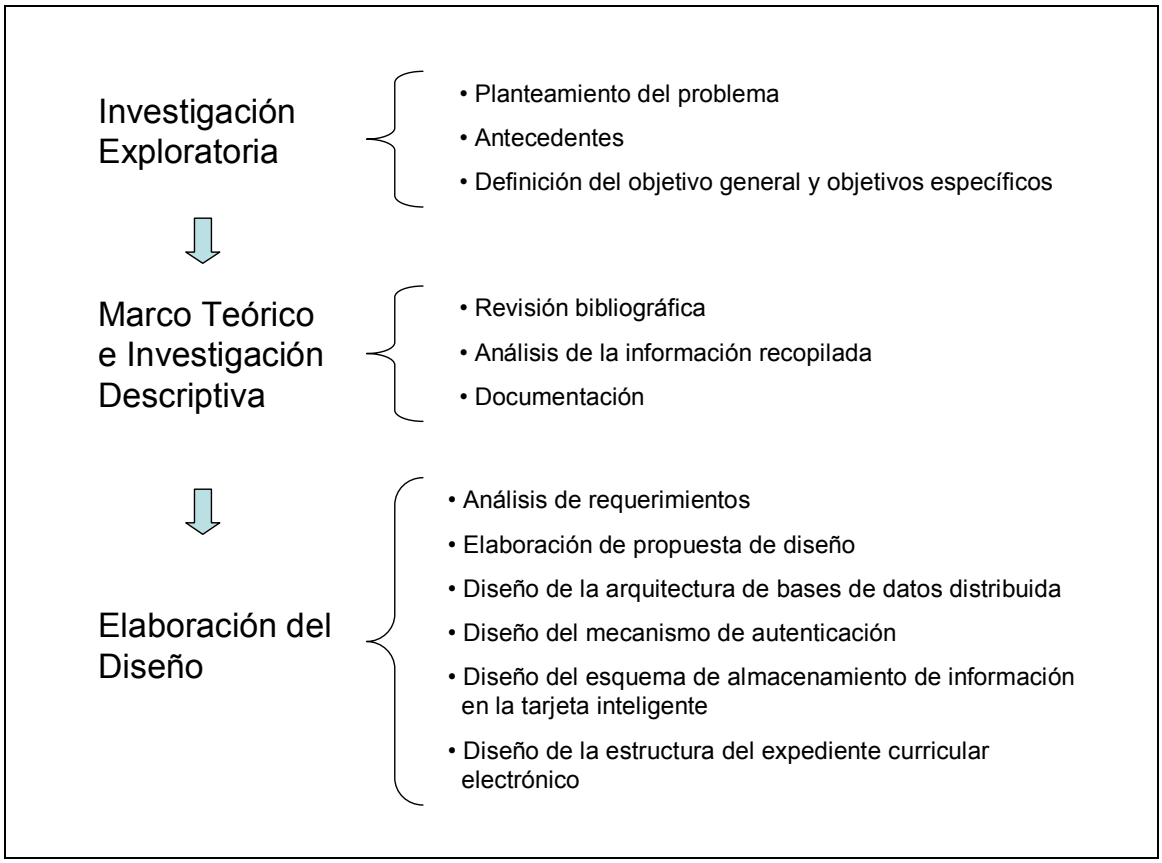

Figura 1.1 – Descripción de la metodología

La siguiente etapa consistió en la elaboración del diseño propuesto. Éste parte del análisis de los requerimientos, lo cual permitió definir algunos aspectos tales como la manera en que se distribuye la información en el sistema, el diseño de la arquitectura y los elementos que incluye, así como los mecanismos que se emplearon para brindar seguridad a la información. La información recopilada sobre la tecnología de tarjetas inteligentes y sobre seguridad de la información, brindó las bases para diseñar un mecanismo seguro de autenticación de los usuarios con el sistema. Para lograr esto, se llevó a cabo un análisis de algunos paquetes de desarrollo de aplicaciones con tarjetas inteligentes que se encuentran disponibles comercialmente y se seleccionó el más

apropiado para este trabajo, de acuerdo a los criterios establecidos en dicho análisis. El tipo de tarjeta inteligente que se incluye en el paquete de desarrollo seleccionado, determinó en gran parte la manera en que se diseñó el mecanismo de autenticación de los usuarios con el sistema. Una vez completado este diseño, se procedió a elaborar un esquema de almacenamiento para almacenar los datos personales del usuario en la tarjeta inteligente.

Como última etapa de este trabajo, se diseñó la primera versión de la estructura de un expediente curricular electrónico, cumpliendo con los requisitos de estar bien definida y de que pueda ser estandarizada para ser implementada por todas las instituciones educativas y entidades laborales que se integren a este sistema.

1.5 Estructura del documento

El documento de esta investigación se encuentra estructurado de la siguiente manera:

En el capítulo II se presenta la tecnología de las tarjetas inteligentes, comenzando por su definición y se citan algunos eventos históricos que contribuyeron al surgimiento y evolución de tales dispositivos, desde 1950 hasta la actualidad. Posteriormente se presentan las formas en que las tarjetas inteligentes se clasifican, así como sus variadas aplicaciones, características, tecnologías empleadas y software para el desarrollo de aplicaciones. Al final del capítulo se mencionan los estándares que definen las propiedades físicas, de comunicación y señalización de datos, así como los protocolos empleados.

El capítulo III presenta el tema de la seguridad de la información. Aquí se definen algunos conceptos básicos relacionados con este tema, así como los elementos que intervienen en ella. Posteriormente se mencionan los mecanismos que permiten la construcción de una solución segura para el intercambio de información, haciendo énfasis

en el tema de la criptografía, y se describen los tipos de algoritmos criptográficos existentes.

En el capítulo IV se presenta el diseño del sistema propuesto, partiendo de los requerimientos para proporcionar una alternativa segura en la verificación de la validez de documentos probatorios. El diseño se divide en cinco secciones para mostrar de manera más clara los aspectos que lo componen. En la primera sección se presenta la manera en que se distribuye en el sistema, la información de los expedientes curriculares. Se comienza con un análisis de las ventajas y desventajas que brindan tanto el almacenamiento centralizado, como el distribuido, y los aspectos a considerar. En base a este análisis, se presenta a detalle como se almacenará esta información. La segunda sección comienza ya con la arquitectura del sistema. Aquí se presentan los elementos que lo conforman y las funciones que éstos realizan. La tercera sección se enfoca al uso de tarjetas inteligentes para brindar un mecanismo seguro de autenticación con el sistema e identificación de los usuarios. Se presenta a detalle el proceso de autenticación mutua que se lleva a cabo entre los usuarios y los servidores del sistema. En la cuarta sección se describe la información que contendrá la tarjeta inteligente en su memoria interna. Primero se presenta un análisis de la información requerida, haciendo una comparación con las capacidades de almacenamiento de la tarjeta inteligente seleccionada para este trabajo. Posteriormente se define un esquema de almacenamiento de esta información y la manera en que se podrá adecuar a la estructura de archivos existente en estos dispositivos. Como última sección del capítulo IV, se presenta el diseño de la estructura de los expedientes curriculares electrónicos empleando el Lenguaje de Marcado Extensible (XML). Para esto, se define primero cada elemento que contendrán los documentos probatorios y posteriormente se presenta el esquema que éstos utilizarán para su almacenamiento.

Seguido del diseño, se presentan las conclusiones que se obtuvieron al finalizar la investigación y desarrollo de este trabajo. Al final se incluyen algunos anexos que complementan este trabajo con información relevante, seguido de la bibliografía empleada y algunos productos resultantes de este proyecto de investigación.

Capítulo II. Tecnología de Tarjetas Inteligentes

2.1 Definición

El término "Tarjetas Inteligentes" ha sido utilizado de manera no muy precisa en algunas fuentes de información al referirlas como aquellas tarjetas que tienen la capacidad de relacionar información con alguna aplicación en particular, como por ejemplo las tarjetas de barra magnética, las tarjetas de barra óptica, las tarjetas con chip de memoria y las tarjetas con microprocesador. Sin embargo, es más preciso utilizar este término para aquellas que tienen chip con memoria y para las que tienen chip con microprocesador (eGov, 2006).

Lo que hace "inteligente" a estas tarjetas es el chip que tienen empotrado. Este chip puede contener memoria para almacenamiento de datos con cierto nivel de seguridad o puede contener además, un microprocesador controlado por un sistema operativo con la capacidad de procesar datos y ejecutar programas de manera local en la tarjeta (Poynder, 2001). En este contexto, la palabra "inteligente" se relaciona a la capacidad que tiene la tarjeta para procesar datos.

Inteligente = Capacidad de procesamiento

Una tarjeta que contiene solamente memoria, puede almacenar una gran variedad de datos incluyendo información personal, financiera, registros de salud, etc., pero no tiene la capacidad de procesar esta información, esto es, tiene una condición "pasiva". En cambio, una tarjeta inteligente es un dispositivo "activo", porque procesa datos y reacciona ante ciertas condiciones dadas (CardWerk, 1999).

Entre algunas definiciones de las tarjetas inteligentes se encuentran las siguientes:

"Una tarjeta inteligente es un tipo de tarjeta de plástico con una computadora de circuito integrado (chip) empotrado que almacena y realiza transacciones de datos entre usuarios" (Cardlogix, 2004).

"Sistema portador de información electrónico que usa tarjetas de plástico del tamaño de una tarjeta de crédito con un circuito integrado incrustado que guarda información de los procesos" (SECTRA, 2000).

"Una tarjeta inteligente es una computadora portátil, resistente a daños, con un almacén de datos programable. Es de forma y tamaño exacto al de una tarjeta de crédito, puede almacenar 32KB o más de información sensible y también puede realizar procesamiento moderado de datos" (Jurgensen & Guthery, 2002).

Son muchas las definiciones que se pudieran encontrar para las tarjetas inteligentes. Sin embargo, la mayoría de ellas se centran en una idea principal: la de contener incrustado un chip de circuito integrado que le permite almacenar información de manera segura e incluso procesar esta información. Tomando como base a las anteriores, se propone la siguiente definición:

"Una tarjeta inteligente es un dispositivo que tiene las características físicas similares a las de una tarjeta de crédito convencional y que además tiene un circuito integrado empotrado, con memoria y capacidades de procesamiento de información, que le permite ejecutar aplicaciones para almacenamiento y transferencia de información en forma segura, confiable y eficiente".

2.2 Historia y Evolución

Han sido varios los factores que en conjunto impulsaron el surgimiento de las tarjetas inteligentes. La necesidad de las empresas e instituciones de contar con una forma para identificar a sus miembros y proveer ciertos privilegios o grados de confianza, motivó el que se utilizaran unas tarjetas de cartón en donde la persona podía identificarse ante esta institución o empresa. Esta tarjeta de cartón fue evolucionando de tal manera que pudiera brindar cada vez más seguridad de su contenido y de esta manera, evitar que fuera copiada o alterada. La necesidad de contar con una alternativa para evitar fraudes con las tarjetas de barra magnética junto con el surgimiento de la tecnología de los microprocesadores, impulsaron la evolución de estas tarjetas al incrustarles un circuito integrado con capacidades de almacenamiento y procesamiento, resultando así, en lo que conocemos como tarjetas inteligentes (Diners Club, 2005; Clark, 1990; eGov, 2006).

Los siguientes hechos históricos relacionados con la evolución de las tarjetas inteligentes fueron obtenidos principalmente del sitio Web de la Administración de Servicios Generales de los Estados Unidos (eGov, 2006). Se hace mención también de otras fuentes de información entre las que se encuentran sitios Web de empresas, artículos y tutoriales.

- **1950.** La cadena de restaurantes estadounidense “Dinner’s club” introdujo la primera tarjeta de crédito como alternativa al pago en efectivo. Tal tarjeta era en un principio de cartón y posteriormente se utilizó el plástico. Esta acreditaba a su titular para disponer bienes y servicios sin pago inmediato de dinero en efectivo, comprometiéndose a realizar el pago en efectivo posteriormente y además podía utilizase en distintos establecimientos que reconocía tal cadena, incluyendo hoteles, restaurantes y tiendas. El club era muy exclusivo y sólo personas como millonarios y hombres de negocios podían adquirir la tarjeta. Al paso de los años, los bancos adoptaron este concepto sin mucho éxito, pero no fue sino hasta 1959 que el Banco de América tomó el riesgo de emitir 60 mil tarjetas sin haber sido solicitadas a 60 mil habitantes en Fresno, California, logrando incrementar su consumo.

- **1951.** El banco "Franklin National Bank" de EE.UU. empezó a utilizar la primera tarjeta de crédito, siguiéndole otros bancos como Chase Manhattan, Bank of America y Marine Midland Trust del mismo país.

  Posteriormente Visa y MasterCard entraron al mercado utilizando estas tarjetas, pero luego fue necesario utilizar un lector electrónico debido a las presiones de problemas como fraudes, modificaciones, cargos bancarios, etc. Esta tecnología aún se utiliza en la actualidad, pero tiene varias debilidades en cuanto a seguridad debido a que cualquiera que posea un lector puede acceder a los datos contenidos en ella y se requiere un servicio de información centralizada para procesamiento y verificación.

- **1960.** Comienza a utilizarse la tarjeta de crédito con banda magnética.

- **1968.** Jurgen Dethloff y Helmut Grotrupp, dos inventores alemanes, patentaron la idea de incorporar un circuito integrado en una tarjeta de identificación. Aplicaciones similares se llevaron a cabo en Japón en 1970 y en Francia en 1974.

- **1970.** El doctor japonés Kunitaka Arimura archivó la primera y única patente del concepto "Smart Card" (CardWerk, 2006).

- **1971**. Intel desarrolló la primera computadora en un chip con la creación su microprocesador modelo 4004. Tal chip era de propósito general y se podía utilizar en muchos dispositivos electrónicos, marcando así el inicio de la industria de los microprocesadores.

- **1974**. El inventor independiente francés Roland Moreno, incluyó un chip en una tarjeta y desarrolló un sistema para utilizar la tarjeta para realizar transacciones de pago. El archivó la patente original de la "IC Card" que después se cambió a "Smart Card" (Tarjeta Inteligente). Después de mostrar su invento a los bancos franceses, la empresa "CII Honeywell Bull" desarrolló a finales del año, la primera tarjeta "CP8 Transac Card" que posteriormente utilizó la red de tarjetas de crédito Carte Bancaire

en sus tarjetas Visa y MasterCard. En aquel tiempo la industria de semiconductores ya tenía la capacidad de proveer circuitos integrados a precios razonables.

- **1977.** Tres fabricantes comerciales: Bull CP8, SGS Thomsom, y Schlumberguer empezaron a producir la IC card que diseñó Roland Moreno.

  Bancos franceses completan especificaciones sobre un sistema de pago que utiliza tarjetas inteligentes. Un año después se desarrolla el primer prototipo.

- **1979.** La empresa Motorola desarrolla el primer microcontrolador seguro en un solo chip para uso en tarjetas inteligentes de bancos franceses.

- **1982.** Se llevó a cabo en Francia la mayor prueba de campo de las tarjetas con chip de memoria serial para uso telefónico.

- **1983.** Se utilizan tarjetas inteligentes en toda la nación de Francia al ser adoptadas por la Administración de Servicio Postal, Telégrafos y Telefonía (PTT) como sistema de pago telefónico.

- **1984.** Los servicios franceses de correos y telecomunicaciones (France telecom) probaron con resultados muy exitosos las tarjetas telefónicas con chip (llamada Télécarte). Además los bancos franceses fueron los primeros en utilizar una tarjeta de débito con chip integrado (llamada Carte Bleue). Las pruebas fueron exitosas para su uso en cajeros automáticos.

- **1986.** En Francia se encontraban en circulación 60 millones de tarjetas inteligentes para uso telefónico. Esto permitió que se explotara la tecnología de las tarjetas inteligentes sin tener que cumplir con estándares tecnológicos anteriores. Las tarjetas telefónicas francesas utilizaban chips EPROM (memoria de sólo lectura, programable y borrable), mientras que las alemanas utilizaban EEPROM (memoria de sólo lectura, programable y borrable eléctricamente). En la actualidad, estas

tarjetas telefónicas se encuentran disponibles en más de 50 países.

- **1987.** Se implementa la primera aplicación a gran escala de tarjetas inteligentes en Estados Unidos en el Departamento de Agricultura para automatizar los procesos de transacciones en el mercado de cacahuates. Cada productor tenía una tarjeta con chip que almacenaba registros de transacciones así como la información del productor.

- **1991.** Se implementan por primera vez las tarjetas inteligentes para transferencias electrónicas de beneficios (EBT) en el Programa de Nutrición de Suplementos Especiales de Wyoming para mujeres, infantes y niños (WIC), reemplazando el uso de cupones y cheques para alimentos. La aplicación permite que la tarjeta se pueda utilizar en sistemas fuera de línea (offline), ya que la transacción se realiza entre la tarjeta y una terminal de punto de venta. En el año 2000, setenta y cinco por cierto de las casas de asistencia del programa ya utilizaban el sistema con tarjetas inteligentes.

- **1992**. En Dinamarca se inició el proyecto DANMONT el cual consistió en utilizar tarjetas inteligentes de prepago llamadas "bolsa electrónica" la cual se podía utilizar para realizar pagos en estacionamientos, compra de boletos para transporte, pagos en máquinas dispensadoras de alimentos, etc. Estas tarjetas eran desechadas una vez que se les acababa el dinero almacenado, pero en 1995 desarrollaron tarjetas de prepago que se podían recargar en cajeros automáticos.

- **1993.** En Francia se lanzaron las primeras tarjetas para aplicaciones multifunción, al agregar la función Télécarte (para teléfonos públicos) a una tarjeta bancaria.

- **1994.** Europa contaba con 342 millones de tarjetas inteligentes de las 484 millones que había en el mundo. Austria las empezó a utilizar en 1996 y Alemania en 1997. Todos los bancos franceses ya contaban con chips en sus tarjetas.

  Estados Unidos se unió a Europa para la planeación de la futura tecnología de las tarjetas inteligentes. Europay, MasterCard y Visa trabajaron en las especificaciones

para incorporar chips en sus tarjetas, resultando en la especificación EMV (utilizando la primera letra de cada uno de ellos), prometiendo compatibilidad entre ellas y así, un futuro para el mundo de estas tarjetas y su uso en las transacciones mundiales.

Alemania comenzó la distribución de 80 millones de tarjetas inteligentes con memoria serial para el uso por sus ciudadanos como tarjeta de salud.

Se fabrica la primera tarjeta inteligente con acelerador criptográfico (STM, 2006).

- **1995.** Más de 3 millones de usuarios de teléfonos móviles en el mundo comienzan a utilizar tarjetas inteligentes para el pago del servicio.

  Se lanzan 40,000 tarjetas con chip multifunción y tecnología múltiple (MARC) para los marinos estadounidenses en Hawaii. Este tipo de tarjeta permitía el almacenamiento y actualización de datos personales de los miembros de los distintos servicios y empleados del Departamento de Defensa de los Estados Unidos, como por ejemplo, información de tratamiento médico y dental, información de movilidad de los soldados y conteo de personal, entre otros datos.

- **1996.** La empresa de manufactura de tarjetas Schlumberger introdujo la primera tarjeta que podía aceptar y ejecutar programas escritos en un lenguaje de alto nivel, llamado Java. Antes de la tarjeta Java, la única forma de cargar software a una tarjeta, consistía en escribir el código y cargarlo por medio de un fabricante de tarjetas. Esto era susceptible a errores y muy costoso. Los fabricantes utilizaban lenguaje C o Forth para crear la tarjeta, pero no se le proporcionaba el código a los dueños de la tarjeta ni a los usuarios.

  Se publica el estándar EMV de interoperabilidad entre tarjetas inteligentes para pagos seguros por las grandes firmas internacionales Europay, MasterCard y Visa. A la iniciativa del gobierno del Reino Unido para la implementación del estándar EMV

se le llama “Chip and Pin” y para Irlanda lo nombran “Chip and Pin Ireland”.

Durante los juegos Olímpicos de Atlanta, VISA lanza a la venta más de 1.5 millones de tarjetas que almacenan el valor en dinero efectivo (Cash Cards), y estuvieron disponibles en versiones desechables y recargables. Estas se utilizaron para compras menores en establecimientos participantes. Actualmente la “Cash Card” se encuentra disponible en Argentina, Australia, Canadá, Colombia y España, y en un proyecto piloto para Nueva York por VISA, MasterCard y Citibank.

MasterCard y VISA patrocinan consorcios competitivos para que resuelvan los problemas de interoperabilidad entre las tarjetas, resultando en 2 soluciones diferentes: 1) *JavaCard*, respaldada por VISA y 2) el Sistema Operativo de Funciones Múltiples (*MULTOS*), respaldado por MasterCard.

- **1998.** La Administración de Servicios Generales del Gobierno de EE.UU. y la Marina de Guerra, unieron fuerzas e implementaron un sistema de tarjetas inteligentes de nueve aplicaciones y una solución de administración de las tarjetas en el Centro de Tecnología de Tarjetas Inteligentes de Washington, D.C. El propósito de este centro fue demostrar y evaluar la integración de las tarjetas multiplicación con otros tipos de tecnologías, promoviendo sistemas disponibles para uso en el Gobierno Federal.

  Microsoft anuncia su nuevo sistema operativo *Windows* para tarjetas inteligentes, enfocando su uso para control de acceso a redes e información sensible, al sector de salud y a la industria del transporte y de entretenimiento., siendo su principal competencia las tarjetas inteligentes con los sistemas operativos *MULTOS* y *JavaCard*. Por otro lado, Francia comienza el uso de tarjetas inteligentes en el campo de la salud para sus 50 millones de habitantes.

- **1999.** Estados Unidos establece un proyecto para utilizar tarjetas inteligentes de identificación para ser utilizadas en las agencias de gobierno para acceso físico y

lógico de todos sus empleados federales.

- **2000.** Las empresas Keyware Technologies y Proton World International, comienzan el desarrollo de tarjetas inteligentes que pueden verificar al portador a través de su huella digital o por reconocimientos de la retina, además de utilizar los mecanismos convencionales de clave PIN y contraseñas A tales tarjetas las nombran *e-purse* (cartera electrónica) y están basadas en la tecnología de la biométrica. Tienen como objetivo reducir el fraude y otros problemas de seguridad (Rohde, 2000).

- **2002.** Hive Minded, una empresa de software en EE.UU. que utiliza la tecnología .NET de la empresa Microsoft, anunció el desarrollo de una plataforma llamada "*SmartCard.NET*", la cual permite la ejecución simultánea de múltiples aplicaciones en forma segura, así como el uso de varios lenguajes de desarrollo. Esta plataforma utiliza una máquina virtual para permitir el uso de tarjetas inteligentes en ambientes de la plataforma .NET (Hive Minded, 2002).

- **2003.** El Consorcio de Tarjetas Inteligentes para WLAN, formado por varias compañías, entre ellas fabricantes de chips y tarjetas inteligentes, así como instituciones educativas, desarrolló la especificación "*WLAN-SIM 1.0*" que define una interfaz para tarjetas inteligentes para proveer autenticación, distribución de llaves de sesión y administración de identidades utilizando tarjetas inteligentes del tipo SIM. Esto permite a los operadores de puntos de accesos inalámbricos extender la tecnología de las tarjetas SIM para autenticar redes WLAN. De esta manera, los usuarios podrán moverse de un punto de acceso a otro de manera segura. Además la empresa que provea el servicio de red identificará al usuario para poder realizar el cobro respectivo de la o las compañías de servicio de Internet que el usuario esté suscrito (WLAN Smart Card Consortium, 2003).

- **2004.** Se empieza a utilizar en Malasia la primera tarjeta VISA sin contacto que es compatible con el estándar global EMV, a la cual denominaron "*Visa Wave*". Con esta tarjeta no se requiere la firma del cliente ni presentar su tarjeta a la persona en

caja cuando se va a realizar un pago, sino solamente pasar la tarjeta a escasos cuatro centímetros de un lector de tarjetas que está en la caja. Esta tarjeta es del tipo de combinación, la cual contiene interfaz tanto para uso sin contacto como de contacto, por lo que puede utilizarse también en lectores convencionales (Smart Card Trends, 2004).

- **2005.** Se finaliza la especificación ISO/IEC 7816-12 la cual especifica las condiciones de operación de las tarjetas con circuito integrado que contienen Interfaz Serial Universal o más conocido como USB (Smart Card Trends, 2005).

  Se aprueba en EE.UU. el Estándar para el Procesamiento de Información Federal (FIPS) 201, el cual se desarrolló en respuesta de la Propuesta Presidencial para la Seguridad de la Patria (HSPD) 12, que tiene como objetivo mejorar la identificación y autenticación de empleados federales y contratistas para acceder a instalaciones y sistemas de información federal. Este estándar especifica, entre varias cosas, las interfaces y elementos de datos de las tarjetas de identificación, así como algoritmos criptográficos e interoperabilidad entre lectores (NIST, 2006).

- **2006.** En un proyecto patrocinado por la Fundación de Bill y Belinda Gates, se entregaron tarjetas inteligentes a 500 prostitutas del área de Mysore en India. Estas tarjetas mantienen el registro médico de estas personas, quienes se deben de realizar un examen médico cada tres meses. Con estas tarjetas, ellas pueden obtener descuentos en tiendas, hoteles y restaurantes, así como acumular bonos para comida y ropa. Pero si no presentan su examen médico, la tarjeta se desactiva. Con esta tarjeta los científicos del Instituto de Ciencia de India pueden leer, por medio de un dispositivo portátil, la información de la tarjeta y mandarla a un servidor central de manera confidencial (Raghu, 2006).

  El gobierno de Estados Unidos realiza un contrato con la empresa Gemalto (resultado de la unión de los dos grandes fabricantes de tarjetas inteligentes Gemplus y Axalto) para la fabricación de pasaportes electrónicos, como parte de su plan para

proveer a todos sus ciudadanos de estos pasaportes en el 2007. Con esta tecnología en los pasaportes, se proveerá de mayor eficacia y eficiencia en los cruces fronterizos, así como el incremento en las medidas de seguridad (Smart Card Trends, 2006).

2.3 Clasificación

Existen varias formas de clasificar las tarjetas inteligentes que están disponibles actualmente. Entre ellas se encuentran las siguientes:

2.3.1 Según su forma de comunicación

La forma de comunicación define cómo son leídos y escritos los datos en la tarjeta. Hay empresas que presentan distintos tipos de tarjetas inteligentes según su forma de comunicación. Sin embargo, en base a éstas, se consideró conveniente generalizar esta clasificación y presentarla en los siguientes cuatro tipos: (Cardlogix, 2001; ID Edge, 2002; Poynder, 2001).

1. **De contacto** – Este tipo de tarjeta contiene contactos eléctricos localizados en su exterior, los cuales conectan con el dispositivo que permite leer y escribir en la tarjeta inteligente cuando ésta se introduce en él. En algunas fuentes, como por ejemplo Everett (2004), hacen referencia a tal dispositivo como "Dispositivo de Aceptación de Tarjeta" o CAD (por sus siglas en inglés "Card Acceptance Device"). Pero para fines de este trabajo, se optó por utilizar el término "lector", ya que es más comúnmente utilizado en este contexto. Para realizar la transferencia de datos, la tarjeta debe permanecer dentro del lector y puede ser retirada una vez que ya se hayan efectuado las transacciones.

   Entre algunas de sus aplicaciones se encuentran las siguientes: seguridad de redes (autenticación), máquinas expendedoras de alimentos, plan de distribución de

alimentos, acumulación de valores, tarjetas de identificación de gobierno, comercio electrónico y tarjetas de registro de salubridad.

2. **Sin contacto –** Estas tarjetas no necesitan hacer contacto físico con el lector para realizar la transferencia de datos. Sólo se requiere que la tarjeta se encuentre dentro de un cierto rango de distancia del dispositivo lector, el cual dependerá del tipo de tecnología de transferencia sin contacto que se esté utilizando. Este tipo de tarjetas utiliza tecnología RFID (por sus siglas en inglés "Radio Frequency Identification" que significa "Tecnología de Identificación por Radio Frecuencia") e incorporan una antena interior que, mediante inducción de radiación electromagnética de baja frecuencia proveniente del lector, genera la electricidad necesaria para alimentar el chip, aunque existen algunas que incorporan una batería interna como fuente de alimentación.

   Estas tarjetas se utilizan en aquellas aplicaciones donde se requiera tomar ventaja de la rapidez que resulta de no tener que insertar la tarjeta en un lector, brindando mayor eficiencia en la operación, además de que prolonga la vida del lector al no ser expuesto a desgaste por el contacto físico de las terminales, como sucede con los lectores de tarjetas de contacto. Entre algunos ejemplos de aplicaciones se encuentran las siguientes: identificación de estudiantes, pasaporte electrónico, máquinas vendedoras de comida, casetas de cobro e identificaciones para acceso a edificios y oficinas.

   Hasta la fecha, tres tecnologías de tarjetas sin contacto han recibido estandarización por la Organización Internacional para Estándares (ISO) y por el Comité Internacional Electro-Técnico (IEC). A estos estándares se les conoce como ISO/IEC, aunque en algunas fuentes de información se utilizan sólo la iniciales ISO (p.e. ISO 14443). Las tres tecnologías de tarjetas sin contacto que definen la ISO/IEC son (Corum & Wehr, 2004; STM, 2005):

a. **Tarjetas de Acoplamiento Cercano** (CCD por sus siglas en inglés "*Close Coupling Devices"*) - Cumplen con el estándar ISO/IEC 10536. Es el primer estándar de tarjetas sin contacto que se definió y, debido a la corta distancia que operan con respecto al dispositivo de lectura y escritura (2 cm. máximo), requiere que se posicionen de manera muy precisa en el mismo, lo que las hace difíciles de utilizar y básicamente no brindan mucha ventaja respecto a las de contacto. Por estas razones, estas tarjetas casi no son utilizadas en la actualidad.

b. **Tarjetas de Proximidad** (PICC por sus siglas en inglés *"Proximity Integrated Circuit Cards"*) - Cumplen con el estándar ISO/IEC 14443 y son aquellas que están hechas para utilizarse a una distancia no mayor a 10 cm. del lector. Esta distancia puede variar dependiendo de los requerimientos de potencia, capacidad de memoria, tipo de CPU y procesador matemático. Son denominadas tarjetas sin contacto de "corto alcance". Al dispositivo de lectura y escritura se le llama "Dispositivo de Acoplamiento de Proximidad" o PCD (por sus siglas en inglés "Proximity Coupling Device"), el cual utiliza una frecuencia de 13.56 MHz.

c. **Tarjetas de Vecindad** (*VICC* por sus siglas en inglés *"Vecinity Integrated Circuit Cards"*)- Cumplen con el estándar ISO/IEC 15693 y son aquellas que están hechas para utilizarse a distancias mayores que las de acoplamiento cercano y las de proximidad. Al igual que las tarjetas de proximidad, utilizan una frecuencia de 13.56 MHz. Son denominadas "tarjetas de largo alcance" y los rangos de distancia para comunicación con el lector dependen del modo de operación y del tipo de lector, ya que este tipo de tarjetas fue diseñado para que operen a distancias entre 50 y 70 centímetros del lector cuando se utiliza una antena sencilla. En otros modos de operación puede alcanzar una distancia de hasta 1.5 metros. (Inside Contactless, 2003).

3. **Híbridas –** Esta tarjeta contiene dos chips empotrados, uno utilizando tecnología de contacto y otro que utiliza tecnología sin contacto. Ambos chips pueden ser chips de microprocesadores o simples chips de memoria. El chip sin contacto se utiliza generalmente en aplicaciones que requieren transacciones rápidas (por ejemplo, el cobro instantáneo en el transporte), mientras que el chip de contacto es utilizado en aplicaciones que requieren de alta seguridad como las bancarias. La tarjeta híbrida también provee una solución alterna a los sistemas tradicionales de tarjetas de contacto durante la transición a tecnologías sin contacto.

4. **De interfaz dual** – También es conocida como "Tarjeta de Combinación". Una tarjeta de interfaz dual es similar a la tarjeta híbrida en que la tarjeta presenta ambas interfaces con y sin contacto. La diferencia más importante es el hecho de que la tarjeta de interfaz dual tiene solamente un solo circuito integrado. Esto permite el uso de un solo microprocesador para cifrar y acceder cierta área de memoria que puede ser accedida para ambas funciones.

2.3.2 Según el tipo de chip

Las tarjetas inteligentes también las podemos clasificar de acuerdo al tipo de chip que implementan, lo cual hacen que varíe su funcionalidad. Actualmente se conocen los siguientes dos tipos (Carlogix, 2004):

1. **Tarjetas de memoria** – A estas tarjetas también se les conoce como tarjetas "Low-End" (Rodríguez, Perovich, Varela & Martínez, 2001). No tienen procesamiento y no pueden realizar manejo de memoria en forma dinámica. Estas tarjetas se comunican con el lector a través de protocolos síncronos. Algunas de estas tarjetas utilizan cierta lógica de seguridad, a nivel de hardware, para controlar el acceso a la información. La empresa Cardlogix (2004) divide las tarjetas de memoria, de acuerdo a su funcionalidad, en los siguientes tres tipos:

a. **Tarjeta de memoria común** - Solamente almacenan datos y no tienen capacidades de procesamiento. Son las más baratas. En cuanto a su comportamiento, se asemejan a un disco flexible. Además, no tienen manera de identificarse con el lector, por lo que el sistema debe saber qué tipo de tarjeta se insertó.

b. **Tarjetas de memoria segmentada / protegida** - Estas tarjetas incluyen lógica de control para el acceso a la memoria, por lo que tienen cierto nivel de inteligencia que les permite proteger de escritura algunas partes o toda la memoria. Algunas de estas tarjetas se pueden configurar para restringir el acceso tanto de lectura como escritura por medio de una llave o contraseña. Las memorias segmentadas se pueden dividir en secciones lógicas para proveer multifuncionalidad.

c. **Tarjetas de memoria con valor almacenado** - Están diseñadas para el propósito específico de almacenamiento de valores o llaves. Existen en tipos desechables y en recargables. La mayoría incorporan medidas de seguridad permanente durante su fabricación, como por ejemplo, contraseñas y lógica almacenada en el chip. Los arreglos de memoria de estos dispositivos están configurados para restar cantidad de celdas de memoria o como contadores de accesos, por lo que no hay memoria para otras funciones. Algunas tarjetas telefónicas contienen un chip con 60 o 12 celdas de memoria, una para cada unidad. Una vez que las unidades de memoria se usan, la tarjeta se vuelve inservible y se tiene que desechar. En el caso de las recargables, este proceso simplemente se realiza en forma inversa durante su recarga.

2. **Tarjetas con microprocesador –** También se les conocen como tarjetas "High-End" (Rodríguez et al., 2001). Estas tarjetas tienen capacidades de procesamiento de datos dinámicos en el chip. Contienen un microprocesador o microcontrolador que administra el manejo de la memoria y el acceso a los archivos por medio de un sistema operativo o COS (por sus siglas en inglés de *"Card Operating System*").

Esta cualidad les permite que tengan muchas funciones y que residan múltiples aplicaciones en la misma tarjeta. Por ejemplo, una tarjeta de débito que además permita el acceso al campus de una escuela. Esta tecnología permite actualizar información sin reemplazar la base de las tarjetas, logrando así simplificar los cambios en los programas y como consecuencia, una reducción de costos.

2.4 Aplicaciones

La función de una tarjeta inteligente es la de ser una llave portátil, esto es, que el dueño de la tarjeta pueda llevarla de un lugar a otro para utilizarla en el contexto de un sistema de aplicación. La tarjeta almacenará generalmente información sensible, la cual el dueño de la tarjeta y el sistema quieren que se mantenga en forma privada. Además de lo anterior, la tarjeta puede proveer servicios a su dueño o al sistema de aplicación por medio del procesamiento de datos en forma segura y confiable (Jurgensen & Guthery, 2002).

Las tarjetas inteligentes se han estado utilizando en una gran cantidad de aplicaciones en todo el mundo y día con día se pueden encontrar nuevos tipos de aplicaciones que hacen uso de ellas. Las siguientes aplicaciones son sólo algunas de las más comunes:

2.4.1 Servicios financieros

Los bancos fueron los primeros en implementar estas tecnologías al utilizarlas para brindar más seguridad al sistema de transacciones. La seguridad en las transacciones que brindan estas tarjetas, permitió a los bancos reducir el número de fraudes y el poder utilizarlas para transacciones financieras sin requerir conexión con la base de datos central, lo que se conoce como "fuera de línea" (off-line). Los bancos utilizan esta tecnología para sus tarjetas de débito, de crédito y para tarjetas de tipo monedero electrónico. Estas últimas almacenan el valor de dinero en efectivo para realizar compras

sin utilizar la red bancaria, descontando el monto de la tarjeta inmediatamente y no de la cuenta bancaria.

2.4.2 Sector salud

Algunos hospitales han empezado a implementar tarjetas inteligentes en su sistema de administración de pacientes agilizando los procesos de captura de información del paciente, control de historias clínicas y prescripción de medicamentos entre otros. Los clientes del hospital cargan su tarjeta todo el tiempo y esto le permite al personal del hospital acceso inmediato al historial médico, medicinas recetadas, información sobre alergias, nombres y teléfonos de familiares y otros datos necesarios para la toma de decisiones de tratamiento médico. De esta manera, el personal del hospital responde a las necesidades del paciente de manera más efectiva, ya que su información está disponible en cualquier momento. A estas tarjetas se les conoce como tarjetas de salud (Health Smart Card, 1999). Rodríguez *et al.* (2001) definen una tarjeta de salud (HealthCard) como "una tarjeta inteligente que contiene información personal, médica y de seguridad, utilizada en sistemas médicos".

2.4.3 Identificación

Las tarjetas inteligentes se pueden utilizar como dispositivo para comprobar la identidad de su dueño. La utilización de mecanismos como el de clave secreta (PIN) permite que el usuario se identifique al introducir esta clave al momento de utilizar la tarjeta en una aplicación. Con este mecanismo, el sistema comprueba que esa persona sea quien dice ser, antes de proceder con cualquier interacción.

2.4.4 Control de acceso físico y presencia

Las tarjetas inteligentes proporcionan una buena forma de establecer la identidad de una persona en una red grande donde no necesariamente se pueda conocer con quien se está

interactuando (Jurgensen & Guthery, 2002). Un ejemplo sería el acceso a puertas en un edificio, donde para poder entrar se deba presentar la tarjeta inteligente en el lector de la puerta. Una vez que el sistema extrae los datos de la tarjeta y verifica los privilegios de acceso para esa tarjeta en particular, procede a abrir la puerta o negarle el acceso. Un mecanismo para reforzar esta seguridad es el uso de claves secretas o el uso de reconocimiento de huella dactilar.

Las tarjetas inteligentes del tipo sin contacto son ideales para aplicaciones donde se requiera identificar la presencia de personas en cierta área. Ejemplos de aplicaciones con este tipo de tarjetas son los mecanismos de seguridad en edificios de gobierno donde se requiere saber, por parte del personal de seguridad, en que lugar se encuentran los empleados en todo momento, para evitar así, actos delictivos como secuestros, atentados, robos, etc.

2.4.5 Sistemas de votaciones electrónicas

Con el empleo de mecanismos de autenticación e identificación en forma segura se pueden utilizar tarjetas inteligentes en sistemas de votaciones electrónicas de manera confiable e incluso poder efectuarse de través de Internet sin que el usuario se encuentre físicamente en el sitio de votaciones (Breunesse, Jacobs & Oostdijk, 2002). En Carracedo, Gómez, Pérez, Moreno & Sánchez (2004) se presenta de manera general, el diseño de un sistema de votaciones electrónicas que utiliza tarjetas inteligentes del tipo JavaCards y el cual puede ser operado de manera remota. El sistema autentica a los usuarios por medio de estas tarjetas. Además, asegura que conserven su anonimato y que puedan votar sólo una vez.

A pesar de las polémicas causadas por el tema de los riesgos de seguridad en los sistemas de votaciones electrónicas, como fue el caso de Estados Unidos, que canceló en el año 2004 sus procesos de elecciones electrónicas para militares y ciudadanos que viven en el extranjero, otros países han continuado con la implementación de esta tecnología. Un ejemplo de esto es la República de Estonia que demostró ser el primer país en utilizar la

opción de votación por Internet usando tarjetas inteligentes sin reportar inconvenientes ni problemas de seguridad (Associated Press, 2005).

2.4.6 Tarjetas telefónicas

Uno de los usos más comunes de las tarjetas inteligentes es en tarjetas telefónicas de prepago. Esta es una de las primeras aplicaciones de las tarjetas inteligentes. Incluso algunas fuentes, como por ejemplo eGov (2006) y ST Microelectronics (2006), mencionan que fue la primera aplicación desarrollada para estos dispositivos. Sin embargo, en otras fuentes como CardWerk (2006) se menciona que se utilizaron primero como tarjetas bancarias. Cuando se empezaron a utilizar para prepago en teléfonos públicos, las tarjetas contenían solamente memoria que almacenaba el valor del crédito de llamadas telefónicas. Esto las hizo susceptibles a alteraciones y consecuentemente a fraudes en el uso de estas tarjetas. Se han implementado nuevos mecanismos de seguridad para evitar alterar el valor almacenado que las ha convertido en un dispositivo muy seguro para este tipo de aplicaciones.

2.4.7 Entretenimiento

Lar tarjetas inteligentes se utilizan en sistemas de entretenimiento como la recepción de canales de televisión satelital (Bezakova, Pashko & Surendran, 2000). En estos sistemas los suscriptores utilizan una tarjeta inteligente que almacena información sobre la suscripción y al introducirla en el equipo de recepción de la señal, este se identifica con el sistema y permite la recepción de la señal de los canales de televisión, dependiendo del servicio que solicitó el suscriptor.

2.4.8 Membresía

Debido a la capacidad que tienen las tarjetas inteligentes para almacenar información en forma segura, se utilizan como tarjetas de membresía en donde se requiera almacenar

información del cliente, su historial de compras, acumulación de puntos para posteriores descuentos y ofertas, etc. Tal es el caso de algunos cines que las utilizan como monedero electrónico para que sus clientes puedan realizar compras de boletos de entrada y consumibles en dulcería, además de darles la ventaja de la acumulación de puntos por sus compras, renta de videos y participación en promociones (Cardlogix, 2001b).

2.4.9 Acceso seguro de datos

Algunas tarjetas inteligentes cuentan con algoritmos de encriptación que, junto con el almacenamiento de llaves, le permiten realizar procesos de autenticación con otros sistemas para tener acceso a información o privilegios en él. Otras proveen de mecanismos para evitar cualquier intento de extracción o alteración por personas no autorizadas, de la información almacenada en ellas. Entre estos mecanismos se encuentra el deshabilitar la tarjeta completamente en caso de que la clave PIN no sea escrita correctamente después de cierto número de intentos, dejando la tarjeta inservible y evitando así que otros tengan acceso a ella. Tal es el caso de la tarjeta *ACOS2* de la empresa *Advanced Card Systemas Ltd*. la cual combina el mecanismo de autenticación y clave PIN para proteger datos almacenados en sus archivos internos (ACS, 2006).

2.4.10 Telefonía celular y telecomunicaciones

Para el sector de las telecomunicaciones, las tarjetas inteligentes proveen una mejora en la seguridad de las redes a través de la identificación de usuarios, el almacenamiento de datos del mismo, y un mecanismo para registrar los eventos de los servicios que se imparten. Estas características brindan un mejor servicio personalizado y la portabilidad en un ambiente muy seguro, especialmente para servicios basados en transacciones.

La red GSM (Sistema Global para Comunicaciones Móviles) desarrolló a principios de los años 90s, el Módulo de Identidad del Suscriptor o SIM (por sus siglas en inglés "Subscriber Identity Module") como medio para autenticar usuarios a esta red.

En un estudio de mercado sobre tarjetas inteligentes realizado por la Smart Card Alliance junto con la empresa de consultoría Frost & Sullivan, encontraron que, en el año 2005, el mayor uso de tarjetas inteligentes en América sería en tarjetas SIM (Frost & Sullivan, 2005), mientras que en el año 2000 se encontraba en segunda posición, ya que las tarjetas telefónicas de prepago representaban el mayor porcentaje.

2.4.11 Procesos industriales

Algunas plantas industriales utilizan tarjetas inteligentes para incrementar el nivel de seguridad en sus procesos. Se emplean como llave de acceso para activar controles de maquinaria, así como para permitir el acceso físico al personal en ciertas áreas críticas de la planta.

2.5 Características y funcionamiento

En temas anteriores se presentó la evolución de las tarjetas inteligentes junto con la diversidad de aplicaciones en las que han sido usadas. Esto ha demostrado que esta tecnología se encuentra en constante evolución y cada vez son más los tipos de tarjetas que se desarrollan. Sin embargo, para tener un panorama más amplio sobre las tarjetas inteligentes y poder crear aplicaciones basadas en ellas, es importante conocer sus características y la forma en que operan.

2.5.1 Características Clave

La tecnología de las tarjetas inteligentes se encuentra en evolución constante y cada vez son más las aplicaciones que las emplean. Esto es debido a que cumplen con ciertas características clave que satisfacen los requerimientos para el desarrollo de tales aplicaciones. Entre estas características clave se mencionan las siguientes: (eGov, 2006)

1. **Costo** – Actualmente estas tarjetas se encuentran oscilando en costo entre escasos centavos de dólar hasta $20 dólares estadounidenses, dependiendo de su funcionalidad y capacidad de almacenamiento. El costo se incrementa conforme aumenta la capacidad de almacenamiento y la complejidad de sus funciones, por ejemplo, el tipo de sistema operativo que utiliza, velocidad de procesamiento, opciones de seguridad, estándares que cumple, etc. A su vez, el costo disminuye conforme el volumen en la compra de tarjetas aumenta.

2. **Confiabilidad** – En el estándar ISO 7816-1 se especifican las características físicas que deben tener estas tarjetas tales como el tamaño y grosor, pero además se definen los valores de tolerancias para que el fabricante realice las distintas pruebas físicas que asegurarán la confiabilidad de estas tarjetas. Entre las pruebas que se realizan se encuentran: resistencia a golpes y caídas, flexibilidad, corrosión, temperatura, humedad, descargas electrostáticas, resistencia eléctrica, disipación de calor, ataques químicos, exposición a campos magnéticos, rayos ultravioleta y rayos X (Everett, 1992-1994).

3. **Corrección de errores** – Los sistemas operativos del circuito integrado actuales ejecutan su propia corrección de errores. El sistema operativo de la terminal debe revisar los códigos de estatus que regresa el COS una vez que la terminal solicita la ejecución del comando (instrucción) a la tarjeta. Estos códigos de errores están definidos por el ISO 7816-4 y los comandos propietarios de la tarjeta. Posteriormente la terminal debe tomar las medidas correctivas necesarias (eGov, 2006).

4. **Capacidad de almacenamiento** –Actualmente se encuentran tarjetas disponibles comercialmente con capacidades de almacenamiento que van desde cientos de bits hasta 8 Mbits, aunque existen compañías que se encuentran desarrollando tarjetas con mucho más capacidad, como es el caso de *Oberthur Card Systems* que publicó en su portal de Internet en febrero de 2006, el lanzamiento de su tarjeta inteligente tipo SIMM (por sus siglas en inglés de "*Single in-line Memory*

Module", que significa "Módulo de Memoria de Alineación Simple") con capacidad de almacenamiento de 512 Mbytes (Oberthur, 2006).

5. **Facilidad de uso** – Se maneja fácilmente, tal como las tarjetas de banda magnética.

6. **Susceptibilidad** –. Es susceptible a daños en el chip por abuso físico, pero es más difícil de dañar o sufrir alteraciones que la de banda magnética.

7. **Seguridad** – Son muy seguras. La información almacenada es muy difícil, más no imposible, de duplicar o alterar, contrario a las de banda magnética que son fáciles de extraerles su información. Se utilizan algoritmos criptográficos, mecanismos de autenticación y claves de acceso para proteger la información. Para lograr examinar o interceptar la información, se requiere del uso de equipo costoso junto con la disponibilidad de contar con la tarjeta, sin que su dueño se percate (Jurgensen & Guthery, 2002).

8. **Velocidad de primera lectura** - El ISO 7816-3 define la velocidad inicial de transmisión en las tarjetas de contacto de 9600 bits por segundo. Sin embargo, esta velocidad se puede cambiar después de su inicialización. Tal es el caso de la tarjeta *Cyberflex Access 32K* de la empresa *Axalto* la cual puede configurarse para una transmisión de datos de hasta 115 kbps (Axalto, 2006).

9. **Velocidad de Reconocimiento -** La velocidad sólo está limitada por los estándares ISO actuales sobre velocidades de entrada/salida.

10. **Características Propietarias** – Incluye aquellas características adicionales que son propietarias del tipo de tarjeta, como por ejemplo, el tipo de sistema operativo y el software de desarrollo.

11. **Potencia de procesamiento** – Las versiones anteriores utilizaban un procesador de 8-bits corriendo a 16 Mhz con o sin procesador matemático para una encriptación rápida. La tendencia actual es hacia los controladores de 32-bits tipo RISC corriendo de 25 a 32 Mhz.

12. **Fuente de energía** – Casi todas utilizan 5 voltios de alimentación, pero existen lectores que soportan tarjetas con otros voltajes comunes tal como el lector *ACR38* de la empresa *Advanced Card Systems Ltd*. que soporta tarjetas con voltajes de 5V, 3.3V y 1.8V (ACS, 2006b).

13. **Equipo de Soporte Requerido –** Para las aplicaciones del anfitrión (host), se requiere un lector, esto es, un dispositivo de lectura y escritura, que cuente con reloj asíncrono, interfaz de comunicación, ya sea serial o USB y fuente de alimentación.

2.5.2 Capacidad y desempeño contra costo

Al incrementar los niveles de procesamiento, flexibilidad y memoria, también se incrementa el costo de la tarjeta inteligente. Hasta el momento, las tarjetas para funciones simples son las que mantienen la mejor solución en cuanto a costo-beneficio (Cardlogix, 2004). Se deben tomar en cuenta estos factores al momento de decidir el tipo de tecnología de tarjetas inteligentes que se empleará para la aplicación. La figura 2.1 muestra en forma gráfica este comportamiento (Cardlogix, 2004):

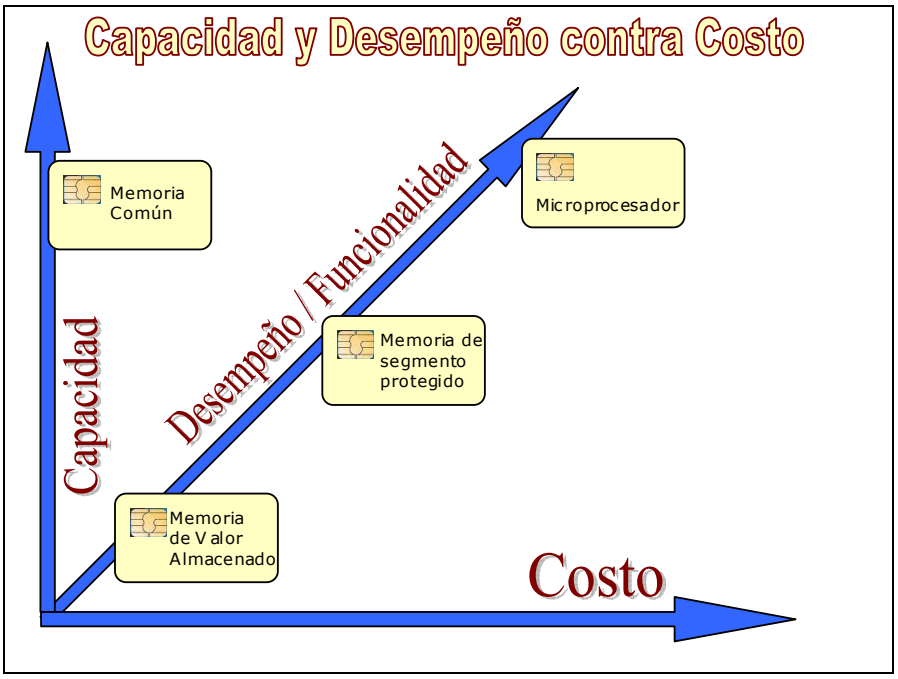

Figura 2.1 Gráfica de capacidad y desempeño vs. costo

Según Jurgensen & Guthery (2002), en el año 2002 una tarjeta inteligente costaba entre 1 y 20 dólares estadounidenses. Como se mencionó anteriormente, hoy en día existen tarjetas que cuestan desde pocos centavos de dólar estadounidenses hasta más de 20 dólares. Este costo depende principalmente de la capacidad de memoria y de la funcionalidad del software incluido en ella. El software puede variar desde un sistema operativo rudimentario que incluye sistema de archivos, comunicación, autorización, encriptación y control de acceso, hasta un sistema operativo más sofisticado que soporte el uso de lenguajes avanzados o lenguajes de interpretación (tales como C, Java o Basic), los cuales permiten agregar nuevas aplicaciones a la tarjeta aún después de ser expedidas (ID Edge, 2002).

2.5.3 Tecnologías de memorias

Una de las partes fundamentales que componen el chip de las tarjetas inteligentes es el módulo de memoria. Esta puede venir incluida en la misma pieza de silicio (chip) o puede encontrarse de manera separada al microprocesador. Existen varios tipos o

tecnologías de memorias y cada una tiene características particulares. El chip de las tarjetas puede contener uno o más de estos tipos de memoria. Barr (2001) describe las tecnologías de memorias más comunes actualmente y las clasifica en los siguientes tres tipos:

1) **Memorias tipo RAM**

Memoria de Acceso Aleatorio (*Random Access Memory*). Esta memoria es volátil (los datos se pierden si se interrumpe la energía que alimenta el chip) y permite tanto lectura como escritura de los datos. Su uso principal es para almacenar datos temporales que ocupa el microprocesador al estar operando. Las tarjetas inteligentes utilizan este tipo de memoria para almacenar datos temporales durante la ejecución de las aplicaciones. Como la cantidad de espacio de memoria RAM es limitada debido a los costos y al área que ocupa en el chip, los programadores deben considerar minimizar su uso por medio de la optimización de las variables y algoritmos que se incluyan en la aplicación. Se han desarrollado dos familias de este tipo de memoria: RAM estática (SRAM) y RAM dinámica (DRAM). La diferencia principal es la duración de vida de los datos almacenados. La memoria SRAM retiene su contenido mientras se le esté aplicando alimentación de corriente. Si ésta se interrumpe por un instante, su contenido será eliminado. En cambio los datos de la memoria DRAM permanecen solamente una fracción de tiempo (en el orden de milisegundos) aunque se siga suministrando corriente de alimentación. Para lograr que los datos permanezcan almacenados en este tipo de memoria, se requiere de un circuito controlador, el cual escribe de nuevo el contenido periódicamente para evitar que se pierda. La memoria DRAM es más lenta que la SRAM, pero es mucho más barata.

2) **Memorias tipo ROM**

Este tipo de memoria puede retener los datos almacenados incluso cuando se le suspende la corriente de alimentación. Se les conoce como “Memoria de Sólo

Lectura" (*Read Only Memory*). Las primeras memorias ROM eran dispositivos alambrados de tal manera que contenían un conjunto de instrucciones y el contenido de la memoria tenía que ser especificada antes de producir el chip. Conforme avanzó el desarrollo tecnológico de circuitos integrados, se desarrollaron nuevas variedades de memorias ROM resultando en los siguientes tipos:

a) **Mask-ROM** (*ROM enmascarada*). En este tipo de memoria se especifican los datos que contendrá antes de su producción, los cuales no podrán ser modificados posteriormente. Esta memoria es barata en alta producción comparada con las demás tecnologías, debido a que requiere menos silicio. Sin embargo, el tiempo de producción de un dispositivo que utiliza este tipo de memoria puede llevar mucho tiempo, ya que se debe esperar a la fabricación del lote de ese chip en particular para que el fabricante de la tarjeta pueda realizar pruebas. Si se requiere hacer cambios en el contenido de los datos, se debe realizar el proceso de nuevo. A esta tecnología de memorias, al igual que las PROM, se les denomina OTP (*One Time Programmable*) ya que sólo pueden ser programadas una sola vez. La memoria ROM es donde se almacena el sistema operativo de las tarjetas inteligentes, el cual, como se verá más adelante, contiene rutinas para realizar la comunicación y el manejo de archivos, así como algoritmos de encriptación para el manejo de la seguridad. Tales rutinas son generalmente instrucciones codificadas en lenguaje ensamblador.

b) **PROM** – Memoria Programable de Sólo Lectura (*Programmable Read Only Memory*). Representa un avance en cuanto a la memoria ROM, ya que puede ser programada por el usuario por medio del "quemado de fusibles" internos que representan los datos. Una vez programada ya no puede ser alterada, por lo que se debe utilizar otro chip cuando se requieran hacer cambios en los datos. Esta tecnología, a diferencia de las memorias ROM, permite que el usuario programe la información que contendrá y no el fabricante,

disminuyendo así el tiempo de producción del dispositivo.

c) **EPROM –** Memoria Programable de Sólo Lectura Borrable (*Erasable Programmable Read Only Memory*). Es similar a la memoria PROM, pero tiene la ventaja de que la información puede ser borrada si se expone por cierto período de tiempo a una fuente de luz ultravioleta a través de una ventana en su encapsulado, para posteriormente ser reprogramada. Sin embargo, esta tecnología no tiene impacto en las tarjetas con chip debido a que el diseño de estas no permite el uso de la ventana para su borrado, por lo que para esta aplicación tiene la misma función que las memorias PROM.

3) **Memorias Híbridas** – Conforme la tecnología de las memorias va avanzando, la línea que divide las ROM de las RAM se ha ido desvaneciendo. Ahora algunos tipos de memoria combinan ambas características haciendo que no se inclinen del todo a algún tipo, por lo que se les conocen como memorias híbridas. A éstas se les puede leer y escribir tal como sucede con la memoria RAM, pero mantienen su contenido aunque se les interrumpa la alimentación eléctrica, como las de tipo ROM. Los tipos de memorias que pertenecen a las híbridas son las siguientes:

a) **EEPROM** – Memoria Programable de Sólo Lectura Borrable Eléctricamente (*Electrically Erasable Programmable Read Only Memory*). Son similares a las EPROM, pero con la diferencia de que en vez de requerir la exposición de luz ultravioleta para borrar los datos, las EEPROM lo hacen por medio de señales eléctricas, lo cual permite que el mismo dispositivo que lee los datos pueda programarlos y borrarlos. Con estas características el usuario puede realizar los cambios que sean necesarios utilizando el mismo chip, reduciendo así el tiempo y los costos de producción. Cada byte de la EEPROM debe borrarse primero, antes de volver a escribir sobre él. Las tarjetas inteligentes utilizan este tipo de memoria para almacenar datos variables, tales como números de cuentas, puntos de membresía, cantidad de dinero electrónico y datos personales.

b) **FLASH –** Combina las mejores características de las memorias mencionadas hasta el momento. Tienen alta densidad, son de bajo costo, no volátiles, rápidas (para leer, pero no para escribir), y son borrables eléctricamente. Son muy similares a las memorias EEPROM, a diferencia de que las FLASH permiten borrar y escribir múltiples locaciones de memoria en una misma operación. Además, son más populares que las memorias EEPROM, desplazando a varios tipos de ROM.

c) **NVRAM** (Memoria RAM No-Volátil) – Esta memoria es físicamente muy diferente de las memorias ROM e Híbridas mencionadas anteriormente. Es básicamente una memoria tipo SRAM pero con una batería de respaldo. Cuando se le suministra alimentación eléctrica, opera como una SRAM común. Cuando se le interrumpe el suministro eléctrico, utiliza el suministro de la batería para retener sus datos. Esta característica la hace más costosa que las memorias SRAM.

2.5.4 Proceso de comunicación

Jurgensen & Guthery (2002) detallan el proceso de comunicación que se lleva a cabo entre la tarjeta inteligente y el lector. Ellos mencionan que tal proceso comienza a partir del momento en que la tarjeta es insertada correctamente en el lector. El lector no aplica la señal de voltaje de alimentación en los contactos del chip de la tarjeta sino hasta que detecte que la tarjeta ha sido insertada correctamente para que los contactos coincidan con las terminales del lector (por medio de unos sensores de alineación). De lo contrario, si se aplicara esta señal de alimentación a los contactos erróneos, el chip pudiera sufrir daños permanentes.

Una vez que el lector aplica voltaje de alimentación al chip de la tarjeta, los demás contactos se mantienen en los estados que se muestran en la tabla 2.1.

Contacto	Estado
Vcc	Voltaje estable aplicado (5V.)
VPP	Sin Señal
RST	Estado - bajo
CLK	Frecuencia estable y apropiada
I/O	En modo “recepción”

Tabla 2.1 Estado inicial de los contactos del chip

El voltaje de alimentación Vcc inicial es de 5 Voltios. Aunque, puede ser cambiado una vez que se establece la comunicación, dependiendo de los voltajes de operación que soporte la tarjeta inteligente. Posterior a la aplicación de este voltaje, se manda la señal para inicializar la tarjeta. Esto se lleva a cabo cambiando el estado del contacto RST a un estado alto. Durante la inicialización, la tarjeta puede realizar varias operaciones internas, pero siempre debe responder al lector con por lo menos el primer byte del valor de una cadena de caracteres llamado “Aknowledge To Reset” (ATR) antes de que ocurran 40,000 ciclos de reloj. El ISO/IEC 7816-3 define la estructura del ATR y menciona que consiste de 33 o menos caracteres, los cuales se utilizan para establecer varios parámetros con el lector al inicializar la tarjeta y establecer un canal de comunicación física entre la tarjeta y el lector. Entre estos parámetros se encuentran el formato de los bits (si considera la presencia de voltaje como un 1 o un 0 lógico), el orden en que se transfieren (si primero el más significativo o primero el menos significativo), información del fabricante y del emisor de tarjetas, el tipo de protocolo de transmisión que utilizará (T=0 o T=1) y un caracter para comprobación de error.

La figura 2.2 muestra un diagrama con los estados que se presentan en el lector cuando se inicializa una tarjeta y al hacer peticiones de ejecución de comandos.

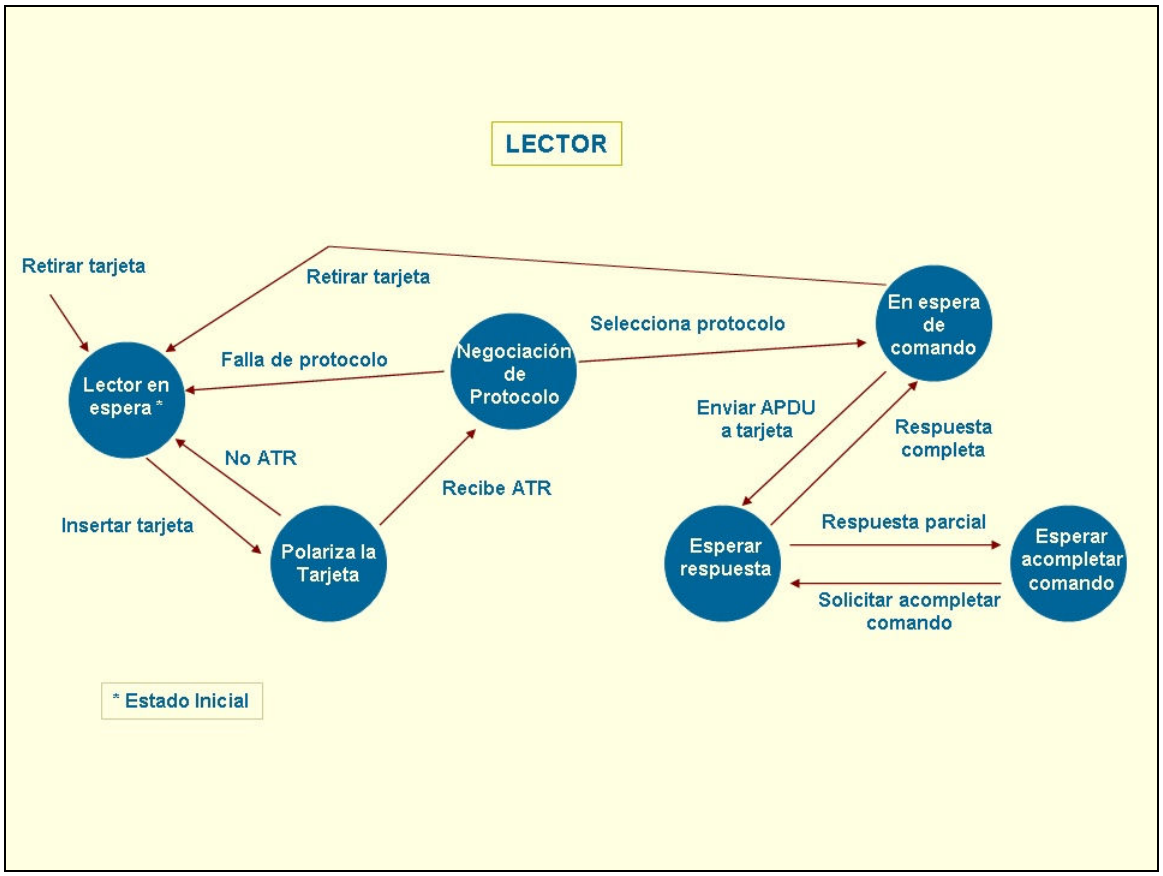

Figura 2.2 Diagrama de estados del lector

El lector permanece en espera hasta que se inserte una tarjeta inteligente. Al insertar una tarjeta, el lector le aplica el voltaje de alimentación y cambia los estados de los contactos como se mencionó anteriormente y espera la cadena ATR como respuesta a la inicialización. Cuando la tarjeta responde con el ATR, se establece la negociación del protocolo de comunicación y otros parámetros como la velocidad y formatos de transmisión. Ya negociado el protocolo y los parámetros, el lector permanece en espera de peticiones de comandos desde la aplicación. Al recibir estas peticiones, el lector los envía a la tarjeta en forma de APDUs (Unidades de Datos de Protocolo de Aplicación), los cuales son la unidad básica de intercambio entre la aplicación y la tarjeta inteligente, y espera respuesta por parte de la tarjeta para cada comando solicitado. Una vez recibida la respuesta, permanece de nuevo en espera para enviar nuevos comandos a la tarjeta. No se puede solicitar otro comando a la tarjeta sino hasta que ésta responda al solicitado anteriormente. Este proceso de comunicación se lleva a cabo en modalidad maestro-

esclavo en donde la tarjeta se encuentra en espera (esclavo) hasta que el lector le solicita ejecutar un comando (maestro).

El diagrama de la figura 2.3 muestra el mismo proceso pero visto desde el lado de la tarjeta inteligente. Se puede observar que la tarjeta permanece sin polarización en su estado inicial. Una vez que se inserta al lector, ésta prepara el ATR y se lo envía al lector tal como se mencionó anteriormente. Luego, la tarjeta inteligente permanece en espera hasta que recibe por parte del lector, la petición para ejecutar comandos por medio de un APDU. La tarjeta inteligente procesa el APDU y regresa la respuesta al lector para volver de nuevo a su estado de espera. Si un comando no puede ser procesado por la tarjeta inteligente, devuelve un código de error al lector y pasa a un estado donde no le permite continuar con la comunicación, por lo que es necesario retirar la tarjeta y volverla a insertar en el lector.

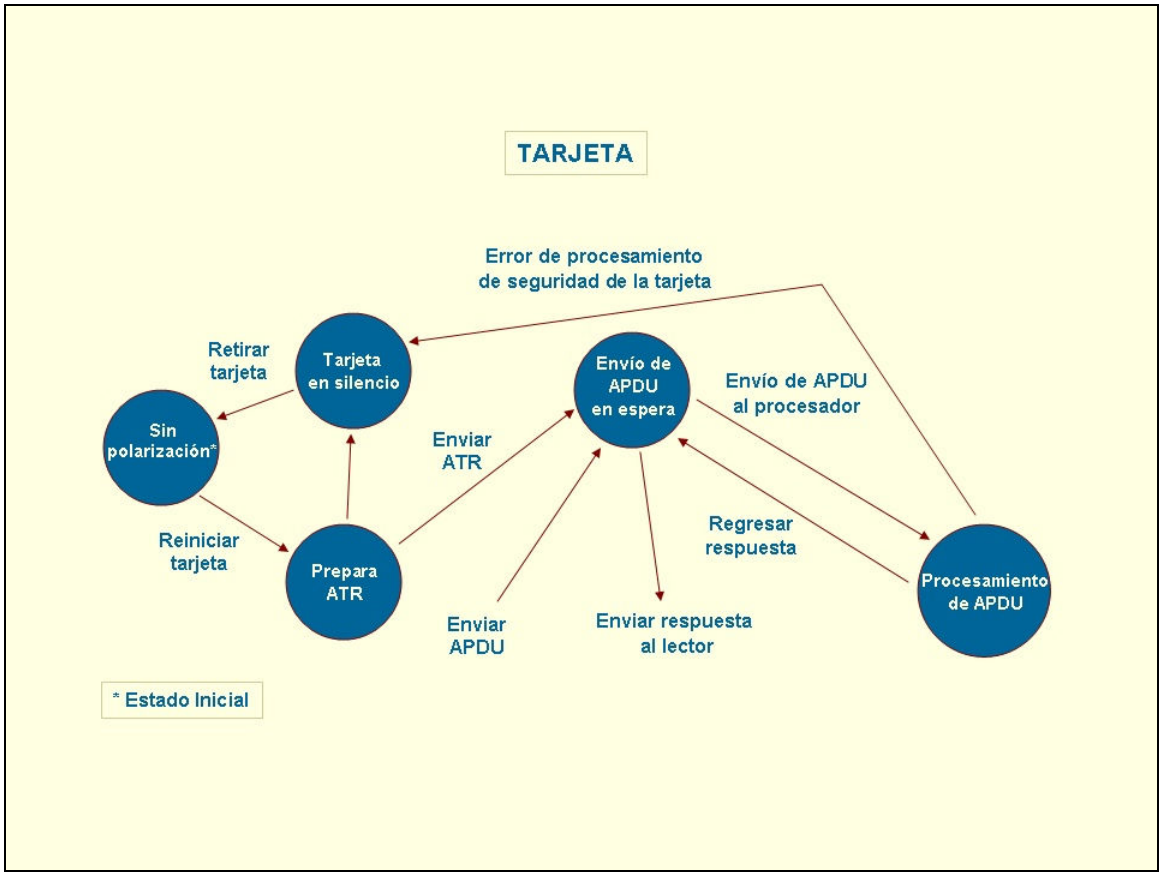

Figura 2.3 Diagrama de estados de la tarjeta inteligente

En un APDU, se pueden transferir comandos completos a la tarjeta inteligente con parámetros o se puede recibir de la tarjeta una respuesta completa (Di Giorgio, 1995).

La estructura de un APDU, según el estándar ISO/IEC 7816, consiste principalmente de un encabezado de 4 bytes, seguido de contenido adicional de longitud variable. Los APDU pueden contener, ya sea un mensaje de ejecución de instrucción (comando) que envía la aplicación a la tarjeta inteligente, o un mensaje de respuesta que envía la tarjeta inteligente a la aplicación. La tabla 2.2 muestra la estructura del APDU.

Encabezado (4 bytes)	Contenido adicional
CLA INS P1 P2	[Lc] [Datos] [Le]

Tabla 2.2 Estructura de un APDU

El encabezado consta de los siguientes 4 campos (de un byte de longitud cada uno):

- **CLA** – Indica la clase de instrucción. Con este campo se puede especificar en que grado las instrucciones cumplen con el estándar ISO/IEC 7816-4 o si son instrucciones propietarias.
- **INS** – Indica el código de instrucción.
- **P1** – Primer parámetro.
- **P2** – Segundo parámetro.

El contenido adicional incluye los siguientes campos:

- **Lc** – Indica la longitud en bytes del campo de datos.
- **Datos** – Contiene los datos que requiere la instrucción o el contenido del mensaje.
- **Le** – Se utiliza para indicar el número máximo de bytes que se espera en un mensaje de respuesta.

En el siguiente ejemplo, se presenta la instrucción “SELECT FILE”, la cual está definida en el estándar ISO/IEC 7816-4 para seleccionar el archivo de datos que estará activo

durante la ejecución de instrucciones subsecuentes. Tiene la estructura que aparece en la tabla 2.3.

CLA	INS	P1	P2	Lc	Datos
80	A4	00	00	02	Identificador del archivo

Tabla 2.3 Ejemplo de estructura de un APDU

Los valores que se muestran están escritos en formato hexadecimal. El valor 80 de CLA indica que la instrucción es de clase propietaria y el valor A4 del campo INS indica que el código de instrucción equivale a "SELECT FILE". P1 y P2 son los parámetros que indican el tipo de archivo y la forma en que éste se seleccionará, ya sea por medio de una estructura lógica de árbol o por medio de un identificador único de archivo. En este caso, indican que utilizará el identificador único de archivo. Lc indica que el campo de datos (el identificador de archivos) tiene una longitud de 2 bytes. Para más información sobre la estructura de un APDU, favor de consultar Cardwerk (2006).

2.5.5 Software de las tarjetas inteligentes

Para el desarrollo de aplicaciones que utilizan tarjetas inteligentes, se requiere el uso de software, el cual forma parte de los elementos involucrados en la aplicación. Jurgensen & Guthery (2002) clasifican el software de la siguiente manera:

1. **Software del Host**

   La mayor parte del software que se utiliza en aplicaciones con tarjetas inteligentes reside en el lado de la aplicación, es decir, en la terminal que se comunica con la tarjeta inteligente, a la cual llamaremos host. Este software está escrito generalmente para computadoras personales que accedan las tarjetas existentes, incorporándolas a sistemas mayores.

En algunas aplicaciones el software del host soporta el uso de distintos tipos de tarjetas inteligentes, aunque existen algunas que están diseñadas exclusivamente para soportar un solo tipo.

El software del host generalmente incluye:

a. Software de aplicación de usuario final.
b. Software a nivel de sistema que soporte la comunicación entre el lector de tarjetas y la plataforma utilizada.
c. Software de nivel de sistema que soporte el uso de la tarjeta requerida para la aplicación.
d. Software necesario para la administración de la infraestructura de las tarjetas inteligentes.

Este software se desarrolla generalmente en lenguajes de alto nivel como C, C++, Java, BASIC, COBOL, Pascal y Fortran y se enlaza con librerías y controladores (*drivers*) disponibles comercialmente, para acceder a los lectores y a las tarjetas. Además, aprovecha las capacidades computacionales y de almacenamiento de información intrínsecas de las tarjeras inteligentes al hacer uso del envío de comandos hacia ella para obtener datos.

2. Software de la tarjeta

Es el software que se ejecuta en el circuito integrado de la tarjeta inteligente. Este software se centra más en el contenido de la tarjeta en particular. Provee servicios computacionales para las aplicaciones que quieran acceder sus contenidos y los protege de las aplicaciones que intenten accederlos de forma incorrecta. Implementa las propiedades de seguridad de datos y procesos y políticas de una tarjeta en particular. Este software se puede clasificar en:

a. Sistema Operativo de la Tarjeta o COS (por sus siglas en inglés de *Card Operating System*)

b. Utilerías

c. Aplicaciones

Para algunas aplicaciones no se requiere software especial para la tarjeta, es suficiente con el software genérico que viene incluido en ella. Cuando se requiere una aplicación en específico, se escribe generalmente en lenguaje ensamblador para la arquitectura del chip empotrado o se utiliza un lenguaje de alto nivel que es interpretado directamente en la tarjeta o compilado en un lenguaje de ensamblador para la tarjeta y luego cargado en ella. La familia de tarjetas *Cyberflex Access* de la empresa Axalto permite la carga de applets desarrollados en lenguaje Java, que se ejecutan en la misma tarjeta usando una máquina virtual que los interpreta (Axalto, 2006). En cambio, las tarjetas *ACOS2* de la empresa *ACS* permiten ejecutar solamente los 13 comandos definidos en su sistema operativo, los cuales realizan funciones relacionadas con la autenticación, manejo de archivos y transacciones monetarias (ACS, 2006).

Otra manera en que se clasifica el software de la tarjeta es en software de aplicación y software de sistema:

1. **Software de aplicación**

Utiliza las capacidades computacionales y de almacenamiento de datos de la tarjeta como las de cualquier otra computadora y relativamente no se toman en cuenta (o no son de tanta importancia) las propiedades de integridad y seguridad de los datos de la tarjeta. Está más enfocado a la persona que utiliza la tarjeta que la aplicación que la accede. Este software se utiliza para personalizar la tarjeta para cierta aplicación y contribuye a que ciertas funciones, que son del software del host, se transfieran a la tarjeta para lograr más eficiencia (mayor velocidad en la interacción entre el host y la tarjeta) o más seguridad (al proteger parte

propietaria del sistema).

2. **Software de sistema**

   Escrito en lenguaje de bajo nivel para la tarjeta en particular y se utiliza para extender o reemplazar funciones básicas de la tarjeta. Utiliza y contribuye a mejorar las propiedades de integridad y de seguridad en los datos de la tarjeta.

A diferencia del software de una computadora común, donde depende del soporte a los servicios que la rodean en su contexto, el software de las tarjetas inteligentes empieza asumiendo que el contexto en el que se encuentra es hostil y es de desconfiar. Hasta que no se presente la evidencia convincente de lo contrario, las tarjetas no confían en el host en el cual se han insertado, y al igual, el host no confía en las tarjetas que están insertadas. Un programa de tarjeta sólo confía en él. Todo lo que esté fuera del programa se tiene que probar como confiable antes de que el programa interactúe con él.

Un programa de host tiene que completar dos tareas antes de que empiecen a realizar transacciones con la tarjeta. Primero, tiene que asegurarse de que la tarjeta con la cual está interactuando es auténtica. Segundo, tiene que convencer a la tarjeta de que él es auténtico. No hay transacción hasta que se realice esta confianza mutua.

2.6 Estándares y especificaciones

Las precursoras de las tarjetas inteligentes que conocemos actualmente son las tarjetas de crédito que se utilizaron originalmente como una forma de identificación en transacciones comerciales. Estas representaron un gran crecimiento en las formas de identificar a clientes a quienes no se les conocía su identidad para poder otorgarles

crédito. Con el uso de esta tarjeta los clientes podían mostrar su certificado de identidad y una situación financiera avalada por un banco u otra institución.

Conforme las tarjetas de crédito eran aceptadas y utilizadas en varios establecimientos comerciales, se creó la necesidad de que fueran operables entre diferentes emisores de tarjetas de crédito y equipos en distintos comercios de todo el mundo. Esta tarea para lograr la interoperabilidad, llevó al establecimiento de estándares internacionales que aplicaron primero a las tarjetas y posteriormente a los lectores y el entorno donde operan. La organización que estableció tales estándares es la Organización de Estándares Internacionales (ISO) y, en algunos campos de actividades técnicas, la Comisión Electrotécnica Internacional (IEC) colabora con ISO en el desarrollo de estándares. De igual forma, el Instituto de Estándares Nacional Americano (ANSI) ayuda a establecer estándares para las tarjetas inteligentes.

La estandarización de las tarjetas inteligentes es un proceso continuo que involucra a muchas organizaciones donde cada una se enfoca a sus propias causas. Sin embargo, los estándares y las especificaciones son las claves para lograr interoperabilidad. Los estándares para las tarjetas inteligentes definen principalmente sus propiedades físicas, las características de comunicación y los identificadores de aplicación del chip empotrado y sus datos. Las propiedades específicas a las aplicaciones han estado siempre en debate entre grandes grupos y organizaciones que crean sus propias especificaciones. En muchos casos, estas especificaciones se logran convertir en estándares. Para que las tarjetas inteligentes tengan interoperabilidad, deben cumplir con los estándares en sus diferentes partes, desde las características físicas de la tarjeta hasta las características de los sistemas que las implementan.

El conjunto de estándares ISO 7816 es el más conocido y el más utilizado en el ámbito de las tarjetas inteligentes de propósito general, pero no es el único que existe. Existen estándares para el uso de estas tarjetas en diferentes aplicaciones como en el sector salud, transporte, servicios bancarios, comercio electrónico e identidad, entre otros. También existen estándares para nuevos tipos de tarjetas inteligentes como las de sin contacto.

Debido a que las tarjetas inteligentes siempre forman parte de un sistema mayor, están sujetas a varios estándares sobre el procesamiento de información, tales como conjuntos de caracteres, códigos de países, representaciones monetarias, criptografía y estándares relacionados con alguna región o incluso a nivel nacional e internacional (Jurgensen & Guthery, 2002). Algunos organismos cuentan con especificaciones que involucran a las tarjetas inteligentes. Tal es el caso del grupo PC/SC (Personal Computer / Smart Card), el cual se conforma de varias empresas, entre ellas fabricantes de tarjetas inteligentes como Bull, Schlumberger, Gemplus y otras empresas como Microsoft, Toshiba y Philips Semiconductors, que desarrolló la especificación que tiene su mismo nombre y que busca su estandarización (PC/SC, 2006). Para más información sobre esta especificación, ver anexo C.

Son muchos los estándares y especificaciones que involucran a las tarjetas inteligentes y constantemente se hacen adaptaciones y mejoras a los mismos. Di Giorgio (1995) menciona que una manera de entender la variedad de estos estándares es organizarlos en dos tipos: Estándares horizontales y estándares verticales.

2.6.1 Estándares y especificaciones horizontales

Son aquellos que pueden ser utilizados en cualquier aplicación, esto es, no son específicos a un sistema, sino que definen aspectos que las aplicaciones pudieran adoptar. Algunos ejemplos de los más utilizados son:

a. **ISO/IEC 7816** – Es una serie de estándares internacionales para tarjetas con circuito integrado que utilizan contactos para la comunicación con el lector. Estos estándares son basados en los ISO 7810 e ISO 7811, los cuales definen las características físicas de tarjetas de identificación. Entre las características que definen los estándares 7816 se encuentran las características físicas, posición de los contactos del chip, señales electrónicas, protocolos de comunicación, comandos entre industrias, estructuras de archivos, identificadores de aplicaciones, comandos para operaciones de seguridad, comandos para

administración de la tarjeta, lenguajes de consultas y verificación por métodos biométricos (Cardlogix, 2001). Para más información sobre la familia de estándares ISO/IEC 7816, consulte el anexo C.

b. PC/SC – Es una especificación desarrollada por varias empresas, entre ellas fabricantes de tarjetas inteligentes como Axalto, Gemplus y otras empresas como Microsoft y Philips. Esta especificación tiene como objetivos principales el facilitar la integración de tarjetas inteligentes con los ambientes de computadoras personales, permitir la interoperabilidad entre distintos tipos de tarjetas inteligentes y lectores en sus diferentes niveles, facilitar el uso de productos y componentes de múltiples fabricantes (neutralidad entre vendedores), permitir la interoperabilidad entre componentes de varias plataformas (neutralidad entre plataformas) y el uso de los avances tecnológicos sin que se requiera volver a escribir el software de aplicación (neutralidad entre aplicaciones) (PC/SC, 2006). El sistema propuesto en este trabajo utiliza esta especificación como capa intermedia entre las tarjetas inteligentes, los lectores y las aplicaciones. Para más información de esta especificación, consulte el anexo C.

c. OCF – Open Card Framework es un marco de desarrollo estándar basado en Java, desarrollado por un consorcio de industrias, entre ellas fabricantes de tarjetas inteligentes como Bull, Gemplus y Schlumberger, además de otras importantes como IBM y Sun Microsystems, que provee soluciones de interoperabilidad en tarjetas inteligentes a través de varias plataformas de hardware y software. Establecido como un estándar abierto, provee una arquitectura y un conjunto de interfaces de programación de aplicaciones (APIs) que le permite a los desarrolladores de aplicaciones construir y utilizar soluciones para tarjetas inteligentes en ambientes compatibles con Open Card (Open Card Consortium, 1998).

d. **JavaCard** – Es la especificación de una plataforma que provee las bases para lograr interoperabilidad entre fabricantes y seguridad en ambientes de tarjetas inteligentes. Con JavaCard se pueden desarrollar aplicaciones utilizando applets, los cuales se pueden ejecutar en tarjetas inteligentes que cumplan con esta especificación logrando así que el desarrollo de tales aplicaciones sea independiente del hardware y del fabricante de tarjetas. Permite que una tarjeta contenga varias aplicaciones y que puedan coexistir entre ellas en forma muy segura, además de que el ambiente de desarrollo utiliza las ventajas del lenguaje Java como por ejemplo, la programación orientada a objetos, seguridad, portabilidad y un gran número de clases disponibles para el desarrollo de aplicaciones. Actualmente se encuentra disponible la versión 2.2.2 de esta especificación (Sun Microsystems, 2006).

2.6.2 Estándares y especificaciones verticales

Los estándares verticales son específicos al tipo de aplicación en que se utilizan las tarjetas inteligentes. Entre algunos de estos estándares se encuentran los siguientes:

a. **Mondex** – Dinero digital que utiliza tarjetas inteligentes solamente (no maneja dinero fuera de las tarjetas).

b. **VisaCash** – Tarjeta de débito que mantiene un rastreo de las tarjetas en el servidor.

c. **Estándares EMV -** Las empresas Europay, MasterCard y Visa formaron la compañía EMV y crearon las especificaciones para tarjetas con circuito integrado para sistemas de pago. Estas especificaciones están relacionadas con el ISO 7816 y crean una base técnica común para tarjetas e implementación de sistemas de valor almacenado.

d. MPCOS-EMV – Tarjetas de propósito general que implementan un tipo propietario de moneda o "tokens".

e. Estándares FIPS - Estándares de Procesamiento de Información Federal (*Federal Information Processing Standards*). Estos estándares son desarrollados por la División de Seguridad Computacional dentro del Instituto Nacional de Estándares y Tecnología (NIST). Los estándares FIPS se diseñaron para proteger recursos federales incluyendo sistemas de computadores y telecomunicaciones. Los siguientes son ejemplos de algunos estándares FIPS que aplican a las tecnologías de las tarjetas inteligentes pertinentes a firmas digitales, encriptación avanzada y requerimientos de seguridad para módulos criptográficos (Cardlogix Corp, 2001; Smart Card Alliance, 2004).

i. FIPS 140(1-3) – Requerimientos de seguridad pertinentes a áreas relacionadas al diseño seguro e implementación de módulos criptográficos, incluyendo su especificación, roles, servicios y autentificación, seguridad física, ambiente operacional, manejo de llaves criptográficas, interferencia y compatibilidad electromagnética (EMI/EMC), entre otros.

ii. FIPS 186-2 – Especifica un conjunto de algoritmos utilizados para generar y verificar firmas digitales. Entre estos algoritmos se encuentran DSA, RSA, y ECDSA.

iii. FIPS 201 – Se encuentra actualmente en proceso. Cubrirá todos los aspectos de las tarjetas multifunción utilizadas en sistemas de administración de identidad a través del gobierno de EE.UU.

2.7 Conclusión

Este capítulo presentó un panorama amplio sobre la tecnología de las tarjetas inteligentes, lo cual ha sido una aportación bibliográfica muy importante para el diseño del sistema propuesto. Los antecedentes históricos permitieron ver cómo, de utilizarse como una simple tarjeta de identificación, las tarjetas inteligentes han evolucionado a tal grado que actualmente se utilizan en muchos tipos de aplicaciones donde se requieren mecanismos de autenticación, identificación y almacenamiento de información en forma segura.

El implementar tarjetas inteligentes como parte esencial de un sistema de almacenamiento y procesamiento de información sensible, permitirá contar con un mecanismo de autenticación e identificación muy seguro, confiable, fácil de transportar y de usar, para la realización de trámites y consulta de información relacionada a expedientes curriculares.

Capítulo III. Seguridad de la información

3.1 Introducción

Hasta hace muy poco, para la mayoría de las organizaciones, la seguridad era cuestión de proteger el acceso a los datos corporativos. Lo importante era impedir que personas no autorizadas tuvieran acceso a información exclusiva o que pudieran provocar algún daño a tal información. A principios de la década de 1980, los sistemas de información evolucionaron de tal manera que se incorporaron a redes en donde la información se podía compartir. Esto trajo consigo una serie de vulnerabilidades ya que, desde el momento que un sistema se encuentra en red, es potencialmente susceptible a ser atacado. Junto con este crecimiento en los sistemas en red surgió también el crecimiento de una nueva industria dedicada a proteger todos esos puntos de acceso vulnerables a ataques. Lo anterior refiere a la industria relacionada con la seguridad de la información.

Una manera de comenzar este tema es definiendo lo que es seguridad. Cardlogix (2004) la define de la siguiente manera: "Seguridad es básicamente la protección de algo que tiene valor para garantizar que no sea robado, perdido o alterado".

La seguridad en los datos implica aspectos tanto técnicos como sociales. El primero involucra el cómo y qué tanto aplicar seguridad a cierto costo razonable. El aspecto social trata temas como la libertad del individuo, preocupaciones sociales, estándares legales y cómo la necesidad de privacidad las intercepta.

Seguridad de la Información

"La seguridad de la información es la aplicación de medidas que procuren la seguridad y privacidad de los datos por medio del manejo de su almacenamiento y distribución" (Cardlogix, 2004).

El concepto de seguridad se está volviendo cada vez más sofisticado. En lugar de limitarse a pensar en barreras de seguridad para proteger la información, se empieza a pensar mucho más en los principios subyacentes que se deben aplicar a la información y a los servicios que necesitamos proteger y a los cuales se quiere conceder acceso. Estos principios se han aplicado gracias a los mecanismos de seguridad en los datos que han surgido a raíz de esta problemática.

3.2 Elementos de la seguridad de los datos

En el proceso de la seguridad de los datos intervienen cuatro elementos importantes que se describen a continuación (Cardlogix, 2001):

1. **Hardware** – Incluye todo lo tangible involucrado en el manejo de la información como servidores, dispositivos de almacenamiento masivo redundantes, líneas y canales de comunicación segura, tarjetas inteligentes y dispositivos remotos que funcionan como interfaces entre el usuario y las computadoras.

2. **Software** – Es todo lo intangible que tiene relación con los datos a proteger. Incluye los sistemas operativos, sistemas de administración de bases de datos, programas de comunicación y de seguridad.

3. **Datos** – Es el elemento que se quiere proteger. Puede incluir desde archivos sencillos hasta bases de datos grandes.

4. **Personal** – Incluye a toda persona que tenga de alguna forma, relación con los datos en cuestión. Esto incluye a los usuarios y generadores de datos, al personal profesional, personal de oficina, personal administrativo y personal técnico.

3.3 Mecanismos para la seguridad de los datos

Entre los servicios o mecanismos que permiten la construcción de una solución segura para el intercambio de información se encuentran los siguientes (Cardlogix, 2001; Nash, Duane, Joseph & Brink, 2002):

1. **Integridad de Datos** – Este mecanismo responde a la pregunta "¿Están mis datos intactos?". Por medio de éste, se asegura que los datos no se han perdido o han sido alterados durante su transferencia. Esto se realiza verificando las características del documento y la transacción. Tales características son inspeccionadas y confirman su contenido y correcta autorización. La integridad de los datos se logra por medio de criptografía electrónica la cual asigna una identidad única a los datos, como si fuera una huella digital. Cualquier intento de cambiar esta identidad es revelado y proporciona como resultado que el documento (datos) ha sido alterado.

2. **Autenticación –** Responde a la pregunta "¿Están los datos correctos y provienen de la entidad correcta?". Este mecanismo verifica las identidades de los usuarios, servidores, dispositivos y sistemas, para asegurar que son genuinos (Clark, 2003). A diferencia de la identificación, la autenticación no necesariamente requiere unicidad, esto es, sólo se exige que se valide una entidad previamente identificada, conservando así la privacidad, por lo que muchas personas, dispositivos o sistemas, pudieran autenticarse con una misma identidad compartida.

3. **Identificación** – Responde a la pregunta "¿Quién es o quién está enviando los datos?" Este proceso consiste en reconocer a un individuo en particular. Esto requiere que la persona o proceso encargado de verificar confronte la información presentada con todas las entidades que conoce, para comprobar con quién se está negociando.

4. **Aceptación** – A este mecanismo también se le conoce como "no repudio". Asegura la imposibilidad de eludir la responsabilidad en la generación o recepción de una transacción. Esto es, que ninguna de las partes involucradas en una transacción pueda negar el envío o la recepción de información. Este mecanismo utiliza generalmente esquemas basados en firmas digitales.

5. **Autorización y Delegación** – Responde a la pregunta "¿Puedo compartir de manera segura estos datos si así lo deseo?". El mecanismo permite asignar y administrar privilegios de acceso a usuarios y grupos adicionales. La autorización es el proceso de permitir acceso a datos en específico dentro de un sistema. Delegación es la utilización de un tercero para administrar y certificar cada uno de los usuarios de un sistema (Autoridades de Certificación).

6. **Auditoría y Bitácora** – Responde a la pregunta "¿Puedo verificar que el sistema esté funcionando?". Este mecanismo provee un monitoreo constante y funciones de asistencia a los sistemas de seguridad. Esta es una examinación y almacenamiento independiente de los registros y actividades para asegurar la conformidad con ciertos controles establecidos, políticas, procedimientos operacionales y recomendar cualquier cambio indicado en estos controles, políticas y procedimientos.

7. **Administración**- Este mecanismo permite la administración del sistema de seguridad. Es la vista general y el diseño de todos los elementos y mecanismos involucrados.

8. **Privacidad y Confiabilidad**- Este mecanismo asegura que sólo los emisores y receptores tienen acceso a los datos. Esto se realiza generalmente empleando una o más técnicas de encriptación para asegurar los datos. Confiabilidad es el uso de encriptación para proteger la información de accesos no autorizados. El texto original se convierte en texto cifrado por medio de un algoritmo para luego ser

descifrado de vuelta al texto original, utilizando el mismo método pero en forma inversa.

3.4 Criptografía

Como parte de los mecanismos para brindar seguridad en las transacciones, se encuentra el uso de la criptografía. Esta ciencia parte de la criptología (*criptos* = oculto, *logos* = tratado, ciencia) la cual es el arte de transformar mensajes claros a otros sin sentido alguno. La criptografía significa literalmente "escritura secreta" (Maturana, 2003) y viene del griego *criptos*= oculto, *grafía*= escritura, y aunque se pueden encontrar muchas definiciones de esta palabra, en el campo de la informática, se considera como más comunes las siguientes:

- "La criptografía es el método para convertir datos que están en forma entendible por los humanos a una forma modificada y después devuelta a su forma original, para que su acceso no autorizado sea difícil" (Cardlogix, 2001).

- "Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo sea en absoluto, para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado, sea capaz de entenderlo" (Maturana, 2003).

Los términos "encriptar", "codificar" y "cifrar" son utilizados indistintamente para referirnos a tales procesos para ocultar información.

Por otra parte, la criptografía se complementa con el criptoanálisis, el cual es la técnica de descifrar textos cifrados sin tener autorización de ellos, es decir, realizar una especie de criptografía inversa para tratar de encontrar las debilidades de los algoritmos y, por consiguiente, aportando a los criptólogos a reforzar sus técnicas de criptografía para hacerlos más seguros. A estos matemáticos e investigadores encargados de romper o encontrar debilidades en los algoritmos se les llama "criptoanalistas", mientras que a las

personas encargadas de inventar nuevos algoritmos se les llama “criptólogos”. Cuando no se lleva a cabo esta relación criptólogo-criptoanalista se puede tener como consecuencia lo que se conoce como “seguridad en la oscuridad”, lo cual significa que un algoritmo es utilizado sin ser probado previamente por expertos en el área y, por consiguiente, es vulnerable a ser descifrado. Es por esto que, siempre es necesario que un nuevo método de cifrado (algoritmo) se desarrolle a la par de un criptoanálisis para garantizar que nadie lo pueda romper (Nash *et al*., 2002; Fúster *et al*., 2001).

3.4.1 Tipos de criptografía

Existen dos tipos de algoritmos criptográficos: simétricos y asimétricos (Nash *et al*., 2002). En ambos tipos se utilizan llaves criptográficas. Una llave criptográfica es similar a una llave física que se usa para cerrar o abrir una puerta y para cada tipo de cerradura existe una llave con una forma específica que se ajusta a aquella. De igual forma cada algoritmo criptográfico necesita una llave con la extensión correcta (número de bits) y sólo la llave que tenga la longitud y el patrón correcto de bits, podrá permitir que el algoritmo descifre el mensaje.

3.4.1.1 Criptografía simétrica

Este tipo de criptografía es la más antigua y consiste en tomar el mensaje original como entrada y por medio de una llave generada de manera aleatoria por parte del emisor, se genera un mensaje cifrado. El término “simétrico” se refiere a que esta misma llave la utiliza el receptor para descifrar el mensaje (regresarlo a su forma original). La figura 3.1 muestra el proceso de cifrado y descifrado utilizando criptografía simétrica:

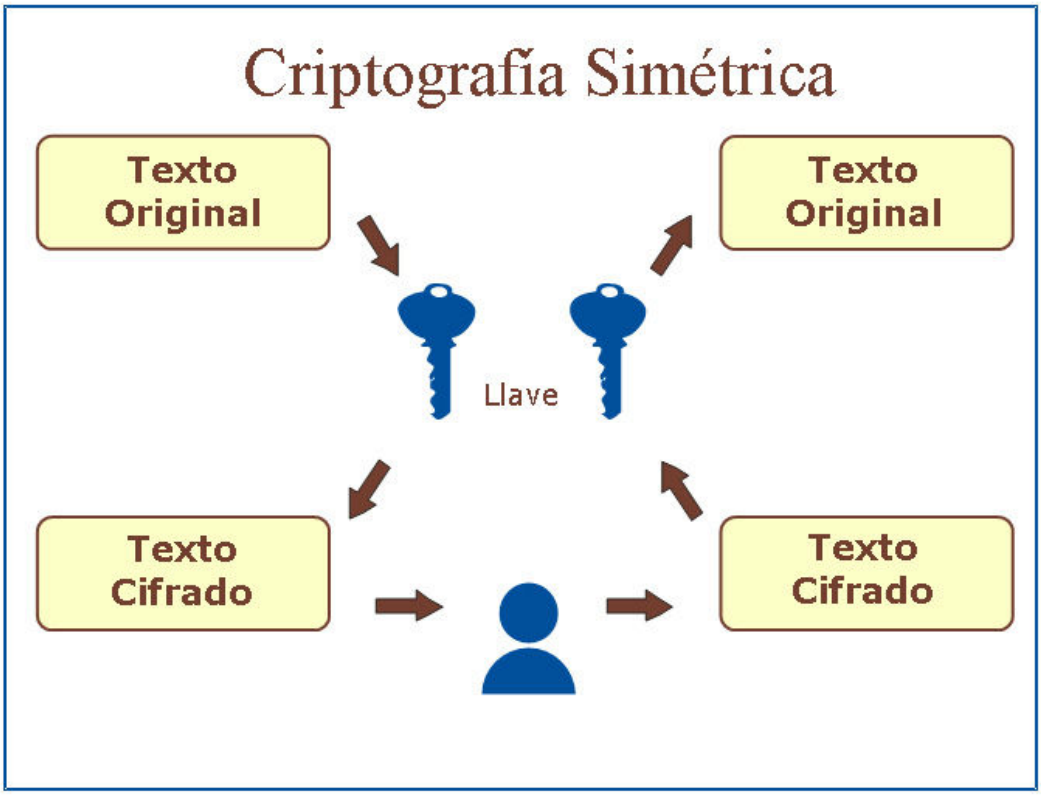

Figura 3.1 Criptografía simétrica

Este tipo de cifrado tiene las ventajas de que es rápido (comparado con el asimétrico) por lo que no impacta mucho en la carga al procesador del algoritmo. El texto cifrado es compacto, ya que generalmente tiene la misma longitud que el texto original y además, es un cifrado seguro. Sin embargo, este tipo de cifrado tiene algunas desventajas, entre ellas que la llave puede ser interceptada por intrusos, debido a que debe enviársele de alguna manera al receptor y esto provocaría que un intruso la capture y pueda descifrar el mensaje. Para cada mensaje que se cifra, se debe generar una nueva llave, dando como consecuencia que el número de llaves que se requiere generar en un ambiente de varios participantes, es aproximadamente el cuadrado del número de participantes, y por lo tanto, no tiene una buena escalabilidad en poblaciones numerosas. Para llevar a cabo esto se requiere una administración compleja de llaves.

3.4.1.2 Criptografía asimétrica

La criptografía asimétrica es aquella que emplea algoritmos asimétricos, esto es, que en lugar de usar una sola llave para la realización de la codificación y la decodificación (cifrado y descifrado), se utilizan dos llaves diferentes: una para cifrar, la otra para descifrar. Estas dos llaves son independientes, pero están relacionadas matemáticamente y siempre se generan juntas. El proceso para generarlas es más complejo que en el algoritmo simétrico. El receptor se encarga por anticipado de generar la pareja de llaves, llamadas pública y privada, y se debe encargar además, de proteger su llave privada. La llave pública la puede conocer todo el mundo ya que por medio de ésta, el emisor genera el mensaje cifrado. Lo importante aquí es que el mensaje no se puede descifrar con la llave pública con la que fue cifrado el mensaje, sino solamente con la llave privada que guarda en secreto el receptor. Dicho en otras palabras, lo que está cifrado con una llave sólo se puede descifrar con la otra. La figura 3.2 muestra el proceso de cifrado y descifrado utilizando criptografía asimétrica.

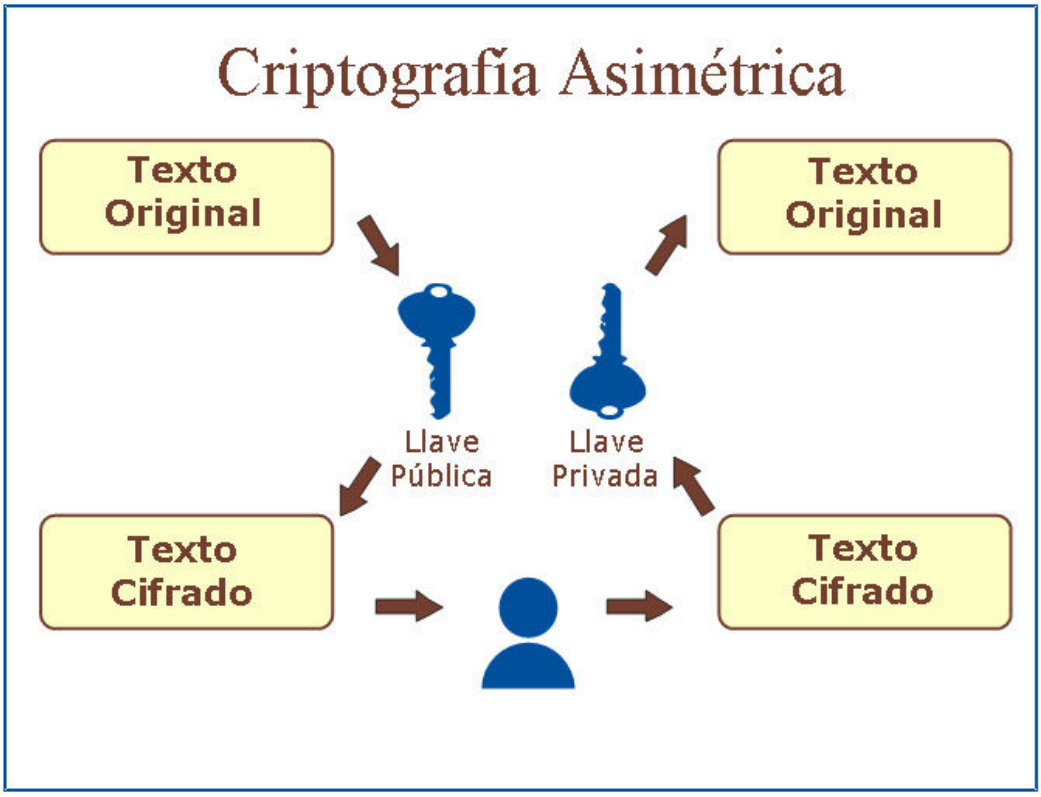

Figura 3.2 Criptografía asimétrica

Este tipo de cifrado es muy seguro y además tiene varias ventajas sobre la criptografía simétrica. Entre estas ventajas están que evita los problemas administrativos de llaves que presenta la criptografía simétrica, ya que cada persona necesita compartir solamente una llave: su llave pública. Además no exige una relación previa entre las partes para hacer el intercambio de documentos cifrados. Por otro lado, dado que no se necesita enviar una llave al receptor (como en el caso de la simétrica), la codificación no sufre por la interceptación de llaves y sólo se puede descifrar el mensaje si se cuenta con la llave privada. Otra ventaja es que soporta firmas digitales y aceptación. Sin embargo, cuenta con algunas desventajas, entre ellas que el cifrado es relativamente lento y además extiende el texto cifrado, requiriendo así más potencia de procesador.

La tabla 3.1 muestra la comparación entre estos 2 tipos de cifrados:

Criptografía Simétrica	**Criptografía Asimétrica**
Utiliza la misma llave para cifrar y descifrar.	Utiliza una llave pública para cifrar y una privada para descifrar.
El cifrado es seguro.	El cifrado es seguro.
El cifrado es rápido.	El cifrado es relativamente lento.
El texto cifrado es compacto.	El texto cifrado se expande.
La llave que genera el emisor para cada proceso de cifrado debe llegar al receptor (está sujeto a intercepción).	No se necesita enviar una llave al receptor por cada proceso de cifrado, por lo que no sufre por la intercepción de llaves.
El número de llaves que se requiere distribuir es aproximadamente el cuadrado del número de participantes.	El número de llaves que se requiere distribuir es el mismo al número de participantes.
Requiere relación previa entre las partes involucradas.	No exige una relación previa entre las partes para el intercambio de llaves.
No se utiliza para firmas digitales ni de aceptación.	Soporta firmas digitales y aceptación

Tabla 3.1 Comparación entre criptografía simétrica y asimétrica

3.4.1.3 Combinación simétrico / asimétrico

Como solución a las desventajas que contienen cada unos de los tipos de cifrado mencionados, en muchas aplicaciones se opta por utilizar una combinación de ambos. Este tipo de cifrado utiliza las ventajas de los dos tipos mencionados anteriormente y como resultante se obtiene un nuevo proceso con las características de velocidad, texto compacto, escalabilidad, facilidad de administración de llaves, resistencia a la interpretación y soporte para firma digital y aceptación.

El proceso de cifrado inicia con la generación de una llave simétrica aleatoria que se utiliza para cifrar la información que se desea enviar. Con este tipo de cifrado (simétrico) aseguramos rapidez y además, el resultado es un texto compacto. Luego, en lugar de mandar la llave generada directamente al receptor, lo cual es inseguro por ser vulnerable a intercepciones, se utiliza el mecanismo de encriptación de llave pública/privada para cifrar la llave generada anteriormente. Esto con la finalidad de que la llave se envíe en forma segura al receptor, quien debe contar con su propia llave privada. A este proceso se le conoce como "operación de llave empaquetada". Posteriormente se une esta llave empaquetada con el texto cifrado para enviarlo al receptor. A este proceso se le conoce como "sobre digital". En dado caso de que un intruso interceptara este sobre, no podrá descifrarlo porque para poder tener acceso a la llave simétrica que descifra el texto, primero necesitaría contar con la llave privada que guarda en forma segura el receptor.

Para el proceso de descifrado, se requiere primero descomponer el sobre digital en las dos partes que lo constituyen: el texto cifrado con criptografía simétrica y la llave empaquetada con criptografía asimétrica. Luego, el receptor debe recuperar la llave empaquetada. Para lograr esto, utiliza su llave privada, permitiendo así que solamente esta persona pueda recuperar la llave empaquetada. Con la llave simétrica extraída, se puede entonces descifrar el texto original que contiene el sobre.

Además de clasificar los algoritmos criptográficos en simétricos y asimétricos, se pueden también clasificar de acuerdo a la manera en que operan. Por ejemplo, Menezes, A., Van

Oorschot, P. & Vanstone, S. (2001) define dos tipos de algoritmos criptográficos de acuerdo al tamaño de entrada de los datos:

1. **De Bloque.** Son aquellos que codifican datos en bloques pequeños de longitud fija (por lo común 64 y 128 bits). Este tipo de cifrado se utiliza tanto en algoritmos simétricos, como asimétricos. Entre algunos ejemplos de algoritmos criptográficos de bloque se encuentran IDEA, DES, BLOWFISH, AES, Diffie-Hellman y RSA.

2. **De Flujo (o de Stream).** Son aquellos que operan en bits de datos individuales del mensaje a cifrar. Los algoritmos de este tipo de cifrado son generalmente más rápidos que los de bloque y requieren menos complejidad de hardware. Además, son más apropiados para cuando la capacidad de datos temporales en hardware (buffer) está limitada o cuando se requiere procesar cada bit individualmente conforme se recibe. Al igual que los de bloque, este tipo de cifrado se utiliza tanto en algoritmos simétricos como asimétricos. Entre algunos algoritmos criptográficos de flujo se encuentran ORYX, RC4 y SEAL.

Aunque existe una gran variedad de algoritmos de cifrado, en este trabajo sólo se describe el algoritmo DES (y su variante 3-DES) ya que, como se verá en el capítulo IV, es el algoritmo que utilizan las tarjetas inteligentes empleadas en el sistema propuesto.

3.4.2 Algoritmos de cifrado DES y 3-DES

El algoritmo DES fue desarrollado originalmente por la empresa IBM en 1974, en respuesta a una convocatoria que lanzó el Instituto Nacional de Estándares y Tecnología de los EE.UU. (NIST) para contar con un algoritmo que protegiera información no clasificada. Se requería que no fuera costoso, que fuera muy seguro y que se pudiera utilizar ampliamente. IBM lo presentó con el nombre de "Lucifer". La Agencia de Seguridad Nacional de los EE.UU. (NSA) lo evaluó y realizó algunas modificaciones

para posteriormente nombrarlo “DES” (Data Encryption Standard) en 1977. Su uso oficial fue reemplazado en 1997 por el algoritmo AES, cuando se demostró que el primero tenía vulnerabilidades, ya que el algoritmo fue quebrado en 1998 utilizando una computadora de $250,000 dólares, al aplicar ataques de fuerza bruta para adivinar la llave, tomándole 3 días de procesamiento. Sin embargo, se sigue utilizando ampliamente para aplicaciones de servicios financieros y otras industrias en todo el mundo (Tropical Software, 2004; RSA Security, 2004).

DES es un algoritmo de cifrado simétrico que utiliza bloques de 64 bits de datos. La llave de cifrado y descifrado consiste de 64 dígitos binarios, de los cuales se utilizan solamente 56 que son generados de manera aleatoria. Los 8 bits restantes no se utilizan en el proceso de cifrado, se utilizan para detección de errores utilizando la comprobación por paridad par.

Al inicio del proceso se realiza una permutación de los datos por cada bloque, posteriormente se realiza un proceso de cómputo complejo que consiste de 16 iteraciones el cual es dependiente de la llave utilizada (básicamente consiste en repetir el proceso 16 veces). Al final se realiza una permutación inversa a la inicial (Daley, W. & Kammer, 1999).

Triple-DES, o también conocido como 3-DES, es una variante del algoritmo DES, el cual básicamente ejecuta tres veces el algoritmo DES sobre el mensaje a cifrar. Esto lo hace utilizando tres llaves de 64 bits cada una, formando un total de 192 bits (24 caracteres). Al igual que el algoritmo DES, cada una de estas llaves utiliza solamente 56 bits y los 8 restantes son para comprobación de paridad, por lo que la llave resultante que se utiliza es de 168 bits. El modo en que opera es que los datos se cifran con la primera llave, luego se descifran con la segunda y finalmente se cifran de nuevo con la tercera llave. Esto lo hace 3 veces más lento que DES, pero miles de millones de veces más seguro si se usa apropiadamente (Tropical Software, 2004).

3.4.3 Uso de la criptografía en el proceso de autenticación

En la sección 3.3 se menciona a la autenticación como uno de los mecanismos para brindar seguridad en la información. La mayoría de los mecanismos de autenticación, si no es que todos, involucra el compartir un secreto entre todos los participantes involucrados en la transacción. Dos de estos mecanismos incluyen distintas formas de cifrado y descifrado de información. La primera utiliza algoritmos de criptografía simétrica, mientras que el segundo utiliza algoritmos de criptografía asimétrica (Jurgensen & Guthery, 2002). Algunas tarjetas inteligentes utilizan criptografía para realizar el proceso de autenticación, tal como se describe a continuación.

3.4.3.1 Proceso de autenticación de tarjetas inteligentes usando criptografía simétrica

Con este mecanismo, cada tarjeta requerirá almacenar dos llaves: una que usará para que se autentique la aplicación de la terminal con la tarjeta y otra que se usará para que la tarjeta se autentique con la aplicación. La aplicación de la terminal requerirá tener almacenado un gran número de llaves, esto es, una por cada tarjeta que tendrá acceso al sistema, además de la que utilice para autenticarse con las tarjetas.

Este esquema presenta algunos riegos de seguridad. Por ejemplo, como la llave que almacena cada una de las tarjetas también debe estar almacenada en la aplicación de la terminal, se pudiera poner en riesgo la identidad de la tarjeta, si por alguna razón las llaves que se almacenan en el servidor son extraídas por personas no autorizadas. Como consecuencia, estas personas pudieran clonar tarjetas usando estas llaves y tener acceso al sistema. Por otro lado, la llave que utiliza la aplicación para autenticarse con las tarjetas se encuentra almacenada en cada una de las tarjetas. Si esta llave se logra extraer de cualquier tarjeta, pudiera utilizarse en otra aplicación, simulando ser la aplicación original.

En la figura 3.3 se muestra cómo se lleva a cabo el proceso de autenticación entre la tarjeta y la terminal. El proceso implica la autenticación de ambas partes, esto es, tanto de la tarjeta como de la terminal. En la figura sólo se muestra la parte donde la tarjeta se autentica con la terminal.

Para realizar este proceso, ambas partes deben tener almacenada la misma llave y mantenerla en privado. La tarjeta, para autenticarse con la terminal, le envía un comando solicitando este proceso. La terminal, en respuesta, cifra un texto arbitrario para enviárselo a la tarjeta y ver si ésta puede descifrarlo. La única manera en que pueda ser descifrado por la tarjeta es si contiene la misma llave con la que fue cifrado por la terminal. Una vez que la tarjeta lo descifra, lo envía de regreso a la terminal y ésta lo valida comparándolo con el original. Si ambos textos son idénticos, significa que la tarjeta posee la misma llave, dando inicio a que establezca una identidad de confianza.

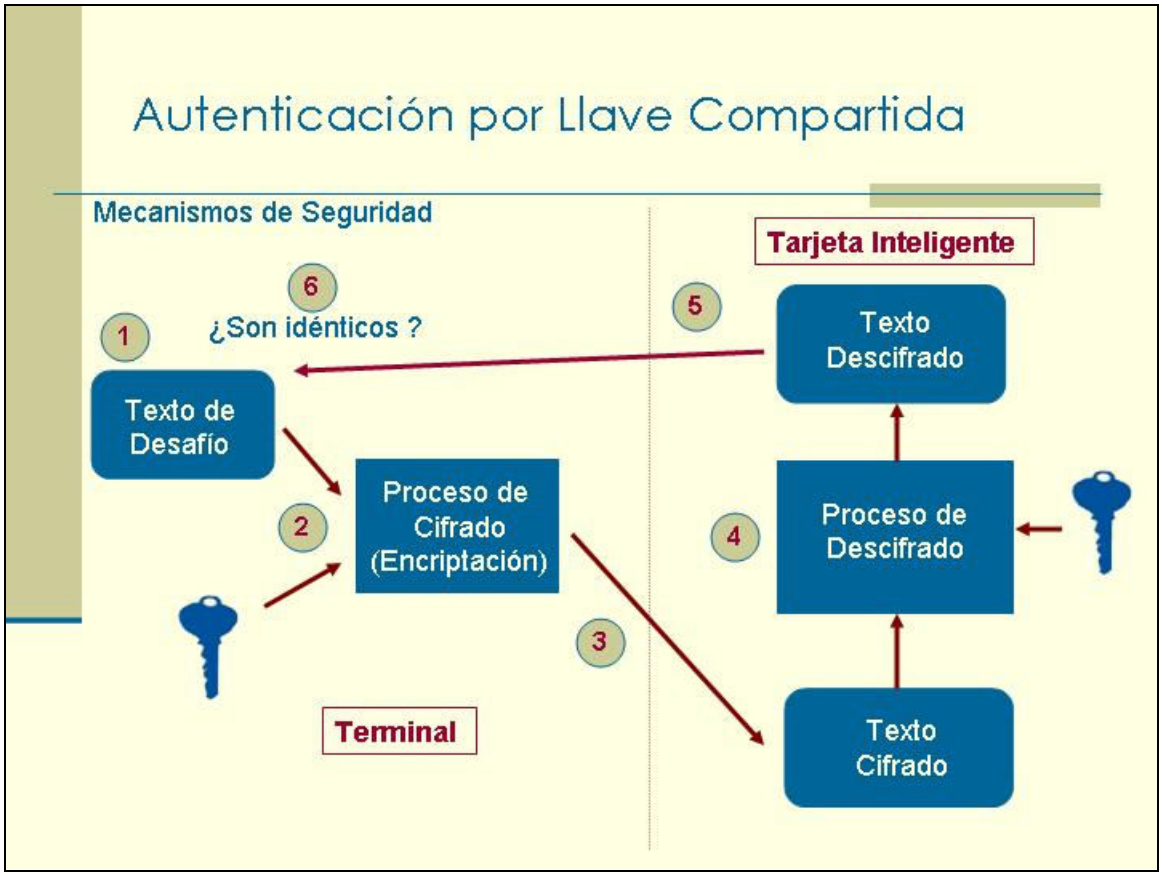

Figura 3.3 – Autenticación de tarjetas inteligentes por medio de llave compartida

Un mecanismo que se utiliza comúnmente para reforzar la seguridad en el uso de tarjetas inteligentes para autenticarse a un sistema, es el de clave secreta (PIN). Este mecanismo utiliza una clave secreta que se almacena en la tarjeta y que sólo el dueño de la tarjeta conoce. Al momento de iniciar una transacción con una aplicación, el dueño de la tarjeta debe introducir esta clave, la cual es comprobada por la aplicación, asegurando así que el usuario se identifique antes de proceder con la transacción.

3.4.3.2 Proceso de autenticación de tarjetas inteligentes usando criptografía asimétrica

Como se mencionó anteriormente, este mecanismo utiliza dos llaves independientes pero relacionadas matemáticamente. Una llave se distribuye públicamente y la otra se mantiene en privado. Algunas tarjetas inteligentes utilizan este mecanismo para autenticación. El proceso se lleva a cabo para ambas partes, esto es, para autenticar la tarjeta con la aplicación de la terminal y viceversa. En la figura 3.4 se muestra cómo se presenta este mecanismo cuando la aplicación requiere autenticarse con la tarjeta. En este caso, la tarjeta requiere saber si la aplicación comparte el mismo secreto que ella. Para lograr esto, la aplicación de la terminal debe mantener oculta su llave privada, esto es, que nadie tenga acceso a ella, sino solamente la misma aplicación, porque esta llave representa su identidad. La llave pública que corresponda a la llave privada puede ser distribuida libremente, por lo tanto, se puede almacenar en toda aquella tarjeta inteligente que requiera acceder a la aplicación. En el ejemplo de la figura 3.4 se muestra que, para que la aplicación de la terminal se autentique con la tarjeta, primero debe solicitarlo. En respuesta a esto, la tarjeta genera un texto arbitrario que usará como reto al cifrarlo con la llave pública que obtuvo anteriormente de la aplicación de la terminal. Este texto cifrado es enviado a la terminal y ésta lo descifra con la llave privada que almacena. Si la aplicación de la terminal logra descifrarlo a su forma original, significa entonces que esa llave privada está relacionada con la llave pública que contiene la tarjeta. Por lo tanto, la tarjeta procede a aceptar la negociación al autenticar la aplicación. Obviamente, el procedimiento inverso permitirá que la tarjeta se autentique con la aplicación de la terminal.

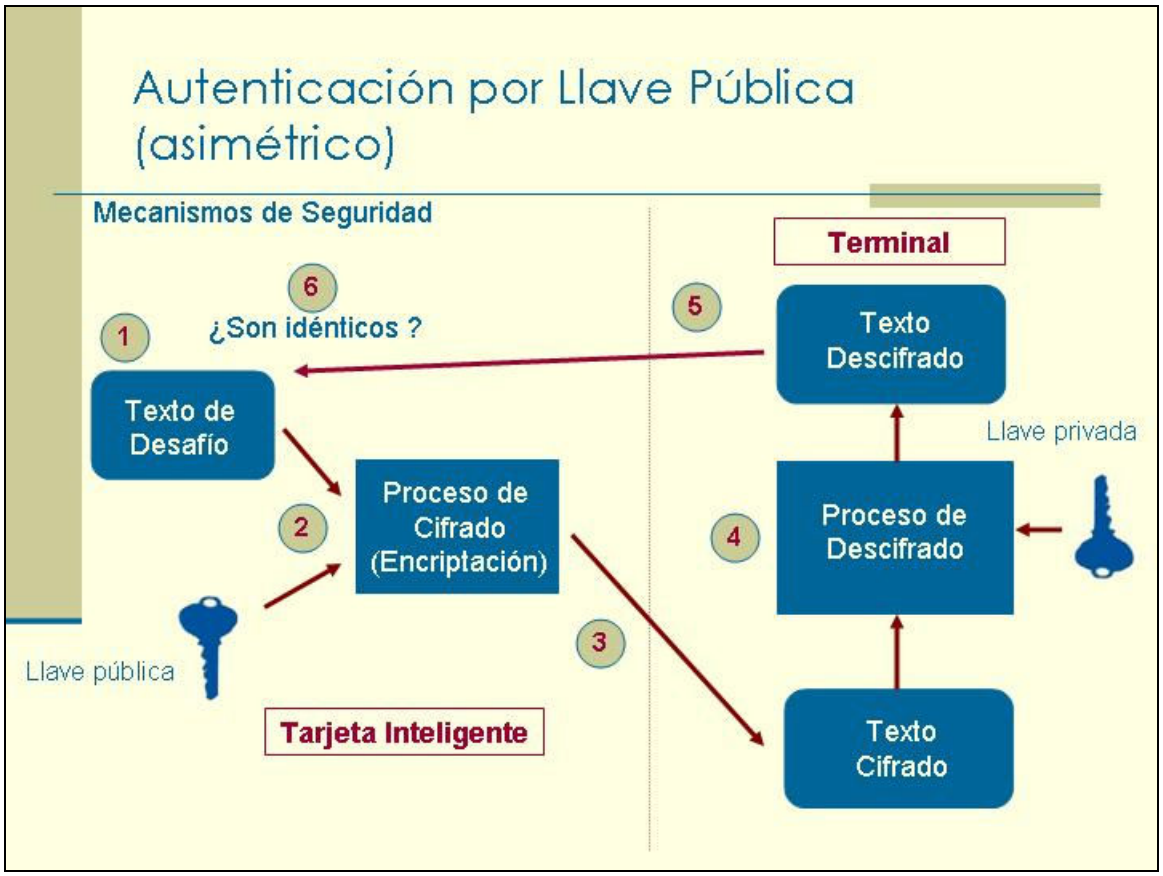

Figura 3.4 – Autenticación de tarjetas inteligentes por medio de llave pública

3.5 Algoritmos hash y firmas digitales

El algoritmo hash es aquel que se utiliza para asegurar que los datos no han sido alterados durante su envío. A grandes rasgos, el algoritmo consiste en comprimir los datos de tal manera que se genera un valor numérico único conocido como "valor hash". Si los datos originales son alterados, se produce un valor hash distinto al producido por los datos originales. El emisor genera un valor hash con los datos originales y envía tanto los datos, como el valor hash al receptor. Cuando éste recibe los datos, vuelve a generar un valor hash digital utilizando el mismo algoritmo y posteriormente compara ambos valores (el generado por el emisor y el generado por el receptor). Si son idénticos, significa que el mensaje no ha sido alterado. Pero si son distintos, significa que en alguna parte del envío los datos fueron alterados (Nash *et al*., 2002).

Un buen algoritmo hash debe detectar cualquier cambio en los datos, por más mínimo que este sea. Además, estos algoritmos tienen la propiedad de que no se puede poner a funcionar el algoritmo hacia atrás y recuperar el texto original. Además, el valor hash resultante no dirá nada sobre el texto original. Entre los más conocidos se encuentran MD2 (de DSA), MD5 y SHA-1.

Una aplicación muy común de este tipo de algoritmo son las firmas digitales. Orlin, (1997-2000) define una firma digital como "una forma matemática precisa de adjuntar la identidad de una persona a un mensaje, son mucho más difíciles de falsificar que las firmas escritas y el mensaje firmado no puede ser modificado sin invalidar la firma". Las firmas digitales tienen la característica de permitir verificar la autenticidad del documento o contrato firmado (mensaje), además de permitir verificar la identidad del firmante. Esto es, que hace posible que el destinatario se asegure de que el mensaje que recibe, es enviado por quien dice ser el remitente. Además, deben ser fáciles de crear, fáciles de verificar, pero difíciles de falsificar.

Si durante el proceso de envío se llegara a alterar, aunque sea una letra de un documento firmado, ya no se podría verificar la firma de tal documento. Para llevar a cabo esto, las firmas digitales hacen uso de los algoritmos hash mencionados anteriormente. La capacidad que tienen estos algoritmos para detectar el más pequeño de los cambios en un texto, es lo que les da su utilidad para verificar la integridad del mensaje.

Las firmas digitales se basan en la criptografía asimétrica, donde se utiliza una llave pública que puede conocer todo el mundo, como si fuera un número telefónico, y una llave privada, que la debe conocer solo la persona que firma el documento.

3.6 Protocolo de Capa de Socket Segura (SSL)

En las últimas dos décadas, universidades, empresas, agencias de gobiernos y personas en general, han sacado provecho de las ventajas que brindan los avances en las tecnologías de redes de datos. Cada vez más se desarrollan aplicaciones que utilizan la red Internet

para cubrir las necesidades de transferencia de información. Sin embargo, la seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada a Internet. Es por esto que se deben utilizar mecanismos para protección de los recursos de las redes privadas, incluyendo el evitar accesos no autorizados y protección de la integridad y privacidad de la información. Una solución segura para proteger enlaces de datos a través de Internet es el Protocolo de Capa de Socket Segura (SSL).

SSL, al cual se le conoce hoy como *Transport Layer Security* (TLS), fue desarrollado originalmente por la empresa Netscape Corporation en 1994 y se propuso como un estándar diseñado para brindar un enlace seguro entre navegadores y servidores de Internet. Esta tecnología permite asegurar un sitio de Internet por medio del cifrado de la información y la autenticación (Coulouris, Dollimore, & Kindberg, 2001). Aunque SSL es el sistema de cifrado de datos más utilizado en Internet, no sólo se utiliza para conexiones Web seguras, sino también para todo tipo de aplicaciones de red que necesitan cifrado en conexiones de punto a punto (Johnson, Gossels & Davis, 2004).

Para que se pueda crear una conexión segura usando tecnología SSL, se requiere que el servidor Web tenga un certificado SSL. Tal certificado contiene, entre otros elementos, la identidad del sitio y la compañía a la que pertenece. Además, el servidor crea dos llaves, una pública y otra privada. La llave pública se utiliza para cifrar información mientras que la llave privada se utiliza para descifrarla. La llave pública no necesita ser secreta, sino que se incluye en un archivo de datos que contiene los detalles del sitio Web (llamado Solicitud de Firma de Certificado o CSR) el cual es validado por una Autoridad de Certificación (*Certification Authority* o CA) y esta se encarga de expedir el certificado SSL conteniendo los detalles del sitio para permitir realizar conexiones SSL. Cuando un navegador Web se conecta a un dominio seguro, se lleva a cabo una negociación (*handshake*) de SSL que autentica el servidor y el cliente estableciendo un método de cifrado y una llave única de sesión. A partir de aquí, se establece una sesión segura que garantiza privacidad e integridad en los mensajes. Cada certificado SSL se crea para un servidor en particular de cierto dominio para una entidad de negocio verificado (SSL.com, 2005).

Entre los datos que contiene el certificado SSL, se encuentran el nombre del dominio, el nombre de la compañía, dirección, ciudad, estado y país. También se incluye la fecha de expiración del certificado, así como los detalles de la Autoridad de Certificación responsable de la expedición de tal certificado. Cuando un navegador Web se conecta a un servidor que utiliza SSL, obtiene el certificado SSL y verifica que no ha expirado, que ha sido expedido por una Autoridad de Certificación en la cual el navegador Web confía y verifica también que está siendo utilizado por el sitio de Internet que lo ha proporcionado. Si una de estas verificaciones falla, el navegador Web despliega una advertencia informándole al usuario que está accediendo a un sitio no seguro por SSL (SSL.com, 2005).

El protocolo SSL consta de dos capas implementadas en bibliotecas de software en el nivel de aplicación tanto en el navegador Web como en el servidor. La primera capa es la que implementa un canal seguro, cifrando y autenticando mensajes transmitidos a través de cualquier protocolo orientado a conexión. A esta capa se le conoce como Capa de Protocolo de Registro SSL (ver figura 3.5). La segunda capa se encarga de llevar a cabo el *handshake* entre el navegador Web y el servidor para establecer y mantener una sesión SSL (un canal seguro) entre ambos. Para cada sesión segura se le da un identificador y cada uno de los participantes puede almacenarlos en una memoria tipo caché para uso posterior, evitando así volver al proceso de crear una nueva sesión.

Debido a que la intención de SSL es añadir comunicación segura a los protocolos de nivel de aplicación existentes, se diseñó para encontrarse en el modelo de capas OSI, entre los niveles de protocolos de transporte (por ejemplo TCP) y los protocolos de aplicación y presentación como pudieran ser HTTP, FTP, SMTP, Telnet, etc.

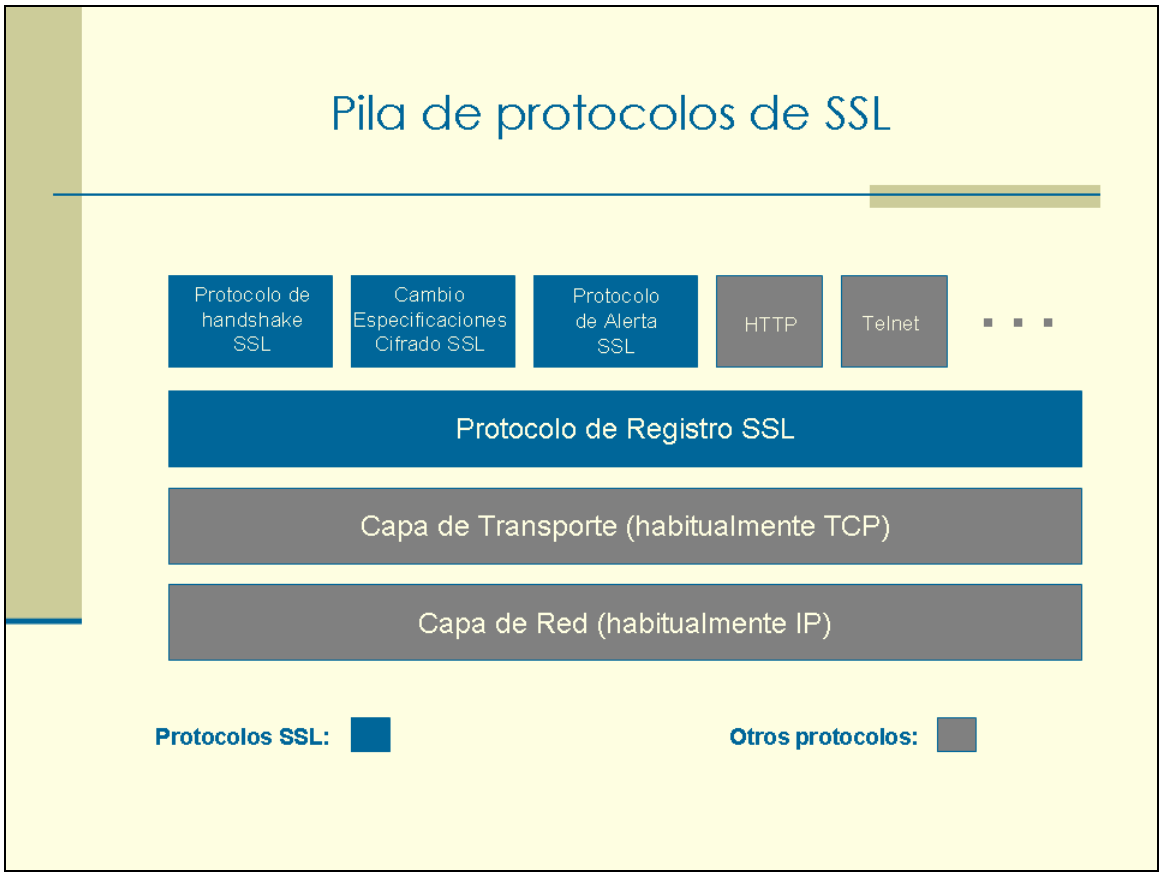

Figura 3.5 - Pila de protocolos de SSL

Como SSL soporta varias opciones criptográficas, al comenzar el *handshake,* el servidor le muestra al cliente una lista de los catálogos de cifrado disponibles, así como de métodos de compresión, en caso de que se utilice. El cliente responde seleccionando uno de ellos o indicando error si no tiene disponible ninguno de los cifrados o tipos de compresión, que el servidor muestra. Además, ambas partes pueden intercambiar certificados de llave pública, utilizando el formato estándar X.509. Para más información de este estándar, consulte Coulouris, Dollimore & Kindberg (2001) en la sección 7.4.4 que habla sobre estándares de certificación y autoridades de certificación.

Para cada sesión SSL, el servidor tiene que autenticarse con el cliente. Esto se hace con la finalidad de evitar que la respuesta que recibe el cliente sea de otro servidor o que la información sea interceptada. Con el proceso de autenticación, el servidor le asegura al cliente su identidad. En el caso de la versión 3.0 de SSL, el cliente también se autentica

con el servidor, llevando a cabo un proceso de autenticación mutua. SSL utiliza criptografía tanto simétrica como asimétrica. La criptografía asimétrica (o criptografía de llave pública) se utiliza para el proceso de autenticación, mientras que la criptografía simétrica (o de llave privada) se utiliza para cifrar los datos que se transmiten asegurando así, la privacidad e integridad del mensaje (Johnson, Gossels & Davis, 2004).

3.7 Conclusiones

En este capítulo presentó una idea general de lo que es la seguridad de la información y algunos mecanismos que se utilizan para llevarla a cabo. Se mostró también la manera en que se lleva a cabo el proceso de autenticación entre tarjetas inteligentes y las aplicaciones con las que operan, utilizando criptografía como herramienta esencial para tal función. Durante la investigación se observó que el tema de la seguridad de la información es muy amplio y dinámico, ya que conforme evolucionan los sistemas informáticos, también evolucionan los mecanismos para protegerlos. Por lo tanto, se puede inferir que cuando se requiere brindar seguridad de la información a un sistema, se debe considerar como algo primordial, su grado de complejidad y a su vez, identificar aquellos puntos de acceso vulnerables a ataques por personas ajenas al mismo. Cualquiera de estos puntos de acceso que permita proporcionar información a personas no autorizadas o externas al sistema, representa un riesgo para la totalidad de dicho sistema. Coulouris, Dellimore & Kindberg (2001), al hablar de seguridad señalan que "El diseño de los sistemas seguros parte de un listado de premisas de ataque y un conjunto de peores casos posibles". Es por esto que se debe tener conocimiento a detalle sobre los aspectos de seguridad que involucra un sistema y revisar cada una de las etapas por las que exista transferencia o administración de la información, incluyendo no sólo a los equipos y sistemas informáticos, sino también al personal que tiene acceso a ella. Además es de suma importancia definir y asegurar que se cumplan con reglamentos de seguridad en todos los niveles del sistema.

Capítulo IV. Diseño del sistema para el almacenamiento y recuperación de expedientes curriculares electrónicos.

4.1 Motivación

La falsificación, duplicado y comercio ilegal de comprobantes curriculares se ha convertido en una problemática que alcanza niveles internacionales. Esta situación deriva en un problema adicional para quienes son responsables de verificar la validez de los documentos probatorios que contienen los expedientes curriculares. Partiendo de dicho problema, y tomando en consideración la complejidad inherente al manejo de grandes volúmenes de documentos en papel, se presenta el diseño de una arquitectura para un sistema que, por medio del uso de tarjetas inteligentes, permite el almacenamiento, administración y recuperación de expedientes curriculares en forma eficiente y segura, además de brindar la seguridad de que los documentos que presenta el usuario son auténticos.

El diseño consiste en una red de servidores de bases de datos distribuidos de acuerdo a regiones establecidas, los cuales permiten almacenar, en formato digital y en forma estructurada, los expedientes curriculares de cada persona con nivel profesional que reside en este país. Además, se incluyen servidores de aplicaciones que operan como intermediarios entre las bases de datos y las terminales desde donde se acceda a la información. Se utilizan tarjetas inteligentes como mecanismo de autenticación con la red de servidores para poder acceder a los expedientes curriculares almacenados en el sistema. Tales tarjetas utilizan un mecanismo de autenticación mutua por medio de algoritmos de criptografía simétrica, así como número de identificación de usuario (PIN) para comprobación de identidad.

Los expedientes curriculares estarán conformados por todos los documentos probatorios tanto de estudios como de experiencia laboral de los usuarios. Su almacenamiento, utilizando un formato estructurado, permite aprovechar las ventajas de las tecnologías de la información para un manejo más eficiente de los expedientes curriculares.

4.2 Requerimientos

Para proporcionar una alternativa en la verificación de la validez de los documentos probatorios, se propone el diseño de un sistema que permite almacenar y recuperar de manera segura, confiable y eficiente, expedientes curriculares electrónicos. Para la elaboración de este diseño, se determinaron los siguientes requerimientos:

1. **Almacenamiento**. El sistema requiere el almacenamiento en formato digital, de los expedientes curriculares de todas las personas con estudios de nivel profesional que residen en la república mexicana. Cada expediente curricular está compuesto de todos los documentos probatorios, tanto de estudios como de experiencia laboral, así como de datos de identificación del profesionista. Entre estos documentos se encuentran los siguientes:

    - Título de grado (licenciatura, maestría, doctorado, etc.)
    - Diplomados
    - Seminarios
    - Certificados
    - Documentos que acrediten experiencia laboral
    - Idiomas
    - Publicaciones
    - Reconocimientos
    - Otros

2. **Mecanismo de acceso seguro y privacidad de la información**. El sistema debe permitir que cualquier institución, organización o empresa, tenga acceso a visualizar el expediente curricular de una persona, siempre y cuando sea con el consentimiento de ésta. Esto, con la finalidad de que los documentos probatorios

que las personas presenten, puedan ser verificados de manera eficiente y segura, en el mismo instante en que los presentan. Se debe contar, además, con un mecanismo que garantice que la consulta de la información curricular que pertenezca a cierta persona, sólo se pueda efectuar si esta se encuentra presente y que se ha identificado correctamente. De esta manera se evitará que otra persona muestre un expediente curricular que no le corresponda o que las empresas e instituciones accedan a los expedientes curriculares sin consentimiento de sus propietarios.

3. **Representación de la información.** Los documentos que se almacenen en el sistema, deben cumplir con una estructura bien definida y estandarizada para todas las instituciones educativas y entidades laborales que se integren a este sistema. De esta manera, los comprobantes podrán ser leídos e interpretados por cualquier institución, empresa u organización que desee tener acceso a ellos. Se deben especificar detalladamente todos los elementos que puede contener cada documento probatorio.

4. **Control del sistema.** Se requiere contar con entidades que tengan la facultad de llevar a cabo los procesos involucrados en el manejo de los documentos que conforman el expediente curricular electrónico, tales como su verificación, almacenamiento y administración. Además, se requiere que el sistema sea confiable en cuanto a la disponibilidad de la información en todo momento.

4.3 Diseño del sistema

En la sección 4.2 se mencionó que se requiere de un sistema que almacene y administre expedientes curriculares, utilizando una estructura bien definida para estos documentos y además que permita que cualquier institución, organización o empresa pueda tener acceso a los mismos por medio de un mecanismo seguro de autenticación e identificación. En base a tales requerimientos, se propone el diseño de un sistema donde se utilicen servidores de bases de datos y servidores de aplicaciones en un ambiente distribuido. El sistema está diseñado de tal manera que pueda cubrir las necesidades de demanda en

cuanto a almacenamiento, disponibilidad de los datos, administración de la información y seguridad de acceso.

4.3.1 Distribución de la información y su administración

Uno de los aspectos importantes a considerar al diseñar un sistema que almacene información y que va a ser accedida por muchas personas a la vez, es el determinar cómo se almacenará esta información y cómo se llevará a cabo su administración.

Berson (1996) menciona que, anteriormente, la mayoría de las organizaciones desarrollaban aplicaciones que residían en computadoras centrales tipo mainframe, dando como resultado, que los datos que estas aplicaciones accedían, se almacenaran también en localidades centrales por medio de bases de datos corporativas. El uso de grandes computadoras localizadas en un solo punto, ejecutando aplicaciones centralizadas, se hacía cada vez más costoso, especialmente si se comparaba con las ventajas que brindaban las microcomputadoras. Posteriormente, las empresas se interesaron cada vez más en implementar bases de datos distribuidas. La decisión de usar datos centralizados o distribuidos, está determinada principalmente por el grado en que se comparten estos datos y el nivel de autonomía local que la organización requiere. Esto es, entre más se requiera que los datos sean compartidos por todas las localidades, más conveniente resulta el utilizar un modelo de almacenamiento de datos centralizado.

Antes de seleccionar la manera en que la información del sistema estará distribuida, se hizo un análisis de las ventajas y desventajas que brindan los distintos modelos de almacenamiento de datos. El modelo de datos centralizado tiene la característica de que la información se almacena en una sola localidad. Esto es, todas las aplicaciones que requieran acceder a la información, ya sean locales o remotas, lo harán por medio de conexiones a un solo punto central. Esto tiene la ventaja de que la información se puede compartir sin problema desde un punto central y su administración es sencilla, ya que hay un solo administrador o conjunto de administradores del sistema responsable de los datos

a nivel global. Además, el concentrar los datos en un solo punto, evita los problemas que pudieran resultar cuando los datos son distribuidos, como por ejemplo, errores de sincronización, fragmentación de la información y réplicas distintas de los datos. Sin embargo, tiene varias desventajas, entre las que se encuentran las siguientes:

- Se requiere contar con medios de almacenamiento de gran capacidad, sobre todo para bases de datos que contienen información de muchos usuarios, ya que toda la información se concentra en un solo punto.

- El acceso simultáneo al sistema central es susceptible a presentar cuellos de botella. Esto implica contar con un servidor y equipo de comunicaciones que soporte la demanda en velocidad para atender estas peticiones simultáneas, así como medios de almacenamiento de rápido acceso.

- Como sólo existe un punto de acceso a la información, representa un solo punto de falla. Es decir, si el servidor o equipo de comunicaciones falla por alguna razón, bloqueará el acceso a toda la información, por lo tanto ningún usuario podrá accederla.

Por otro lado, el modelo de datos distribuidos tiene la principal característica de que los datos se encuentran almacenados en diferentes localidades. Las bases de datos distribuidas aportan las ventajas de la computación distribuida al dominio de la gestión de de los datos. Berson (1996) y UPM (2006) hacen mención de las siguientes ventajas que ofrece el distribuir los datos en múltiples localidades:

- Se tienen los datos localizados más cerca de su fuente, haciendo el acceso más rápido y eficiente. Además estos datos se pueden compartir con otras localidades.

- Mayor disponibilidad de los datos al contar con múltiples copias de datos críticos en diferentes localidades, eliminando así la posibilidad de que exista un solo punto de

falla.

- Permite la fragmentación, tanto horizontal como vertical y almacenar los fragmentos en distintas localidades.

- Se refuerza la autonomía local. Es decir, cada localidad tiene cierto grado de control sobre sus propios datos.

- Balance de cargas en la aplicación que proporciona a los datos.

- Facilidad de crecimiento en las aplicaciones y en las demandas de clientes. Resulta más fácil agregar datos o servidores de procesamiento de información.

Son muchas las ventajas que brindan los modelos de datos distribuidos. Sin embargo, éstos también pueden presentar algunas desventajas, como las siguientes (UPM, 2006):

- El desarrollo del software es costoso, ya que añade complejidad para coordinar todas las localidades de los datos.

- Existe mayor probabilidad de errores. Como las localidades que constituyen el sistema funcionan en paralelo, es más difícil asegurar el funcionamiento correcto de los algoritmos, así como de los procedimientos de recuperación en fallas del sistema.

Además, se deben tomar en cuenta algunos aspectos importantes que hacen que las bases de datos distribuidas operen adecuadamente y brinden las ventajas que se mencionaron anteriormente. Entre estos aspectos se encuentran los siguientes (Elmasri & Navathe, 2002; Bunn, 2001):

- Contar con transparencia de red o de distribución. Esto implica que los usuarios puedan acceder a los datos sin que se requiera conocer la locación de los mismos. Además, se debe contar con mecanismos para acceder los objetos por nombre sin que cause ambigüedad. Como por ejemplo, el acceso a páginas Web, que utiliza un Localizador de Recurso Uniforme (URL), para acceder a los recursos en la Web.

- Contar con transparencia de réplica. Esto implica que el usuario desconozca los detalles sobre si se utilizan copias de la información en diferentes localidades. El sistema debe aparentar que sólo se están realizando transferencias de información en la misma localidad.

- Contar con transparencia de fragmentación. Esto implica que el usuario desconozca si se utilizan mecanismos para fragmentar los datos almacenados. El sistema debe aparentar que toda la información está almacenada en una misma localidad.

Al estudiar las ventajas y desventajas que brindan ambos modelos, se hizo un análisis para posteriormente determinar la manera en que los expedientes curriculares electrónicos se almacenarán en el sistema. El análisis se describe a continuación:

Como el sistema contempla el almacenamiento del expediente curricular de cada profesionista que reside en el país, se requiere contar con una base de datos muy extensa y con capacidad de expansión. El utilizar un modelo centralizado implicaría contar con medios de almacenamiento de gran capacidad y alto desempeño, para almacenar todos los expedientes curriculares de los usuarios y cumplir con las demandas de velocidad en respuesta, ante solicitudes desde empresas e instituciones de todo el país. Por otro lado, centralizar los datos y la administración de los mismos, tendría como consecuencia que se contara con un solo punto de falla. Este sistema debe estar disponible en todo momento, ya que constantemente se estarán realizando consultas de los expedientes curriculares, desde diversas empresas e instituciones. Por lo tanto, tener un solo punto de falla, no representa una solución viable.

Como se requiere contar con entidades que verifiquen los documentos probatorios de los usuarios, para su posterior almacenamiento y administración, se debe brindar cierto grado de responsabilidad y autonomía a estas entidades. Por lo tanto, resulta más conveniente distribuir las responsabilidades de tal manera que, cada entidad verifique, almacene y administre únicamente los documentos probatorios que le correspondan.

En base a lo anterior, se determinó utilizar medios de almacenamiento distribuido entre distintas entidades, donde cada una tenga autonomía sobre el almacenamiento y administración de los documentos probatorios que éstas verifiquen. No es necesario almacenar réplicas de todos los expedientes curriculares en las distintas entidades, ya que sería contar con información redundante, y no brindaría ventajas sobre el modelo centralizado. Para esto, se utiliza una arquitectura que permite distribuir el almacenamiento del expediente curricular en fragmentos, donde cada fragmento corresponde a un documento probatorio. Como el expediente curricular de un usuario se conforma de comprobantes de estudios y de experiencia laboral, cada uno de éstos se almacenará en la entidad que realizó su verificación. La figura 4.1 muestra un ejemplo de esta distribución.

Se muestra también que una misma entidad puede almacenar más de un documento probatorio, pues el lugar de almacenamiento depende del lugar donde fue verificado. Incluso puede haber casos en los cuales el expediente curricular se almacene completo en una sola entidad. Es decir, que todos los fragmentos que lo conforman se encuentren almacenados en una misma localidad. Los datos personales que identifican al usuario se almacenarán en la entidad que agregue el expediente curricular al sistema.

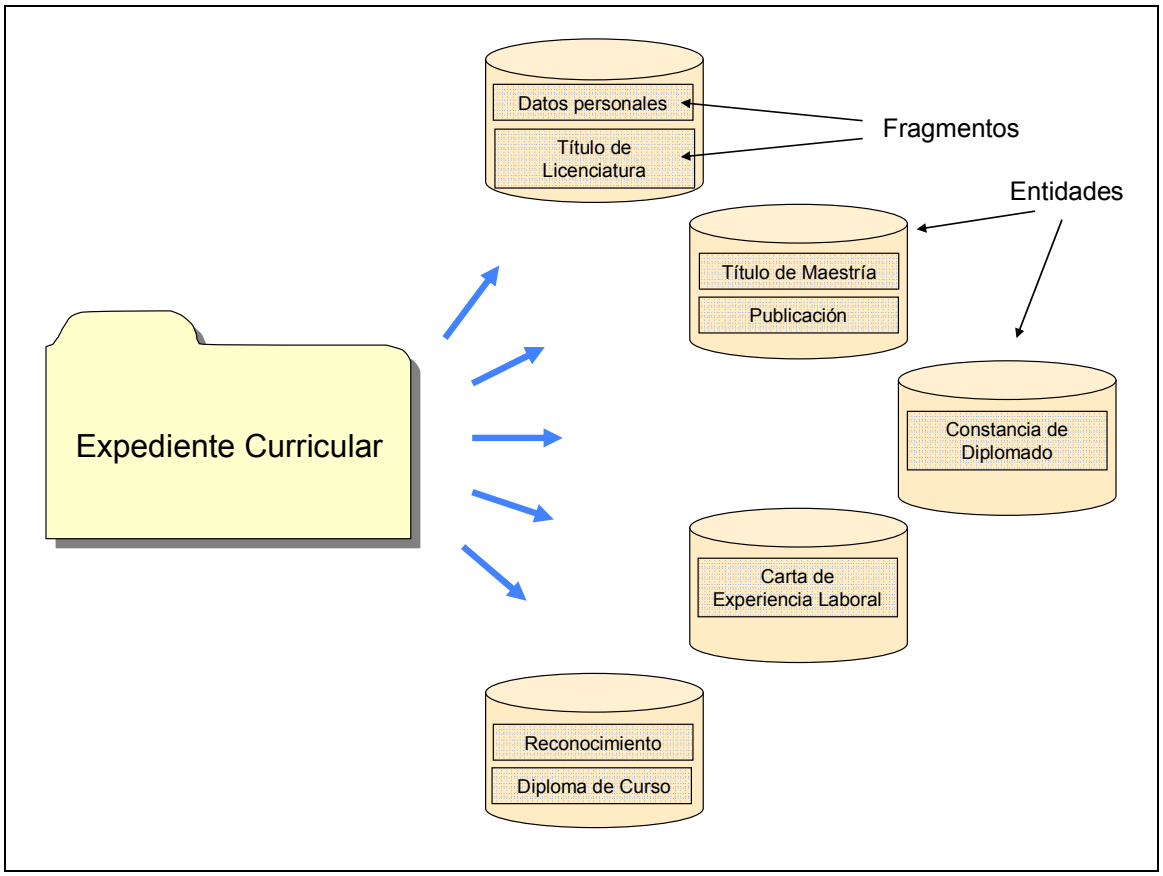

Figura 4.1 Ejemplo de distribución de almacenamiento del expediente curricular

4.3.2 Arquitectura del sistema

Para implementar un sistema que permita almacenar expedientes curriculares en forma distribuida entre entidades, se propone el diseño de una arquitectura compuesta por servidores de administración de bases de datos, servidores de aplicaciones y aplicaciones cliente. Estos tres elementos se describen a continuación:

4.3.2.1 Servidores de administración de bases de datos (DBMS)

El uso de bases de datos no permite aislar de las aplicaciones, los detalles sobre cómo se estructuran y almacenan los datos. Los servidores de administración de bases de datos

(DBMS) proveen a las aplicaciones con medios consistentes para el acceso eficiente a los datos por medio de lenguajes de definición y manipulación de estos, además de contar con mecanismos para brindar independencia, consistencia, integridad, seguridad y recuperación de los datos (Bunn, 2001). Estas características cumplen con los requerimientos del sistema de almacenamiento de expedientes curriculares. Por lo tanto, los DBMS serán elementos primordiales en el diseño de esta arquitectura.

Entre los requerimientos del sistema se encuentra que sea confiable y esté disponible en todo momento. Esto implica que el sistema tenga la capacidad para brindar acceso a miles de usuarios de manera simultánea, debido a que los expedientes curriculares podrán ser visualizados por cualquier empresa e institución del país. Para esto, se investigó la posibilidad de utilizar alguna plataforma o diseño existente que sirviera como base para el diseño propuesto, en donde se distribuyan tanto los datos como la administración de los mismos y que brinde alta disponibilidad.

La empresa *Sleepycat Software* (adquirida por la empresa *Oracle* en febrero de 2006), desarrolló la base de datos llamada "*Berkeley DB High Availability*" la cual consiste de un conjunto de librerías que permite crear aplicaciones de bases de datos para brindar alta disponibilidad. Entre sus características se encuentran las siguientes (Oracle, 2006):

- **Escalabilidad** – Permite agregar servidores sin que se incremente la complejidad o aumenten en gran medida los costos del sistema.

- **Flexibilidad** - Permite personalizar sus funciones de acuerdo a la aplicación que la vaya a integrar.

- **Administración sencilla –** El conjunto de librerías que contiene se integra a la aplicación, por lo que requiere de mínima administración de sus funciones. La mayoría de las funciones de administración se pueden programar para que sean automáticas.

- **Acceso concurrente** – Permite atender múltiples consultas de manera simultánea sin afectar la operación o consistencia de la base de datos.

- **Alta disponibilidad** – Utiliza réplicas para distribuir la carga de los servidores, además de permitir que el sistema siga funcionando aún cuando uno de los servidores falle.

- **Confiabilidad** – Permite la recuperación de los datos en caso de una falla o inconsistencia de la base de datos. Brinda las propiedades *ACID* (por las siglas en inglés de Atomicidad, Consistencia, Aislamiento y Durabilidad), las cuales se describen a continuación:

    - **Atomicidad** – Permite realizar un grupo de operaciones en una sola unidad o transacción.

    - **Consistencia** – Cada transacción que se realiza debe dejar a la base de datos en un estado válido, de acuerdo a reglas establecidas. Si una transacción falla o se interrumpe, se realiza el proceso inverso y se deja a la base de datos en un estado válido.

    - **Aislamiento** – No se presentan anomalías debidas al acceso simultáneo a la base de datos por varios usuarios. Los cambios hechos por un usuario no serán vistos por otros sino hasta que se complete la transacción.

    - **Durabilidad** – Garantiza que una vez que se realiza una transacción exitosa, el estado de la base de datos persiste, incluso aunque el sistema falle.

Las características anteriores son las apropiadas para el sistema que se presenta en este trabajo, ya que brindan tanto confiabilidad de que la información no se perderá, como la seguridad de que la información estará disponible en todo momento, aún si uno de los

servidores falla. Además, permitirá un tiempo de respuesta inmediato ante las múltiples consultas simultáneas de expedientes curriculares que se estén realizando en todo el país.

Como ejemplo de éxito en cuanto a la implementación de bases de datos basadas en el software de la empresa *Sleepycat* se encuentra la empresa *Google*, la cual lo utiliza en su motor de búsqueda por Internet para brindar alta disponibilidad y respuesta inmediata a sus millones de usuarios (Oracle, 2006). Tomando como base esta referencia, se propone implementar el diseño de una red de servidores basado en las soluciones de distribución que brinda la empresa *Sleepycat*. Tal diseño se describe a continuación:

La base de datos que almacena todos los expedientes curriculares se fragmenta en bloques grandes. Cada uno de estos bloques corresponde a una entidad y contiene los siguientes elementos:

- Un servidor de aplicaciones.
- Un servidor de bases de datos designado como “maestro”.
- Uno o más servidores que operan como “réplicas” del servidor maestro.

El servidor maestro tiene la función de atender las consultas que requieran actualizar datos. Esto es, aquellas que impliquen agregar o modificar información de la base de datos de los expedientes curriculares. Por ejemplo, al crear un nuevo expediente curricular o al agregar o modificar un documento probatorio de un expediente curricular existente. Las réplicas almacenan una copia exacta de los datos que contiene el servidor maestro y se actualizan constantemente. Estas tienen la función principal de atender solicitudes únicamente de lectura para permitir el balance de tráfico de consultas que se solicitan a esa entidad. En la operación normal del sistema, la cantidad de consultas de lectura será mucho mayor que las de actualización de datos. Es por esto que el contar con servidores de réplicas permitirá brindar un tiempo de respuesta inmediato ante la gran cantidad de consultas simultáneas de lectura, además de contar con alta disponibilidad para asegurar la operación sin interrupción en caso de que uno de los servidores falle. La figura 4.2 muestra la operación del servidor maestro y los servidores de réplicas.

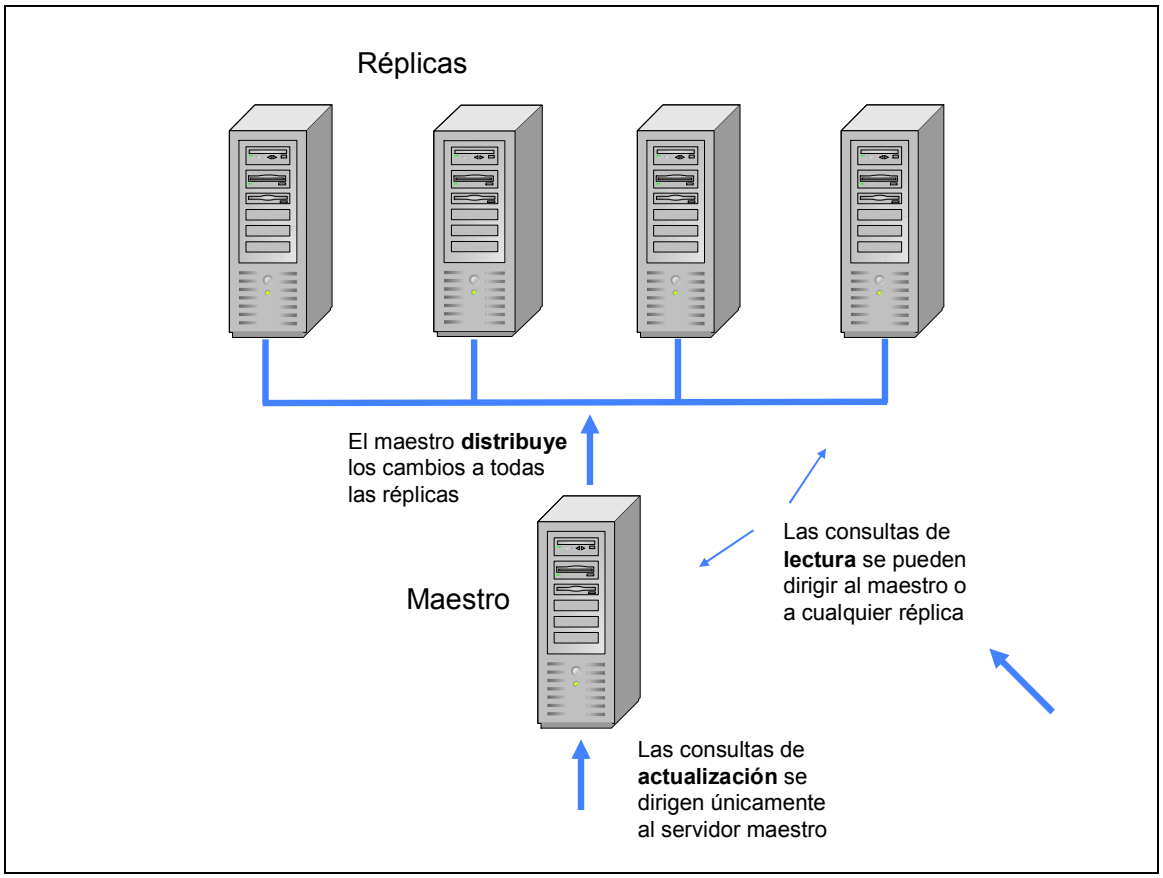

Figura 4.2 Servidor maestro y servidores de réplicas

La mayor carga de procesamiento le corresponde a los servidores de bases de datos. Esto es debido a que, entre sus funciones, se encargan de realizar la búsqueda de los registros de usuarios, extraer los documentos probatorios que se encuentren almacenados tanto en el mismo servidor, como en servidores de otras entidades y presentar el resultado de la consulta al servidor de aplicaciones.

Como parte del sistema de réplicas se cuenta con procesos que monitorean la actividad del servidor maestro. Cada servidor de réplica mantiene comunicación con el servidor maestro para monitorear su estado. En caso de que el servidor maestro falle y no pueda atender una solicitud de actualización de datos, un temporizador programable en cada réplica detectará el evento y disparará una alerta para que se lleve a cabo, de forma inmediata, el proceso de selección de un nuevo servidor maestro. Tal proceso se lleva a

cabo entre las réplicas existentes. La réplica que sea seleccionada operará como maestro a partir de ese momento, de manera transparente para administradores y usuarios. Una vez que el servidor maestro anterior se recupera de la falla, procede a cambiar de rol operando ahora como una réplica (Oracle, 2006). La figura 4.3 muestra un ejemplo de este proceso cuando el servidor maestro presenta una falla.

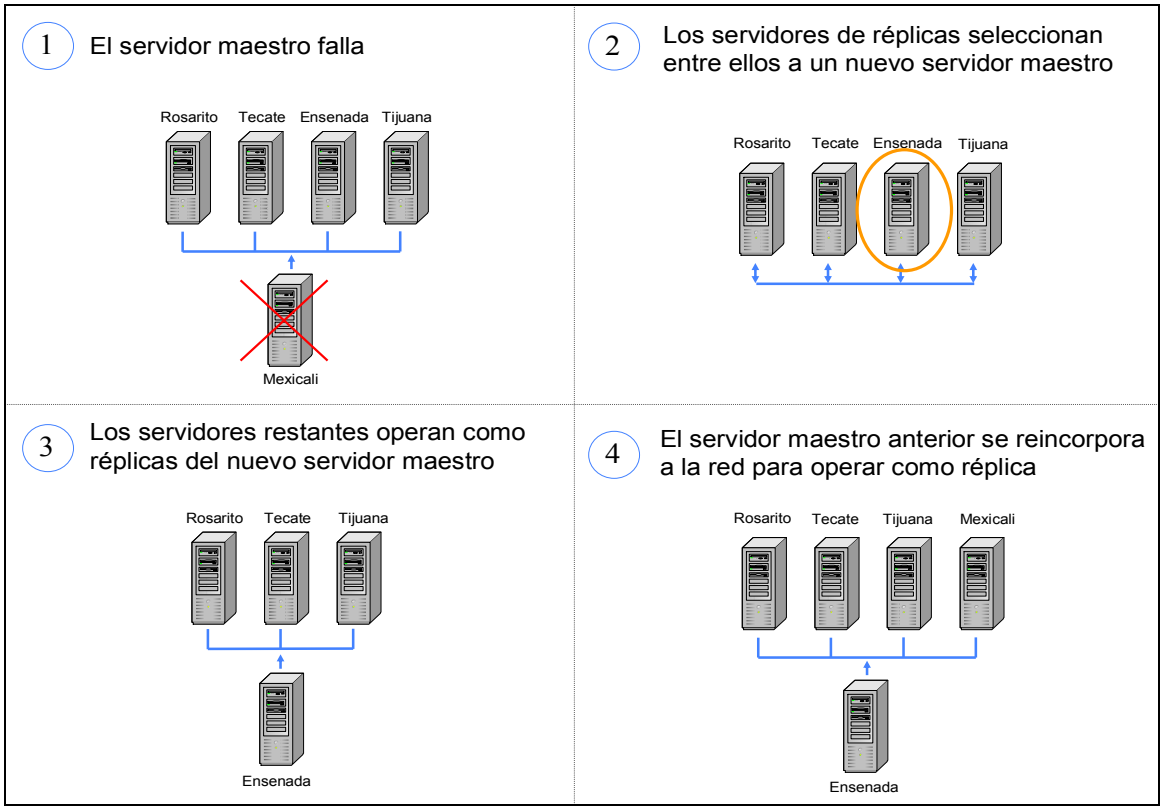

Figura 4.3 Proceso de selección del servidor maestro

En este ejemplo se observa que el servidor "Mexicali" presenta una falla. En ese momento, el mecanismo de monitoreo, el cual es compartido por los demás servidores incluyendo el de aplicaciones, detecta que el servidor maestro no está operando correctamente. Los servidores que se encontraban operando como réplicas de ese servidor maestro inician un mecanismo para la selección del nuevo servidor maestro. El servidor de "Ensenada" resulta ser el asignado y los demás continúan operando como réplicas. A partir de ese momento el servidor "Ensenada" recibe las consultas que requieren actualización de datos y se encarga de notificarles a las réplicas para que actualicen su

información de acuerdo a un mecanismo de actualización ya establecido. Una vez que el servidor "Mexicali" se recupera de la falla y vuelve a operar, detecta que ya existe un servidor asignado como maestro, entonces procede a integrarse a la red y operar como réplica, solicitando de inmediato actualizar sus datos.

4.3.2.2 Servidores de aplicaciones

El servidor de aplicaciones es quien recibe, por parte de los clientes, las solicitudes para visualización de los expedientes curriculares. Contiene un mecanismo que monitorea la carga de tráfico de las réplicas de esa entidad para determinar a cuál de ellas acceder y que ejecute la consulta. Además es quien le dice a los servidores de bases de datos de otras entidades de certificación, quién es el servidor maestro en ese momento y cual es la carga de procesamiento de las réplicas. En caso de que el servidor de aplicaciones fallara durante una consulta desde otra entidad de certificación, se utilizará un mecanismo de "broadcast" para encontrar al servidor maestro. Por otro lado, si el servidor de aplicaciones se encuentra inhabilitado, los servidores de bases de datos de otras entidades de certificación utilizarán al servidor maestro para atender las consultas, ya que no existirá un mecanismo para monitorear la carga de las réplicas. El utilizar al servidor de aplicaciones para encontrar al servidor maestro y brindar información sobre la carga de las réplicas, permite agilizar las consultas de los documentos probatorios.

El servidor de aplicaciones funciona como capa intermedia entre los clientes y los servidores de bases de datos. Provee las pantallas de entrada y presentación de datos por medio de un servicio Web. Esta arquitectura está basada en el patrón de diseño MVC (Modelo-Vista-Controlador), el cual separa la presentación de datos e interacción con el usuario, del núcleo de la aplicación (Bergin, 2003). Esto es, divide las interfaces gráficas de interacción con el usuario, del manejo de los datos. Este patrón de diseño utiliza tres componentes llamados *modelo*, *vista* y *controlador*. El primero representa los datos y las reglas de negocio que gobiernan el acceso y manipulación de datos. Se construye de tal manera que no requiera tener conocimiento sobre la manera en que los datos se

presentarán al usuario. La vista maneja la presentación visual de los datos representados por el modelo. Tiene la responsabilidad de mantener consistencia de su presentación cuando el modelo cambia. El modelo puede tener muchas vistas, las cuales se deben registrar con él para notificarles sobre cambios de estado en sus funciones. El tercer componente, el controlador, proporciona significado a las órdenes del usuario, actuando sobre los datos representados por el modelo. Cuando se realiza algún cambio, entra en acción, ya sea por cambios en la información del modelo o por alteraciones de la vista. Las vistas se asocian con los controladores, los cuales actualizan el modelo conforme el usuario interactúa con las vistas (Bergin, 2003; Sun Microsystems, 2002). Este patrón de diseño facilita la implementación de nuevos clientes para una aplicación. Esto es, cuando se requiera un nuevo tipo de presentación de datos e interacción con del sistema, simplemente se agregan nuevas vistas y controladores que sean adecuados al cliente. El diseño del núcleo del sistema no se ve afectado. El utilizar el patrón de diseño MVC para el sistema de expedientes curriculares facilitará el acceso a visualizar expedientes curriculares desde prácticamente cualquier dispositivo que tenga acceso a Internet y utilice tarjetas inteligentes.

Las funciones de presentación de datos y de interacción con el usuario pueden implementarse de forma independiente en servidores distintos, para balancear el tráfico de consultas. Para fines de simplificar los diagramas de este diseño, se utiliza únicamente un servidor que implementa ambas funciones. La decisión de implementar estos servicios en distintos servidores, dependerá de la cantidad de consultas que se lleven a cabo en determinada entidad. Las funciones principales de los servidores de aplicaciones son las siguientes:

- **Interfaces de entrada de datos** – Provee de interfaces de interacción con el usuario para los distintos tipos de aplicaciones clientes que se utilicen. Para el caso de los clientes basados en navegador Web, se presentará este servicio por medio de una página Web de entrada de datos. Cada servidor de aplicaciones puede contener diferentes tipos de interfaces de entrada de datos según la demanda de aplicaciones cliente lo requiera. Es decir, habrá clientes que consulten expedientes curriculares

desde aplicaciones móviles tales como teléfonos celulares, asistentes personales (PDAs), kioscos de información, etc., por lo que permite expandir la funcionalidad del sistema, sin que implique cambios en la arquitectura o en el manejo de los datos. Las interfaces de entrada de datos corresponden al componente "controlador" del patrón de diseño Modelo-Vista-Controlador (MVC) que utiliza la arquitectura propuesta.

- **Interfaces de presentación de datos** – Provee de interfaces para la presentación de los resultados de las consultas realizadas sobre los expedientes curriculares. Al igual que las interfaces de entrada de datos, se utiliza un servicio en formato de página Web para los clientes que utilizan un navegador de Internet convencional e interfaces de presentación de datos para los demás tipos de clientes.

- **Comunicación con los servidores de bases de datos** – Realizan las consultas solicitadas por los clientes a los servidores de bases de datos. El algoritmo que monitorea la carga de los servidores se encarga de dirigir la consulta al servidor adecuado para atenderla.

4.3.2.3 Aplicaciones cliente

Los usuarios que requieran visualizar información sobre su expediente curricular desde una estación de trabajo, lo harán utilizando un software de navegador Web, al cual se le agregará un módulo (plug-in) para permitir la autenticación e identificación al sistema por medio de tarjetas inteligentes. Como se ve en la sección 4.3.3, el uso de tarjetas inteligentes resuelve la necesidad de contar con un mecanismo seguro de autenticación e identificación de usuarios, para poder acceder a los expedientes curriculares. Entre las principales funciones de las aplicaciones cliente se encuentran las siguientes:

- **Establecer comunicación con la tarjeta inteligente**. Esto se realiza por medio de un software intermedio (middleware) para aislar los detalles de comunicación y

gestión de los recursos, tanto de la estación de trabajo como del lector y la tarjeta inteligente, permitiendo así que se utilicen varios tipos de lectores de tarjetas con diferentes interfaces de comunicación. Así mismo, permite el uso de distintos tipos de tarjetas inteligentes y lectores sin realizar cambios en la aplicación. Esto se logra agregando módulos que soporten los distintos lectores y tarjetas inteligentes, conforme se vaya requiriendo. Existen varias iniciativas de la industria que tienen como objetivo lograr interoperabilidad entre los distintos proveedores de lectores y de tarjetas inteligentes, así como de las aplicaciones. Entre tales iniciativas se encuentran la especificación *Personal Computer / Smart Card* (PC/SC) y la plataforma *Open Card Framework* (OCF). Ambas proveen interfaces de programación de alto nivel para, entre otras cosas, facilitar el desarrollo de aplicaciones, lograr interoperabilidad entre los componentes de distintos proveedores y aislar de las aplicaciones los detalles de las capas inferiores de comunicación con los lectores y las tarjetas inteligentes. Aunque ambas iniciativas son similares, se optó por utilizar la especificación PC/SC debido a que, como se ve en la sección 4.3.4, el tipo de tarjetas inteligentes seleccionado para este trabajo es compatible con tal especificación. Para más información sobre PC/SC consulte el anexo C.

- **Comunicación con el servidor de aplicaciones**. La aplicación cliente se encarga de realizar solicitudes de HTTP al servidor de aplicaciones, al igual que lo hace un navegador de Internet, recibiendo como respuesta una página Web que despliega información del expediente curricular. Se utiliza el protocolo de seguridad *Secure Sockets Layer* (SSL), el cual ahora se conoce como *Transport Layer Security* (TLS), para proporcionar una comunicación segura entre la aplicación cliente y el servidor de aplicaciones, utilizando encriptación de datos, autenticación y privacidad de la información.

El diseño también contempla aplicaciones cliente que permiten agregar y realizar cambios en los expedientes curriculares. Estas operarán dentro de las instalaciones de las entidades que verifiquen y administren los expedientes curriculares. Para evitar su uso por personas ajenas a tales entidades, se emplearán mecanismos se seguridad para que

sean operadas únicamente dentro de las instalaciones y por el personal autorizado.

4.3.2.4 Entidades de certificación

En la sección 4.2, al mencionar los requerimientos del sistema, se menciona que es necesario contar con entidades que se encarguen de realizar los procesos de validación y administración de los documentos probatorios. Para cubrir esta necesidad, en este trabajo se propone la creación de entidades, a las que llamamos "*Entidades de Certificación*", que lleven a cabo la validación de documentos probatorios, así como su almacenamiento y administración. La validación de los documentos probatorios se realizará por medio de mecanismos bien definidos que consistan, además de una inspección visual, en la verificación de la información, con las respectivas entidades que los expidan.

Cada entidad de certificación contará con un servidor de aplicaciones y uno o varios servidores de administración de bases de datos. Se propone contar con entidades de certificación regionales, donde cada región corresponda a un estado del país. Esto brindará autonomía a cada estado de la república sobre el manejo y almacenamiento de expedientes curriculares. De ser necesario, se contará con más entidades de certificación por estado. Esto dependerá de las necesidades específicas de cada caso. Lo anterior se podrá llevar a cabo debido a que este diseño es escalable. Esto es, permite agregar entidades de certificación y servidores de réplicas sin que implique cambios en el diseño o un incremento en la complejidad del sistema. Por otro lado, no es necesario que los servidores de réplicas se encuentren en la misma localidad que el servidor de aplicaciones. Estos pueden estar distribuidos en distintas ciudades brindando así mayor seguridad de disponibilidad en caso de que una localidad no esté operando. Incluso, esta arquitectura permite que exista más de un servidor de aplicaciones por cada entidad de certificación sin afectar su operación. De esta manera se puede mejorar al tiempo de respuesta y asegurar disponibilidad en caso de que uno de éstos falle. La figura 4.4 muestra un ejemplo de la asignación de entidades de certificación y la distribución de los servidores que contiene. Para simplificar la figura 4.4, se muestra sólo un servidor de

aplicaciones, el cual corresponde a la entidad de certificación del estado de Baja California. Se observa que esta entidad contiene cuatro servidores de bases de datos interconectados entre sí y que a su vez, se comunican con los servidores de otras entidades de certificación para acceder a los documentos probatorios que almacenan.

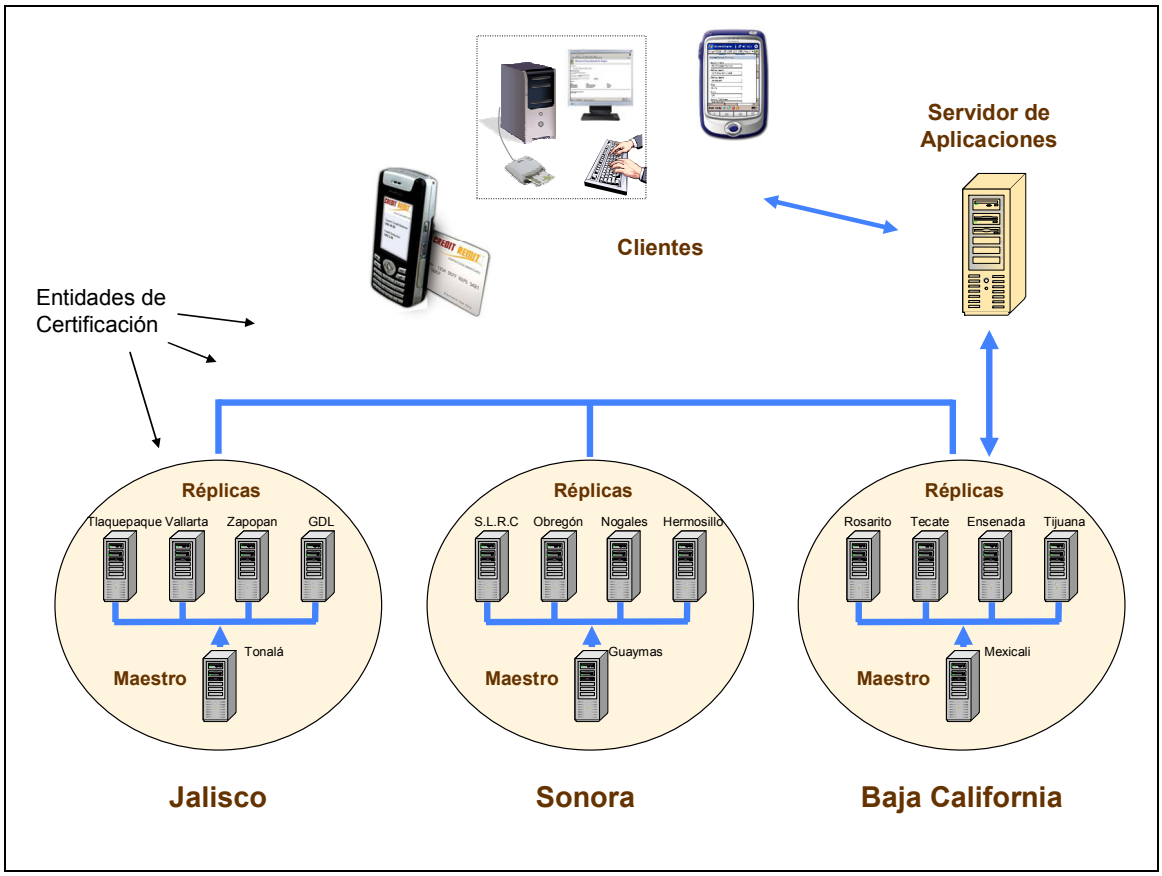

Figura 4.4 Entidades de certificación y distribución de servidores

La asignación del servidor maestro no depende en ningún sentido de la ciudad o lugar donde se encuentre, sino que depende exclusivamente del proceso de selección que se lleva a cabo entre los servidores de esa entidad. Por lo tanto, este proceso es transparente tanto para los usuarios como para los operadores de la entidad de certificación.

4.3.2.5 Distribución de los expedientes curriculares electrónicos

En la sección 4.3.1 se menciona que, para contar con una arquitectura de almacenamiento distribuido, los expedientes curriculares se distribuirán en fragmentos, donde cada fragmento corresponde a un documento probatorio. Cada uno de estos se almacenarán en la entidad de certificación que realice su verificación. En caso de ser requerido, los documentos probatorios podrán ser trasferidos a otra entidad de certificación. Lo mismo aplica para los datos personales del usuario. Cada entidad de certificación tendrá responsabilidad del almacenamiento y administración de los documentos probatorios que verifica. Sin embargo, habrá ocasiones en que se requiera transferir un documento probatorio o los datos personales del usuario hacia otra entidad de certificación por razones de administración. Tal caso se puede presentar cuando una persona solicite un cambio en un documento probatorio debido a errores o que requiera actualización de la información contenida en él. En este caso es más conveniente delegar la responsabilidad a la entidad de certificación que realizará los cambios. Sin embargo, es necesario definir de manera adecuada, las políticas para la transferencia de documentos probatorios y eliminar así cualquier vulnerabilidad en la seguridad del sistema.

Cuando un profesionista acude a una entidad de certificación y solicita por primera vez el almacenamiento de sus documentos probatorios, se genera un documento que contiene sus datos personales. Tal documento servirá como punto de partida para acceder a sus documentos probatorios que se almacenen en el sistema. El mecanismo para relacionar los documentos probatorios con los datos personales del usuario consiste en el uso de identificadores para cada documento probatorio. La figura 4.5 un ejemplo la distribución de un expediente curricular y los documentos probatorios que contiene, así como los identificadores para cada documento probatorio.

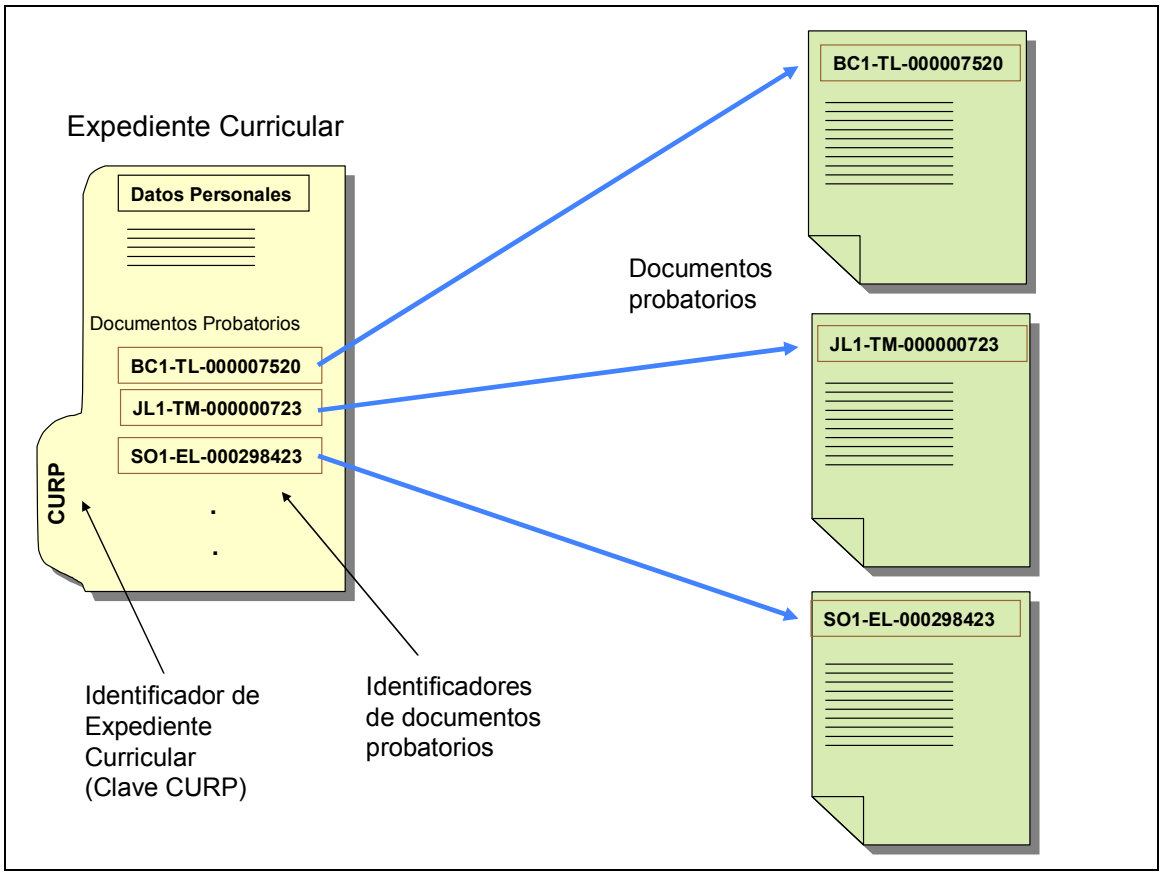

Figura 4.5 Distribución de un expediente curricular y sus documentos probatorios

Conforme un profesionista agregue documentos probatorios al sistema, se agregarán los identificadores en el documento que almacena sus datos personales. No hay límite en la cantidad de documentos que se pueden agregar a un mismo expediente curricular pues, como se ve en la sección 4.3.7, se utiliza una estructura de almacenamiento que es extensible. En la figura 4.5 se observa que el identificador de documento probatorio está compuesto por trece dígitos, los cuales se describen a continuación:

- Los tres primeros caracteres corresponden al identificador de entidad de certificación en donde se encuentra almacenado el documento probatorio. Este se compone de los dos caracteres del código de entidad federativa, seguido por un tercer caracter que permite unicidad en caso de que exista más de una entidad de

certificación por entidad federativa.

- Los dos caracteres que le siguen identifican al tipo de documento. Esto permitirá brindar información sobre los tipos de documentos probatorios que el profesionista tiene almacenados, sin necesidad de descargarlos. Además permite un mejor manejo de la información, ya que funciona como índice para optimizar búsquedas en la base de datos. Entre algunos ejemplos de tipos de documentos se encuentran los siguientes:

    - TL – Título de licenciatura.
    - TM – Título de maestría.
    - CD – Certificado de diplomado
    - EL – Experiencia laboral.

- Nueve dígitos que identifican al documento en particular. Este es un número consecutivo que se genera cuando se agrega un documento probatorio al sistema. El contar con 9 dígitos permitirá al sistema identificar hasta mil millones de documentos probatorios de cierto tipo por cada entidad de certificación. Es un número muy extenso, pero asegura que no se tendrá que cambiar la estructura de almacenamiento por razones de diseño en los identificadores.

En la figura 4.5 se puede observar que se utiliza un identificador de expediente curricular que corresponde a la Clave Única de Registro de Población (CURP) del usuario. El CURP es un instrumento que sirve para registrar en forma individual a todos los habitantes de México, nacionales y extranjeros, así como a las mexicanas y los mexicanos que radican en otros países, en los registros de personas de las dependencias y entidades de la Administración Pública Federal. La clave contiene 18 elementos de un código alfanumérico. De ellos, 16 son extraídos del documento probatorio de identidad de la persona (acta de nacimiento, carta de naturalización, documento migratorio o certificado de nacionalidad mexicana), y los dos últimos los asigna el Registro Nacional

de Población (SEGOB, 2006). Como ejemplo de éxito en la implementación de este identificador único, se encuentra al estado de Colima, el cual ha logrado que el 98% de sus habitantes cuente con su clave CURP (Gobierno del Estado de Colima, 2007). Por lo tanto, el utilizar la clave CURP permite contar con un identificador único que garantiza que no se repetirá en todo el sistema.

4.3.3 Seguridad en los enlaces de comunicación

4.3.3.1 Uso de redes privadas virtuales en Internet

En la sección 4.3.2 se describió una arquitectura compuesta por servidores de bases de datos y servidores de aplicaciones que estarán distribuidos por entidades de certificación. Esta distribución implica el uso de enlaces de comunicación entre las redes de servidores de bases de datos de las distintas entidades de certificación, así como enlaces entre los servidores de aplicaciones y los clientes. El utilizar enlaces dedicados para comunicación entre las entidades de certificación no sería una opción viable ya que resulta muy costoso. Actualmente la red pública Internet nos brinda una infraestructura de enlaces redundantes y de bajo costo para comunicar dispositivos de distintos lugares del mundo. Es por esto que se deben aprovechar las ventajas que brinda la comunicación a través de Internet. Entre una de estas ventajas se encuentra el que cualquier persona en el mundo se pueda conectar a un sitio de Internet, siempre y cuando exista un proveedor del servicio en su área. Internet es el lugar virtual común donde todo el mundo es bienvenido para hacer negocios, comunicarse, buscar información, o simplemente, divertirse navegando por la red. Sin embargo, también contiene un gran potencial para el uso indebido, el abuso y la actividad criminal (Strassberg, K., Gonder, R., Rollie, G., 2003). El contar con enlaces que utilicen esta red pública representa muchos riesgos en cuanto a la seguridad de la información. Los mecanismos para determinar quienes tienen acceso a la información se vuelven cada vez más complicados debido a las vulnerabilidades que tienen los sistemas actuales. El sistema que almacena y administra expedientes curriculares no se debe exponer a un riesgo de tal magnitud. Una persona que lograra acceder al sistema sin autorización, pudiera tener acceso a visualizar y modificar tanto los expedientes

curriculares, como los mecanismos para protegerlos. Es por esto que se requiere contar con mecanismos para proveer enlaces seguros de comunicación entre las distintas entidades de certificación. Por otro lado, se requiere que los distintos tipos de clientes, incluyendo instituciones educativas, empresas y usuarios móviles, puedan acceder al sistema para visualizar los expedientes curriculares, sin que implique para ellos gastos adicionales, ya sea por la instalación y configuración de software adicional o por costos de infraestructura.

Para resolver lo anterior, se optó por utilizar enlaces de Redes Privadas Virtuales o VPN (por sus siglas en inglés de *Virtual Private Network*). Una VPN crea un túnel virtual que conecta a dos puntos. La información viaja en forma cifrada de tal manera que los usuarios de la red pública no puedan interpretarla si logran interceptarla (Bradley, 2007).

Existen muchos productos de proveedores que ofrecen hardware, software, cifrado y esquemas de autenticación para la tecnología de las VPN, por lo tanto es difícil elegir el más apropiado, ya que cada uno brinda distintas características que resultan en ventajas y desventajas de acuerdo a la aplicación donde implementen. Las redes VPN tradicionales se basan en el Protocolo de Seguridad de Internet (IPSec) para proveer un túnel de comunicación entre dos puntos. IPSec opera en la tercera capa (capa de red) del modelo de referencia OSI (por sus siglas en inglés de *Open System Interconnection*) brindando seguridad a la información que viaja entre dos puntos, sin que se encuentre asociado a alguna aplicación en específico ya que está basado en brindar comunicación de red a red, dejando todos los servicios abiertos. La mayoría de las implementaciones de VPN basado en IPSec, requieren de software adicional. Esto brinda una capa extra de seguridad debido a que se debe contar con el software apropiado para lograr el enlace, además de conocer la configuración para que opere correctamente. La desventaja de esto es el costo adicional que implica proveer y configurar este software en las aplicaciones cliente (Bradley, 2007). Por lo tanto, implementar enlaces VPN que utilizan IPSec resulta más apropiado para enlaces fijos donde se requiera un nivel de seguridad muy alto y controlable.

Por otro lado, existe otro tipo de enlace VPN muy utilizado el cual está basado en el Protocolo de Capa de Socket Segura o SSL (por sus siglas en inglés de *Secured Socket Layer*). En el capítulo III, sección 3.6 se mencionan sus características y la manera en que opera. El protocolo SSL está orientado a ser utilizado en enlaces entre navegadores y servidores Web. Este tipo de enlace tiene la ventaja de ser independiente de la plataforma y la mayoría de los navegadores de Internet actuales cuentan con el software cliente necesario para operar SSL. Además, permite un control de acceso más preciso, ya que provee túneles de comunicación para ciertas aplicaciones en específico, en vez de permitir un enlace a la red de la institución o empresa, como en el caso de los VPN basados en IPSec. De esta manera, los usuarios que se enlacen por medio de SSL, podrán acceder únicamente a las aplicaciones que se habiliten en el servidor. Una desventaja de utilizar enlaces SSL es que los usuarios no tendrían acceso a otros recursos de la red como impresoras y archivos compartidos, ya que está orientado a aplicaciones Web donde se requiere software de navegación por Internet (Bradley, 2007).

Cada una de estas soluciones brinda ventajas y desventajas, dependiendo del tipo de aplicación en donde se vayan a implementar. En el diseño del sistema de expedientes curriculares se requiere contar con enlaces seguros entre los distintos tipos de clientes y los servidores de aplicación. Para este tipo de enlaces resulta más conveniente utilizar VPN basado en SSL. De esta manera, cualquier usuario podrá conectarse al sistema desde una estación de trabajo o dispositivo móvil y visualizar su expediente curricular. Esto únicamente requerirá que las estaciones de trabajo y los dispositivos móviles cuenten con software para navegación Web y soporten autenticación basada en SSL.

4.3.3.2 Conectividad entre clientes y entidades de certificación

Para el caso de la conectividad entre las entidades de certificación, se utilizarán enlaces VPN basados en IPSec. Esto permitirá una comunicación segura entre los distintos servidores de bases de datos a través de la red pública Internet. En este caso no resulta

complicado instalar y configurar software adicional en los servidores, ya que estos estarán fijos y controlados en todo momento.

Además de contar con enlaces VPN basados en SSL y IPsec, se debe contar con firewalls (corta fuegos) en los puntos de conexión con la red externa de cada una de las entidades de certificación, con políticas bien definidas sobre qué servicios pueden ser accedidos y quiénes tienen acceso a ellos. También es muy importante cumplir con reglamentos de seguridad en todos los niveles de la red, así como llevar un procedimiento de mantenimiento, tanto del sistema de bases de datos, como de las políticas de seguridad. La figura 4.6 muestra el diagrama simplificado de conectividad entre los clientes y las entidades de certificación.

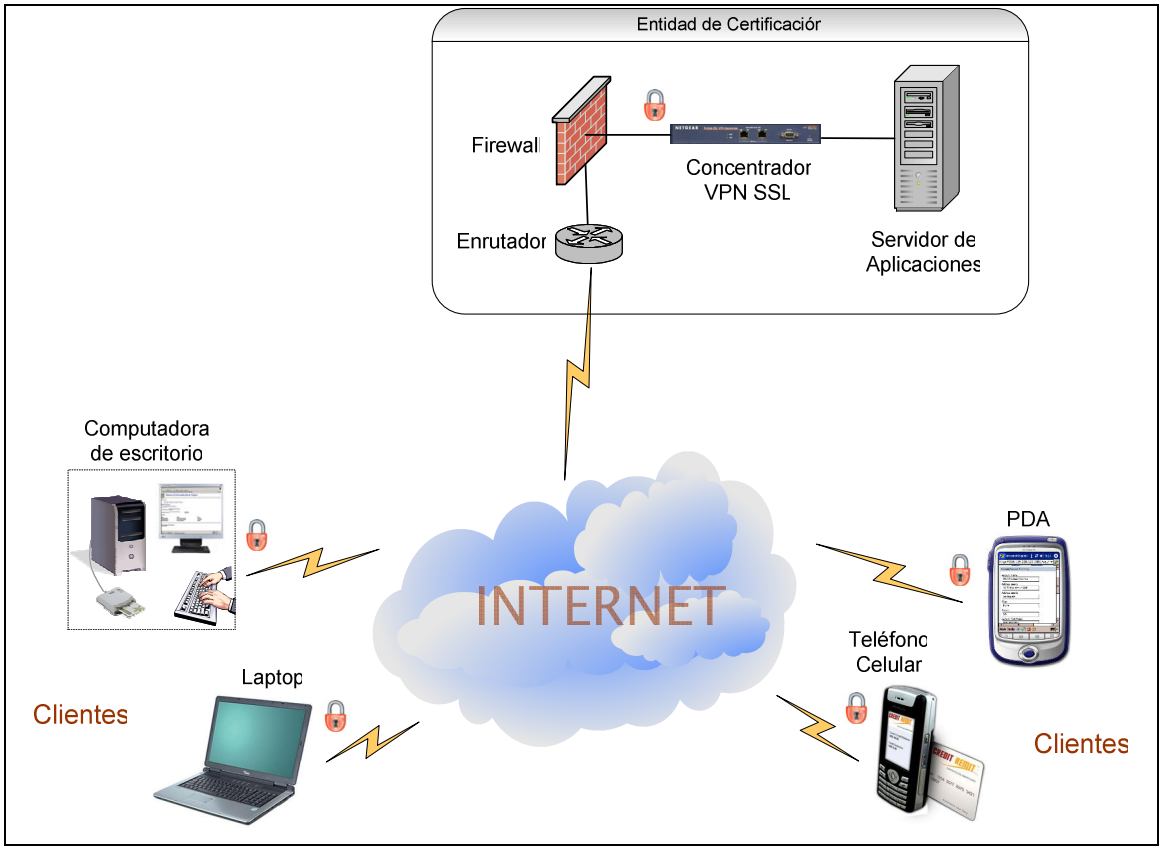

Figura 4.6 Diagrama de conectividad entre los clientes y las entidades de certificación

Como primer punto de acceso a una entidad de certificación se encuentra el enrutador. Este dispositivo interactúa con otros enrutadores para permitir comunicación con otras redes. Una de sus principales funciones consiste en determinar las mejores rutas por las cuáles viajan los paquetes de información a través del conjunto complejo de redes que forman Internet (Norton, 2001). Aunque este dispositivo no está orientado a brindar seguridad en los enlaces, la mayoría de los enrutadores actuales incluyen funciones tales como el filtrado de paquetes por medio de reglas de acceso y traslación de direcciones de Internet.

Después del enrutador se encuentra el firewall. Este dispositivo tiene la función de controlar el acceso hacia dentro y hacia fuera de la red que conforma la entidad de certificación. Se pretende que el firewall opere como un muro de protección contra los diferentes tipos de ataques externos a los que se enfrentan las redes actuales. Como ejemplos de estos ataques se encuentran, el engaño de direcciones IP (*IP spoofing*) en donde un usuario externo hace creer a los servidores y equipos de red que los está accediendo desde la misma red a la que éstos pertenecen. Esto le abre las puertas para tener acceso a equipos que han sido restringidos por origen de conexión. Otro ataque común es el rastreo de conexiones (*eavesdropping*) en donde un usuario reúne datos sobre conexiones entre dos puntos para posteriormente acceder a la red. Un tercer ejemplo de ataque común son los que resultan a consecuencia de vulnerabilidades de los servicios y aplicaciones. Si un usuario externo encontrara una falla o hueco en algún servicio o aplicación, pudiera comprometer en gran medida la seguridad de todo el sistema. Por último, los ataques de rechazo de servicio o DoS (por sus siglas en inglés de *Denial of Service*) en los cuales un atacante o grupo de atacantes coordinan el envío masivo de paquetes a un equipo de red o servidor de una empresa, logrando que se saturen las conexiones y obligue a que los recursos no se encuentren disponibles para los usuarios (Red Hat Inc., 2005).

La mayoría de los firewalls consisten en el filtrado de paquetes, utilización de proxies (intermediarios) o la combinación de ambos, así como otras funciones que brindan seguridad tales como el enmascaramiento y traslación de direcciones y puertos de red. El

filtrado de paquetes opera por medio de reglas de acceso basadas en distintas variables de los encabezados de las capas de red y de transporte (tercera y cuarta capa del modelo de referencia OSI, respectivamente). Entre estas variables se encuentran la dirección de red tanto de fuente como destino, así como protocolo y puertos utilizados. Algunos firewalls implementan el filtrado basado en el estado del paquete. Esto es, verifican los encabezados de las capas de red y capas de aplicación del modelo OSI, para verificar si es legítimo y que los protocolos están operando como se esperaba. El filtrado de paquetes es independiente de la aplicación y se manejan dos formas de operación en cuanto a las reglas de acceso. Una de ellas consiste en permitir el tráfico en general y negar únicamente el acceso a aquellas conexiones que estén especificadas en las reglas de accesos. La otra consiste en negar todo acceso y permitir únicamente aquellas conexiones que estén incluidas en las reglas de acceso. Esta última provee más seguridad, pues se niega el acceso a todo lo que no se encuentre especificado. Sin embargo, puede resultar complejo configurar las reglas de acceso para este tipo, ya que se deben identificar correctamente los servicios, protocolos y condiciones para aquellas conexiones que se les brinde acceso (MOREnet 2003).

Los firewalls tipo proxy operan como intermediario entre los clientes y los servidores. Trabaja en los niveles de aplicación del modelo de referencia OSI. Cuando un cliente solicita un servicio al servidor desde una red insegura, el proxy recibe la solicitud y analiza su validez de acuerdo a un conjunto de reglas. Si es válida, la reenvía al servidor. La respuesta del servidor al cliente se lleva de forma inversa. De esta manera no hay un enlace directo entre el cliente y el servidor. Por lo tanto, se brinda cierto grado de seguridad al analizar la información en los niveles de aplicación, ya que permite que el proxy tome decisiones en base a su contenido (MOREnet 2003). El utilizar un firewall que implemente las funciones de filtrado de paquetes y funciones de proxy brindará la protección necesaria para evitar los distintos tipos de ataques que se mencionaron anteriormente.

Como segunda capa de seguridad se encuentra el dispositivo que proporciona una VPN basada en seguridad SSL. De esta manera los datos que se transfieren entre los clientes y

el servidor de aplicaciones viajan en forma cifrada, protegiendo su integridad y privacidad. Además, el utilizar VPN con SSL, permite autenticar al servidor de aplicaciones y restringir las aplicaciones que los clientes pueden tener acceso. En el diagrama de la figura 4.7 se muestra la implementación de un dispositivo que provee enlaces VPN basados en SSL. Existen dispositivos que realizan varias funciones para brindar seguridad en redes, incluyendo firewall, enlaces VPN y enrutador. En este diseño se muestran tales funciones implementadas en dispositivos independientes. Esto con el objetivo de presentar una idea clara sobre los mecanismos de seguridad de acceso a la red y a los servidores.

4.3.3.3 Conectividad entre las entidades de certificación

Los servidores de bases de datos de todas las entidades de certificación estarán interconectados entre sí para que tengan acceso a los distintos fragmentos que conforman los expedientes curriculares. Esto formará una red grande de servidores. La información que se transfiere entre las bases de datos de las distintas entidades de certificación es muy sensible, ya que pertenece a la de los documentos probatorios, así como información de los usuarios y llaves de encriptación para los procesos de autenticación. Para poder transferir esta información por la infraestructura de la red pública Internet, es necesario utilizar mecanismos para proteger su integridad y privacidad. El uso de enlaces VPN basados en IPSec proveerá un túnel de comunicación segura entre las entidades de certificación. Los enlaces serán fijos y controlados, por lo que utilizar software adicional y configuración no representará un costo adicional. Al igual que los enlaces entre los clientes y los servidores de aplicaciones, se utiliza un firewall con filtrado de paquetes y funciones de proxy para proveer la protección necesaria contra los distintos ataque externos más comunes. La figura 4.7 muestra el diagrama de conectividad entre las entidades de certificación utilizando enlaces VPN basados en IPSec.

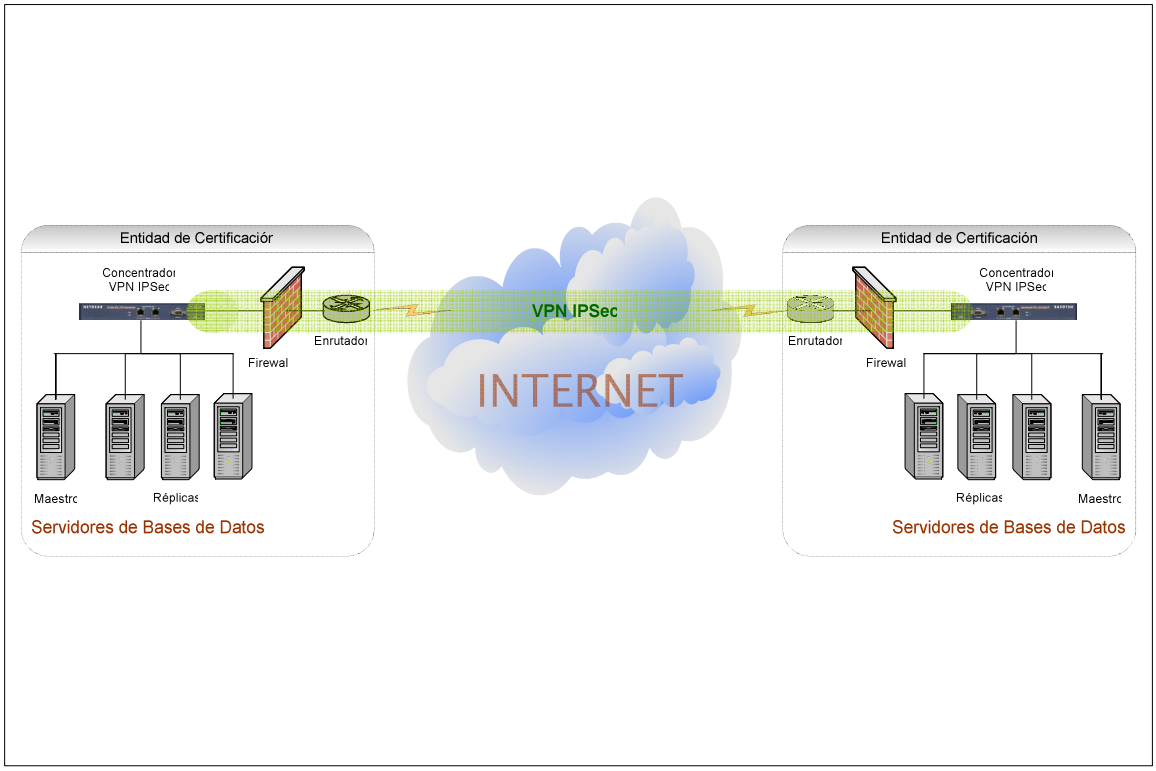

Figura 4.7 Diagrama de conectividad entre entidades de certificación

Para simplificar el diagrama de la figura 4.7, se omite el servidor de aplicaciones. Este servidor también forma parte de la conectividad por medio del VPN IPSec. Sin embargo, el firewall limita el acceso a sus servicios para que, los servidores de otras entidades de certificación, puedan acceder únicamente al servicio que les informa quién es el servidor maestro en ese momento y cuál es la carga de procesamiento de cada réplica. Tal información es necesaria para proveer balance de carga en los servidores.

La figura 4.8 muestra el diagrama de conectividad tanto para enlaces entre las entidades de certificación y los clientes, como entre las distintas entidades de certificación.

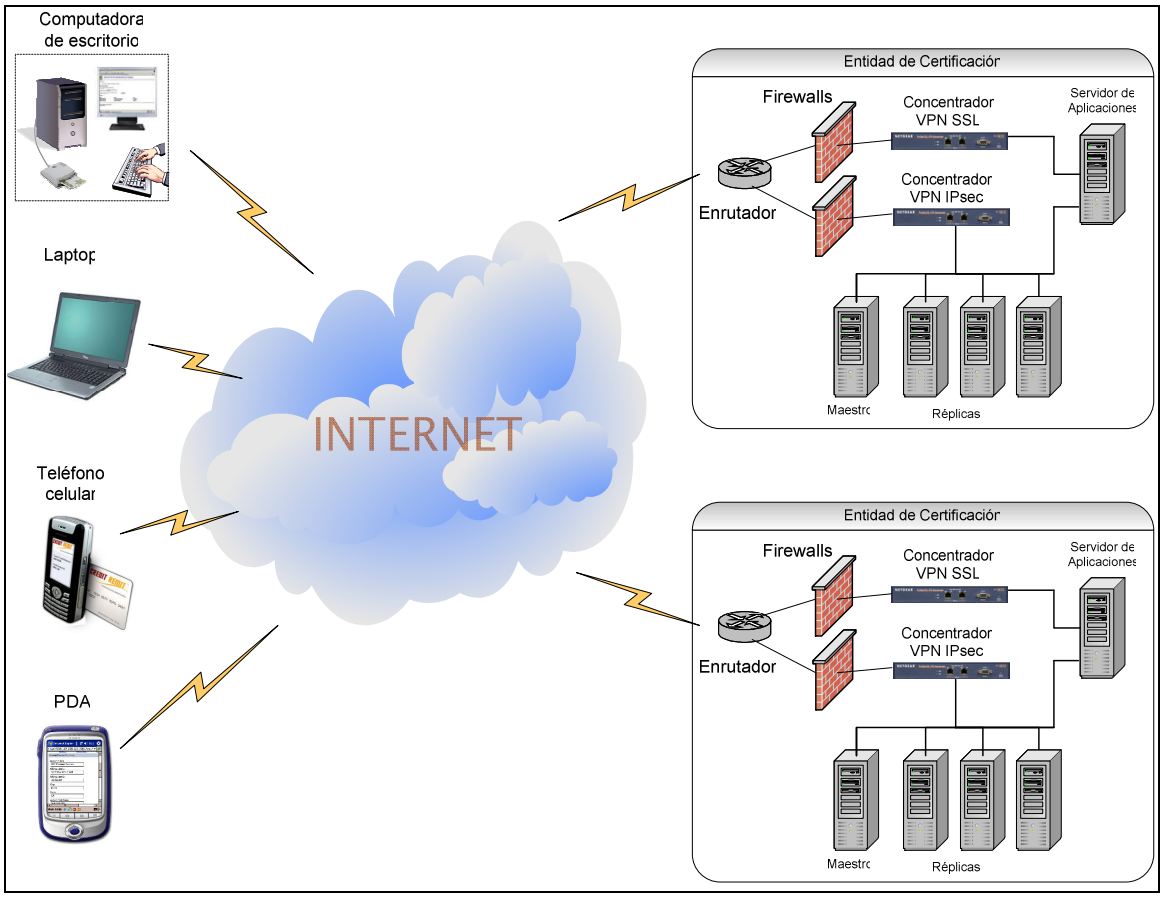

Figura 4.8 Diagrama de conectividad de las entidades de certificación

4.3.4 Mecanismo de autenticación e identificación

Este trabajo de investigación se centra en el uso de tarjetas inteligentes ya que es un elemento importante en el sistema de almacenamiento de expedientes curriculares electrónicos. En el capítulo II se mencionó en gran parte el uso de la tecnología de las tarjetas inteligentes, en aplicaciones donde operan como dispositivos de almacenamiento de información segura y portátil, así como mecanismo de autenticación e identificación. Son muchas las aplicaciones de uso masivo que respaldan la confiabilidad en el uso de estos dispositivos. Tal es el caso de los bancos e instituciones de gobierno, quienes confían en esta tecnología para manejo de dinero y de información confidencial. En la sección 4.2 se mencionó como requisito el contar con un mecanismo que garantice que la consulta de información relacionada con comprobantes de estudios de cierta persona, sea

accedida solamente si la persona en cuestión está presente y se ha identificado exitosamente. Se propone el uso de tarjetas inteligentes como mecanismo de autenticación con el sistema de almacenamiento y recuperación de expedientes curriculares.

4.3.4.1 Análisis de kits de desarrollo de aplicaciones con tarjetas inteligentes

Para seleccionar qué tipo de tarjeta inteligente utilizar, se analizaron distintos tipos existentes, tomando en cuenta sus características principales tales como capacidad de memoria, mecanismos de seguridad de los datos, compatibilidad con estándares y costo. Durante la investigación se encontró que existen algunas empresas que venden kits (paquetes) de desarrollo para evaluación y elaboración de aplicaciones prototipo. Tales kits incluyen generalmente dispositivos lectores de tarjetas inteligentes, software para desarrollar aplicaciones y algunas tarjetas inteligentes de muestra para la realización de pruebas. El proceso ideal para seleccionar uno de estos kits consiste en definir primero las características que se desea que tengan, posteriormente comparar los existentes y seleccionar el que más cumpla con tales características. Sin embargo, en este trabajo de investigación se optó por conocer primero las características de los kits existentes y luego hacer un balance entre lo que se requiere y lo que estos kits pueden ofrecer. Posteriormente el diseño se ajusta de acuerdo a las características con las que se cuente. El costo por tarjeta es un factor muy importante en la decisión para su selección. Considerando que cada profesionista poseerá una de estas tarjetas, se debe seleccionar una opción que no sea muy costosa, pero que a su vez cumpla con los requerimientos del sistema. Existe un gran número de compañías que fabrican tarjetas inteligentes, sin embargo son pocas las que venden estos kits de desarrollo de aplicaciones de sus tarjetas.

Un kit de desarrollo se compone básicamente de los siguientes elementos:

1. Dispositivo de aceptación de tarjeta (CAD), comúnmente conocido como “lector” de tarjetas. Aunque este dispositivo se utiliza tanto para leer como para escribir

datos en la tarjeta, el nombre "lector" ha sido utilizado por la mayoría de las fuentes bibliográficas.

2. Software de desarrollo de aplicaciones, controladores del lector (drivers), ejemplos de aplicaciones y tutoriales.
3. Tarjetas inteligentes de muestra.

A continuación se mencionan las características de tres productos que se consideraron los más adecuados para la elaboración del proyecto, además de que fueron los que publicaron sus características en catálogos en línea. Posteriormente se menciona un análisis de la selección del kit de desarrollo que se utilizará en el sistema de almacenamiento y recuperación de expedientes curriculares.

1. - Empresa Axalto

Esta empresa tiene mucha experiencia en la fabricación de tarjetas inteligentes y en los últimos 25 años ha vendido más de 3 mil millones. Fabrica tarjetas para varios sectores incluyendo el sector financiero, público, redes, telefonía y transporte, entre otros. Entre sus productos, vende kits de desarrollo para elaborar distintos tipos de aplicaciones. El de mayor interés para este proyecto es un modelo que incluye software y lector para desarrollar aplicaciones que utilizan tarjetas inteligentes Java (conocidas como Java Cards). Estas tarjetas contienen un intérprete de un subconjunto de la máquina virtual de Java que se ejecuta por encima del sistema operativo de la tarjeta, facilitando así su portabilidad y programación. El kit de desarrollo que tiene disponible en sus catálogos es el siguiente:

Cyberflex Access SDK 4.5 - Este kit de desarrollo opera bajo la plataforma Microsoft Windows y utiliza tarjetas JavaCard con capacidades de multifunción y criptografía. Provee servicios de seguridad como la generación de certificados digitales y verificación, autenticación, cifrado y descifrado. Soporta los siguientes tipos de tarjetas inteligentes:

Cyberflex Access – Son tarjetas tipo JavaCard con las siguientes características:

- Memoria EEPROM en versiones de 16K, 32K y 64K.
- Compatibles con la Plataforma Global (Open Platform) y JavaCard v.2.1.1.
- Estándares ISO 7810, 7813, 7816 1-2-3 y 4 (parcial).
- Especificaciones FIPS 140-2 nivel 3 validado.
- Uso de clave secreta (PIN) con bloqueo de intentos programable.
- Firma digital RSA y verificación con llave de hasta 1024 bits.
- Criptografía DES, 3-DES (CBC-EBC) y hash SHA-1.
- Programación orientada a objetos.
- Número de serie único por tarjeta.
- Capacidades para carga y descarga de applets.
- Generación real de número aleatorios.

Cyberflex Access e-gate – Tienen las mismas características que *Cyberflex Access*, pero además incorporan una interfaz USB para conexión directa a la PC.

Cryptoflex – Estas tarjetas son ideales para aplicaciones donde se requiera utilizarlas como llave de acceso en infraestructuras de llave pública. Tienen las siguientes características:

- Memoria EEPROM de 32K.
- Estándar ISO 7816-1,2,3,4 con T=0.
- Especificaciones FIPS 140-2 nivel 2.
- Generación de llaves RSA (512, 768, 1024 y 2048 bits).
- Generación de llaves DES (56 y 112 bits).
- Cálculo de firmas (512, 768, 1024 y 2048 bits).
- Carga de datos cifrados (con algoritmos DES y tripe-DES).
- Generación de número aleatorios.
- Algoritmos Hash SHA-1.
- Uso de clave secreta (PIN).
- Restricción de acceso de comandos de archivos.

Cryptoflex e-gate – Tienen las mismas características que *Cyptoflex*, pero además incorporan interfaz USB para conexión directa a la PC por medio de un adaptador.

Lector – El kit de desarrollo no incluye lector de tarjetas, sólo el software de desarrollo.

Tarjetas – El kit de desarrollo no incluye tarjetas de muestra. Se deben adquirir por separado. Las tarjetas *Cyberflex Access e-gate* tienen un costo de 23 dólares estadounidenses cada una (consultado el 30 de mayo de 2006 del sitio Web de la empresa Axalto).

2. - Empresa Cardlogix

Esta empresa cuenta con un kit de desarrollo llamado "*Smart Toolz*" que facilita el desarrollo de aplicaciones que utilizan tarjetas inteligentes ya que incluye lector, software de aplicación y ejemplos de programas. El paquete completo tiene un precio de $398 dólares estadounidenses (consultado el 20 de mayo de 2006, del sitio Web de la empresa Cardlogix). El software de desarrollo opera bajo la plataforma Microsoft Windows incluyendo las versiones para servidor y para la plataforma .Net. Las características que menciona el fabricante son las siguientes:

- Permite el diseño de estructura de los archivos de la tarjeta inteligente.
- Permite el diseño y personalización de bases de datos para utilizarse con tarjetas inteligentes.
- Contiene aplicaciones listas para implementarse en tarjetas de salud, monedero electrónico y de membresía.
- Utiliza cifrado de archivos.
- Lenguajes de programación para el desarrollo de aplicaciones: Delphi y Visual C++, con ejemplos de programas.

El fabricante no especifica las características del lector, pero menciona que soporta tarjetas de memoria y tarjetas con microprocesador. Incluye cinco tarjetas con microprocesador. Sin embargo, no especifica a detalle sus características. Sólo menciona que utilizan mecanismos de seguridad con algoritmos criptográficos DES, Triple-DES y FlowFish, además de contar con capacidades para compresión de registros.

El fabricante puede proveer más información técnica respecto a las tarjetas inteligentes que incluye y los mecanismos que utiliza para la seguridad, además de contener información sobre cómo se lleva a cabo la personalización del sistema de archivos que la tarjeta tendrá. Sin embargo, para poder obtener esta información, la empresa solicita el envío de un documento donde se firme un acuerdo de confiabilidad entre el cliente y la empresa, el cual incluye el no difundir información respecto a detalles técnicos de los productos que vende la empresa.

3. - Empresa ACS

Esta empresa vende un kit de desarrollo que tiene un costo de $99 dólares estadounidenses (consultado el 20 de marzo de 2006 del sitio Web de la empresa ACS). El software de desarrollo opera bajo las plataformas de Microsoft Windows, MacOs y Linux. Contiene algunos programas de ejemplo de aplicaciones entre los que se encuentra una tarjeta para escuelas que funciona como monedero electrónico e identificación de alumnos. También incluye una aplicación que simula un casino virtual operado por tarjetas inteligentes en la modalidad de monedero electrónico. El código fuente de tales ejemplos está disponible en los lenguajes Visual Basic, Visual C++, Delphi y Power Builder 5.0.

El kit contiene dos lectores de tarjetas inteligentes. Uno se utiliza para tarjetas de contacto convencionales y el segundo se utiliza para tarjetas tipo SIM, tal como aquellas que se utilizan en los teléfonos celulares. Ambos lectores tienen las siguientes características:

- Interfaz que cumple con el estándar 7816-1/2/3.

- Compatibilidad con la especificación PC/SC
- Soporta tarjetas con protocolos T=0 y T=1 y voltajes de 1.8V, 3V, y 5V
- Interfaz para conexión a la computadora por puerto USB 2.0.

También incluye 20 tarjetas inteligentes de muestra, de las cuales la mitad son de memoria que utilizan un mecanismo de protección de escritura y seguridad de datos, mientras que la otra mitad son tarjetas inteligentes con microprocesador del tipo *ACOS2*. Entre sus características se incluyen las siguientes:

- Memoria EEPROM de 8KB para datos de usuario.
- Compatibles con el estándar ISO 7816-3, protocolo T=0.
- Utilizan el algoritmo de encriptación DES y 3-DES para autenticación mutua por medio del almacenamiento de llave secreta.
- Contienen 5 códigos secretos de aplicación para lectura y escrita de archivos.
- Implementan número de clave secreta (PIN) para identificación de usuario.

4.3.4.2 Selección del kit de desarrollo

Al inicio de este proyecto se contempló el utilizar la tecnología de las JavaCard y se realizó una investigación sobre las empresas que venden kits con este tipo de tarjetas. Sin embargo se encontraron muchos obstáculos ya que hay muy pocos de estos productos, además de que algunas empresas no brindan suficiente información como para poder realizar una evaluación previa a su adquisición. Se optó por buscar en otros países además de Estados Unidos y se obtuvieron los mismos resultados, la información que proveen no es suficiente. Por otro lado, se observó que actualmente la tecnología de tarjetas con Java está siendo orientada para aplicaciones en dispositivos móviles, tal como los productos de GSM, la telefonía celular y las telecomunicaciones. Sin embargo, no se encontró suficiente bibliografía relacionada con los mecanismos de autenticación e identificación para aplicaciones similares a la de este trabajo. Esto es, se encontró teoría sobre su funcionamiento, estándares y tendencias, pero fue muy escasa la documentación

sobre aplicaciones reales y actuales que se orientaran a esquemas de almacenamiento de información en forma segura. Aún, después de haber encontrado estos obstáculos, se optó por analizar las características del kit de desarrollo que vende la empresa *Axalto*. Este kit brinda todas las características en cuanto a capacidad de almacenamiento, costo y aspectos de seguridad. Sin embargo, se observó que no incluye tarjetas de muestra como lo hacen otros productos y el precio de cada una de estas es de 23 dólares estadounidenses. Este precio se considera elevado para el tipo de aplicación que se está desarrollando.

La segunda opción con la que se cuenta corresponde a kit de desarrollo de la empresa *Cardlogix*. Este tiene un precio de $398 dólares estadounidenses y además de contar con características de seguridad, lo que representa la mayor ventaja es el hecho de contar con la opción de personalizar la estructura de archivos que reside en la tarjeta inteligente. Esto nos permitiría adaptar la tarjeta a nuestro diseño en vez de ajustarse a la forma en que la tarjeta almacena la información. Además, contiene aplicaciones diseñadas previamente para el sector salud y otras como monedero electrónico y tarjeta de membresía, lo que facilitaría el diseño de la aplicación. Sin embargo, la empresa no especifica más características sobre el tipo de tarjetas inteligentes que contiene, ni sus mecanismos de funcionamiento y de diseño.

El hecho que motivó a descartar este producto para la elaboración de este proyecto, es de que la empresa requiere, para poder obtener más información o comprar sus productos, que el cliente firme un acuerdo donde se compromete a no difundir detalles técnicos de los productos que la vende la empresa. Como parte de los objetivos de este trabajo es el de dar a conocer las tecnologías existentes para la elaboración de aplicaciones con tarjetas inteligentes y mencionar los mecanismos empleados para el diseño del sistema de almacenamiento y recuperación de documentos electrónicos curriculares, incluyendo aspectos de la seguridad, la investigación se vería opacada si omitiéramos detalles técnicos de los productos comerciales utilizados.

Como mejor opción, se determinó utilizar el kit que vende la empresa ACS. Este, además de tener un precio accesible de $99 dólares estadounidenses, contiene muchas de las

características que se requieren para un prototipo inicial de este proyecto. Las tarjetas con microprocesador que incluye de muestra, cuentan con algoritmos de encriptación para autenticación con la aplicación que interactúa, así como clave secreta (PIN) para identificar al dueño de la tarjeta. Sus 8 Kbytes de memoria son suficientes para la información que se pretende almacenar en la tarjeta y además tienen protección de archivos internos por medio de claves de acceso. La empresa provee las especificaciones de las tarjetas que incluye y explica a detalle su sistema de almacenamiento de archivos, así como los aspectos de seguridad. Por otro lado, sus tarjetas no son tan costosas como la JavaCard de la empresa *Axalto*, sino que tienen un precio de $2.99 dólares estadounidenses cuando se adquieren en pocas cantidades. Este precio baja si se adquieren en grandes cantidades. Por otro lado, su sistema de autenticación utiliza criptografía simétrica DES y 3-DES y aunque se mencionó en el capítulo III que la criptografía asimétrica tiene varias ventajas sobre la simétrica entre ellas, el permitir el uso de firmas digitales, mecanismos de aceptación y mejor administración de llaves, el contar con criptografía simétrica 3-DES brindará un mecanismo muy seguro para los fines del sistema propuesto en este trabajo. Lo anterior es debido a que no se requiere el uso de firmas digitales ni mecanismos de aceptación. Sólo se requiere contar con un mecanismo de autenticación que sea seguro.

En conclusión, el kit de desarrollo de la empresa *ACS* es el más adecuado para utilizarse como punto de partida para el diseño del mecanismo de autenticación e identificación del sistema propuesto en este trabajo. La selección de la tarjeta inteligente del tipo *ACOS2*, determinará en gran parte la forma en que se almacenarán los datos en ella, así como el mecanismo de autenticación que será empleado. El mecanismo de autenticación mutua que estas tarjetas proveen se basa en la verificación de llaves secretas compartidas por la tarjeta y la aplicación de la terminal o sistema al cual se conectan.

Por otro lado, la empresa *ACS* ha desarrollado nuevos productos de estas tarjetas inteligentes, entre las que se encuentran la *ACOS3* y la *ACOS5*. Tales tarjetas proporcionan mejores mecanismos de encriptación, así como más capacidad de almacenamiento de datos, además son compatibles con las aplicaciones desarrolladas

para tarjetas inteligentes del tipo *ACOS2*. Esto brinda la confianza de contar con un tipo de tarjetas inteligentes que se encuentra en mejora constante para brindar mayor seguridad, capacidad y eficiencia.

4.3.4.3 Autenticación e identificación usando tarjetas inteligentes

La tarjeta inteligente será la llave de acceso a los expedientes curriculares y solamente se podrá realizar cualquier proceso, ya sea una consulta, modificación o almacenamiento de nuevos documentos probatorios, si la tarjeta se encuentra insertada en el lector y se ha verificado la identidad del portador. Este proceso es similar a las tarjetas bancarias, las cuales son necesarias a la hora de realizar una transacción en un cajero automático.

El proceso de autenticación mutua consiste de una serie de pasos en donde se realiza una comprobación de llaves secretas entre la tarjeta inteligente y el sistema. Este intercambio de llaves se realiza de una manera segura utilizando números aleatorios y encriptación de datos con el algoritmo de criptografía simétrica 3-DES. En la sección 3.4.3.1 se describe el proceso de autenticación de tarjetas inteligentes usando criptografía simétrica. Para las tarjetas inteligentes tipo ACOS2, el proceso es similar en que también utiliza criptografía simétrica, pero con la diferencia de que estas tarjetas utilizan dos llaves de encriptación. Una llave identifica a la tarjeta mientras que la otra a la terminal a la cual se conecta. Esto permite que la terminal (o aplicación de la terminal) se autentique con una sola llave de encriptación, mientras que cada tarjeta puede tener una distinta. Tanto la tarjeta, como la terminal, deben mantener el par de llaves en su memoria. A estas llaves se les conoce como *llave de la terminal* (K_T) y *llave de la tarjeta* (K_C). Tales llaves son almacenadas al momento de personalizar la tarjeta (véase anexo A) y posteriormente no pueden ser leídas ni modificadas por ninguna aplicación, sino que son utilizadas internamente como parte del proceso de autenticación mutua.

Como en este diseño, el proceso de autenticación se llevará a cabo entre la tarjeta y el servidor de aplicaciones, nombraremos a estas dos llaves de la siguiente manera: K_T para

referirnos a la llave de la tarjeta y K_S para referirnos a la llave del servidor. Este tipo de tarjeta tiene un generador de números aleatorios que es utilizado en el proceso de autenticación, al cual llamaremos RND_T. De la misma forma, el lado del servidor debe generar números aleatorios, por lo que se empleará el término RND_S para referirnos a tal número.

Si el proceso de autenticación mutua es exitoso, se genera una llave que representa a la sesión y es utilizada para cifrar y descifrar datos durante la misma. Una sesión se inicia al concluir exitosamente el procedimiento de autenticación mutua y termina al retirar o reiniciar la tarjeta.

Cada tarjeta inteligente contendrá una llave de encriptación distinta a las demás. Esto aumentará la seguridad, ya que si por alguna razón se lograra descifrar la llave que pertenece a la tarjeta de un usuario, esto no atentaría contra la seguridad de la información de los demás usuarios. Y así, en caso de que sucediera un problema de seguridad con una tarjeta en particular, se borraría de los servidores el registro de esa tarjeta inteligente en particular y se le asignaría una nueva al usuario, con otra llave de encriptación. Para lograr esto, el servidor debe generar una llave de encriptación distinta para cada tarjeta inteligente que vaya a utilizar en el sistema. Sin embargo, necesita contar con un mecanismo que identifique a la tarjeta inteligente antes de iniciar el proceso de autenticación mutua, y que la relacione con las llaves de encriptación y el usuario que la porta. Como cada tarjeta inteligente tiene almacenado un número de serie único (proporcionado por el fabricante), utilizaremos esta característica para identificarlas en el proceso de autenticación mutua y que de esta manera el servidor determine qué llave para el proceso de autenticación mutua le corresponde a esa tarjeta inteligente en particular. Para esto, el servidor contará con una relación del número de serie de la tarjeta, con su respectiva llave de encriptación. La figura 4.9 muestra un ejemplo de la relación de los números de serie de las tarjetas inteligentes y sus respectivas llaves de encriptación. La clave CURP será la llave para relacionar la tarjeta inteligente y las llaves de encriptación con el expediente curricular del usuario.

No. de serie (8 bytes hex)	**ID de usuario** (Clave CURP)	**Llave de Tarjeta (K_T)** (16 bytes hex)
81 0F 17 A1 DC 0E A0 00	CARJ730814HBCSML09	90 45 67 45 34 67 56 89 FE 56 EF 67 90 23 56 DE
A1 0F 17 A1 DC 0E A0 00	RACO780914HBCSML04	45 86 34 56 23 A5 AC 67 60 12 A4 5E 10 64 10 B1
21 0F 17 A1 DC 0E A0 00	SICA711212HBCSML906	14 58 39 20 E9 F7 CA 45 48 29 30 49 58 F7 7E A5
C9 0E 17 A1 DC 0E A0 00	RORM801211MDFSBL09	FE EF 51 09 48 23 18 48 EE A7 84 99 AA E4 34 11
FF F9 BF F7 3E FF FF FF	TACA691114HBCSML01	01 11 34 86 38 FF A6 A9 09 00 47 39 48 AB
FF B5 E7 7F FC 9F FF BE	SOQL720624HBCSML03	11 11 46 69 47 00 FF 44 68 47 77 7F CD AA 65 88
FF BF FF F7 3E DF FF FF	FISL760712HBCSML08	46 57 68 AD AA BC 67 47 88 93 47 F5 7E 9A AD 77

Figura 4.9 - Ejemplo de relación de números de serie, usuarios y llaves de encriptación

La relación anterior se almacenará en cada servidor de base de datos del sistema. Es la única información que se encontrará duplicada en todas las entidades de certificación. Esto permitirá encontrar la información del usuario de manera inmediata cuando se solicite un expediente curricular. Antes de poder realizar alguna consulta o modificación de un expediente curricular, se debe pasar primero por el proceso de autenticación de la tarjeta e identificación de la persona que la porta. El servidor de aplicaciones no solicitará información sobre los expedientes curriculares a los servidores de bases de datos, sino hasta que verifique la autenticidad de la tarjeta inteligente y valide el registro del usuario. Además, la tarjeta inteligente no podrá iniciar ninguna operación, incluyendo el proceso de autenticación con el sistema, sin antes verificar que el usuario haya escrito correctamente su número de identificación personal. El diagrama de secuencia que aparece en la figura 4.10 muestra los pasos que sigue el proceso de autenticación mutua entre la tarjeta inteligente y el servidor de aplicaciones.

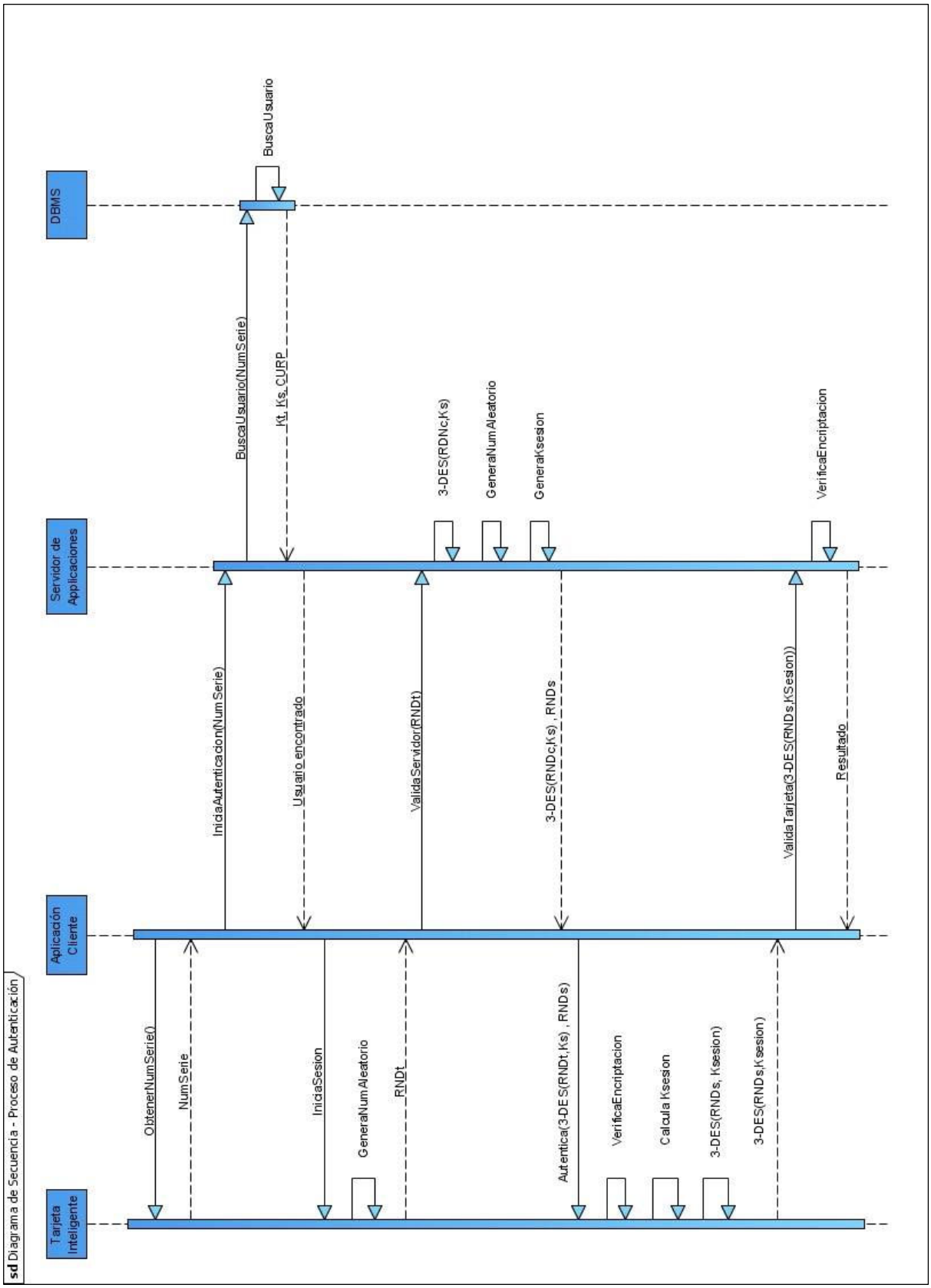

Figura 4.10 Diagrama de secuencia del proceso de autenticación mutua

El proceso de autenticación mutua entre la tarjeta inteligente y el servidor de aplicaciones comienza después de que la aplicación detecta que una tarjeta ha sido insertada en el lector y se encuentra en un estado de espera de comandos. Básicamente, el comportamiento es el de una relación maestro-esclavo, donde la aplicación inicia la comunicación (maestro) mientras la tarjeta inteligente está en estado de espera para responder a la petición de comandos (esclavo). Posterior a esto procede el proceso de validación del portador de la tarjeta inteligente, el cual consiste del uso de la clave PIN. Si el usuario no introduce la clave correctamente, la tarjeta niega toda comunicación posterior y se debe volver a insertar la tarjeta para empezar de nuevo el proceso[1]. Las tarjetas tipo *ACOS2* tienen la opción para programar, durante la etapa de personalización, el número de intentos de introducción de clave PIN que el usuario puede hacer. Si se excede de la cantidad programada, la tarjeta se vuelve inservible y se debe solicitar una nueva. Los pasos que proceden a la validación del usuario se describen a continuación:

1. La aplicación le solicita a la tarjeta inteligente obtener su número de serie. Este es un número único por cada tarjeta, el cual es de 8 bytes y se encuentra almacenado en un registro de acceso libre. Esto es, no se requiere el proceso de autenticación ni el envío de llaves secretas para tener acceso a él. Además, este dato no puede ser modificado o eliminado, ya que es de sólo lectura (para más información sobre la estructura de los registros y funcionamiento de la tarjeta *ACOS2*, consulte ACS, 2000).

2. La aplicación cliente solicita al servidor de aplicaciones de la entidad de certificación a la que se conecta, iniciar el proceso de autenticación mutua. Al solicitar esto, le envía como parámetro el número de serie de la tarjeta en cuestión.

3. El servidor de aplicaciones abre una conexión con el servidor de bases de datos local (DBMS) y le solicita la información del usuario que corresponde al número de serie. El servidor de bases de datos en cuestión puede ser tanto el maestro como alguna réplica, dependiendo de la carga de consultas en ese momento. El DBMS realiza una búsqueda en la relación de usuarios de su base de datos y si encuentra al usuario, le

[1] Esta parte se omite en el diagrama de la figura 4.10 para simplificar la explicación del proceso.

responde enviándole las llaves de encriptación tanto de la tarjeta (K_T), como del servidor (K_S), así como el identificador de usuario (CURP). Si no encuentra al usuario, se lo notifica al servidor de aplicaciones.

4. El servidor de aplicaciones le notifica al cliente que el usuario fue encontrado, como respuesta del inicio del proceso de autenticación mutua.

5. El cliente le solicita a la tarjeta inteligente que inicie sesión.

6. La tarjeta inicia el proceso de sesión, el cual es parte necesaria de su proceso de autenticación. Una vez que se establezca la sesión, esta permanecerá hasta que la tarjeta se extraiga del lector o hasta que se reinicie por medio de la aplicación cliente.

7. La tarjeta genera un número aleatorio (RNDt) como respuesta del inicio de sesión.

8. El cliente al recibir el número aleatorio generado por la tarjeta, le solicita al servidor de aplicaciones que realice el proceso de validación, el cual implica cifrar este número aleatorio con la llave del servidor y devolverlo a la tarjeta para que ésta pueda comparar si ambas partes comparten la misma llave.

9. El servidor de aplicaciones cifra el número aleatorio (RNDt) con la llave del servidor (Ks) utilizando el algoritmo de encriptación 3-DES. El resultado se lo devuelve a cliente junto con un número aleatorio (RNDs) que el servidor genera y además le envía la llave de sesión, la cual es calculada en base a las llaves almacenadas K_T y K_S. La llave de sesión se utilizará posteriormente para cifrar y descifrar los datos que se transfieren entre la tarjeta y el servidor, brindando privacidad en la información.

10. El cliente le solicita a la tarjeta que ejecute su proceso de autenticación, el cual consiste en comprobar si el número aleatorio que le envió en un principio al servidor, fue cifrado con la misma llave de encriptación que ella almacena. Para lograr esto, la tarjeta al igual que el servidor, cifra el número aleatorio inicial. Si ambos números

son iguales, entonces significa que ambas partes comparten la misma llave de encriptación. De lo contrario, la tarjeta devuelve un error y se mantiene bloqueada a transacciones posteriores. Hasta este momento solamente la tarjeta ha comprobado la identidad del servidor. Los siguientes pasos complementan el proceso, ya que ahora es el servidor quien debe comprobar la identidad de la tarjeta.

11. La tarjeta calcula la llave de sesión, usando los mismos datos que utilizó el servidor.

12. Con esta llave de sesión la tarjeta cifra el número aleatorio que generó el servidor y lo devuelve a la aplicación en respuesta de la petición del proceso de autenticación.

13. La aplicación cliente recibe este dato y se lo envía al servidor de aplicaciones solicitándole que lo valide.

14. El servidor de aplicaciones cifra de la misma manera el número aleatorio y lo compara con el resultado que generó la tarjeta. De esta forma comprueba la identidad de la tarjeta por medio de la comparación de ambos resultados.

15. El servidor de aplicaciones le notifica a la aplicación cliente sobre el resultado del proceso de autenticación. Si este se llevó a cabo correctamente, se puede proceder con la transacción en cuestión, ya sea la consulta o una modificación en el expediente curricular de ese usuario, según sea el caso.

4.3.5 Datos de la tarjeta inteligente

La sección anterior presentó el uso de tarjetas inteligentes como un mecanismo seguro de autenticación e identificación con el sistema, para el acceso a los expedientes curriculares. En el capítulo II se menciona que existen tarjetas inteligentes con capacidades de almacenamiento de información que varían entre pocos bits hasta varios megabytes. Esta característica de las tarjetas motivó la idea de almacenar una copia del expediente curricular de los usuarios en sus tarjetas inteligentes, brindando la ventaja de

que pudiera ser consultado en una modalidad "offline" (sin conexión). Es decir, desde terminales que no estén conectadas a las bases de datos de expedientes curriculares. Sin embargo, el kit de desarrollo que se seleccionó para este trabajo, el cual cubre las necesidades en cuanto a mecanismo de autenticación, identificación y costo, cuenta con sólo 8 KB de memoria. Esto limita la cantidad de información que se puede almacenar en el expediente curricular. Por lo tanto, se optó por eliminar la opción de incluir una copia del expediente curricular en la memoria de la tarjeta inteligente. Esto se reflejará en el hecho de que siempre debe de existir una conexión a las bases de datos que almacenan los expedientes curriculares cuando se requiera consultar alguno de estos. Lo anterior tiene la ventaja de brindar más seguridad, ya que de esta forma se obliga a que la aplicación cliente que consulta la información, acceda al sistema y verifique la identidad de la persona, antes de que se proceda a desplegar su expediente curricular.

Sin embargo, se optó por incluir entre los datos, información de identificación del portador de la tarjeta inteligente, la cual no requerirá del proceso de autenticación mutua, ni claves para accederla. Entre esta información se incluyen datos personales, como nombre completo, domicilio, números telefónicos y tipo de sangre. El hecho de incluir esta información en la memoria de la tarjeta, le brindará la ventaja de poder utilizarse como tarjeta de identificación, incluso en aplicaciones que no tengan conexión con el sistema de expedientes curriculares. Esto es, se podrán desarrollar aplicaciones sencillas en donde se requiera leer información de la persona e incluso integrar estas aplicaciones con otras más grandes para aprovechar el uso de esta información. Entre algunos ejemplos de aplicaciones que podrán hacer uso de esta característica se encuentran las siguientes:

- **Sistemas de emergencia** – Las ambulancias y hospitales podrán extraer información de la persona en caso de una emergencia, utilizando un lector portátil de tarjetas inteligentes.

- **Registro a eventos** – Se podrá utilizar la tarjeta para identificarse a la hora de registrarse a eventos como congresos, seminarios, conferencias, etc. El usuario

presentará su tarjeta y la persona encargada del registro obtendrá de manera instantánea los datos de la persona.

Como se menciona en el análisis de kits de desarrollo de la sección 4.3.4.1, la tarjeta ACOS2 de la empresa *ACS Ltd*. tiene 8 KB de memoria para datos de usuario. Este espacio se organiza de acuerdo a la configuración de la tarjeta, la cual se realiza durante la etapa de personalización. El espacio de memoria se divide en archivos y cada uno de éstos se compone de registros. Existe la restricción de que cada registro puede tener una longitud máxima de 32 bytes, además de que la cantidad y longitud de los registros que contendrá la tarjeta, debe definirse desde su etapa de personalización y no podrá ser alterado una vez que la tarjeta se utilice en forma normal por el usuario final. Por lo tanto, es de suma importancia definir claramente los requerimientos de almacenamiento de la información personal durante la etapa de diseño para determinar la estructura de los archivos que contendrán estas tarjetas, ya que cualquier cambio que se requiera en ellas, implicará programar nuevas tarjetas a todos los usuarios.

Las tarjetas inteligentes, además de almacenar llaves de autenticación, códigos de acceso, clave PIN y otros datos que la identifican de las demás (véase Anexo A), almacenarán en archivos de usuario los siguientes datos:

1. **Fecha y hora de última modificación** – Esta información incluye la fecha y hora de la última modificación del expediente curricular y de los datos personales del usuario de la tarjeta inteligente. Se almacenará en un archivo restringido que solamente podrá ser leído o modificado cuando se ha autenticado a una entidad de certificación y se ha introducido la clave PIN. Esta fecha se utilizará como parte de un mecanismo para verificar si la tarjeta no ha sido clonada.

2. **Datos personales del usuario**. Contendrá un documento en formato XML con información que identifica al usuario portador de la tarjeta. Esta información podrá ser leída desde aplicaciones sin necesidad de autenticación con el sistema central. Sin embargo, la escritura o modificación de esta información requerirá

autenticarse con el sistema incluyendo el uso de una clave secreta para escritura, además de la introducción de la clave PIN por parte del portador de la tarjeta.

3. **Archivo de validación DTD**. Se utilizará para definir la estructura de los bloques del documento XML que contiene los datos personales del usuario definiendo así, los elementos válidos y el tipo de datos que se puede utilizar. Este archivo servirá como mecanismo para que las aplicaciones que lean la información del usuario, comprueben la validez de los campos de datos que se están enviando. Esto permite flexibilidad en cuanto al desarrollo de nuevas versiones de la estructura de los datos personales, sin que se tengan que hacer cambios en las aplicaciones cliente.

4.3.6 Diseño del esquema de almacenamiento de la información personal en la tarjeta

Debido a que el diseño de la estructura de archivos en la tarjeta requiere determinar el tamaño de los mismos desde la etapa de personalización, se requirió un análisis para calcular el espacio que ocupan los datos personales del usuario. Se tomó como referencia la estructura de información personal en una tarjeta de salud (HealthCard) que aparece en Rodríguez (2001) para definir los campos requeridos.

En algunos campos se utilizó codificación de la información la cual deberá ser interpretada en el lado de la aplicación que accede a la misma. Esto con la finalidad de utilizar menos espacio y dejar bytes libres para almacenar otros elementos.

La tabla 4.1 muestra una estimación del espacio requerido para la información personal del usuario, así como descripción y ejemplo de cada campo.

Campo	Tipo	Tamaño (bytes)	Ejemplo
CURP	char	18	CARJ730814HBCSML09
Nombre completo	char	50	Julio César Castillo Ramírez
Fecha de nacimiento	date	8	14081973 (14 agosto de 1973)
Ciudad de nacimiento	char	20	Mexicali
Estado de nacimiento	char	20	Baja California
País de nacimiento	char	2	MX (México)
Sexo	char	1	M (Masculino)
Domicilio - País	char	2	MX (México)
Domicilio – Estado	char	20	Baja California
Domicilio - Ciudad	char	20	Mexicali
Domicilio - Colonia	char	20	Residencias
Domicilio - Calle	char	20	Olga
Domicilio- Número	char	6	84-C
Teléfono fijo	char	20	(686)566-42-98
Teléfono móvil	char	20	(686)135-9211
Tipo de Sangre	char	3	O+
Total = **250** bytes			

Tabla 4.1 Estimación de espacio requerido para datos personales

El análisis de la tabla 4.1 nos permite ver que se requieren aproximadamente 250 bytes para almacenar los datos personales de un usuario. A manera sencilla, se pudiera utilizar un registro de 32 bytes de la memoria de la tarjeta por cada campo de la tabla, resultando en un total de 17 registros. El campo del nombre completo excede estos 32 bytes, por lo que se pudiera dividir en dos, usando uno para los nombres y otro para los apellidos. Sin embargo, este esquema de almacenamiento está muy restringido en cuanto a que no se puede aumentar el tamaño de los campos una vez que se definan y además, no permite agregar más campos en caso de que se requieran.

Para este proyecto se decidió utilizar un esquema de almacenamiento que permitiera variar la longitud de los campos, de acuerdo a como se vaya requiriendo. De esta manera, no se tendrá que limitar el espacio para cada campo, haciendo más eficiente el uso de la memoria. Sin embargo, el análisis anterior se realizó con el propósito de calcular una estimación del espacio que ocupará el archivo que almacene la información personal del usuario ya que, en las tarjetas inteligentes tipo ACOS2, no se permite modificar la capacidad ni estructura de los archivos, una vez que se realiza el proceso de

personalización. El uso de un esquema basado en XML (por sus siglas en inglés de *Lenguaje de Marcado Extensible*) será la mejor opción para estructurar esta información. Este esquema trae consigo varias ventajas, incluyendo el poder repetir campos sin necesidad de reservar el espacio previamente, como lo es el caso de las personas que cuentan con varios números telefónicos o que requieran incluir más detalle sobre su dirección actual. Por otro lado, se pueden definir otros campos para brindar más información, como por ejemplo la profesión de la persona, información de contactos y números telefónicos adicionales. Cabe mencionar que si utilizamos etiquetas para cada campo, tendremos que diseñarlas de una longitud mínima posible para evitar consumir mucho espacio. Por ejemplo, para almacenar el nombre de una persona usando XML, se escribiría de la siguiente manera:

```
<usuario>
  <nombre>
    Julio César
  </nombre>
  <paterno>
    Castillo
  </paterno>
  <materno>
    Ramírez
  </materno>
</usuario>
```

La aplicación que lee esta información debe realizar la verificación de las etiquetas por medio de un analizador de sintaxis.

Basándonos en la forma en que definiremos las etiquetas, podemos determinar la manera en que almacenaremos los datos del usuario en la tarjeta y calcular de nuevo el espacio estimado. Para esto, debemos redefinir los campos que contendrá el documento para hacer más óptima la estructura de los datos y de esta manera facilitar la administración de la información. Por ejemplo, para realizar búsquedas por nombre, es más óptimo si el campo de nombre se divide por nombres y apellidos.

En el anexo D se muestra un ejemplo de estructura de los datos personales de un usuario. Se observa que en esta definición de estructura se repiten algunas etiquetas, como por

ejemplo en la información de un contacto, donde también utiliza etiquetas del nombre, dirección y teléfono. El utilizar un esquema de esta manera nos permitió que la estructura sea flexible y que se pueda extender de acuerdo a la cantidad de información que requiera incluir el usuario. Es decir, habrá usuarios que requieran menos campos o menos información en los campos que otros.

En el ejemplo del anexo D el usuario incluyó los números telefónicos tanto de su casa, como de su oficina y celular, información de un contacto para referencia en casos de emergencia, y además sus dos títulos de grado (licenciatura y maestría). Estos datos tienen el propósito de presentar al usuario de manera general, pero no detalla sus estudios ni su experiencia laboral. En dado caso de que requiera demostrar la validez de sus documentos probatorios con alguna empresa o institución, se debe llevar a cabo el proceso de visualización de su expediente curricular, el cual consiste en autenticarse al sistema e introducir su clave PIN. Por otro lado, los datos personales, aunque no tienen restricción de lectura, no pueden ser alterados al menos que el usuario lo solicite y acuda a una entidad de certificación para llevar a cabo tal proceso.

El archivo resultante del ejemplo del anexo D requiere 1161 bytes de almacenamiento. Considerando que esta estructura es flexible y que pueda extenderse, debemos tomar en cuenta los casos extremos y dejar suficiente espacio adicional. Además es importante considerar futuras actualizaciones de la estructura (más etiquetas) y como se mencionó anteriormente, que el tamaño de archivo debe ser especificado desde su programación inicial, por lo tanto resultaría costoso reemplazar todas las tarjetas de los usuarios si se encontrara la situación de excedernos en el espacio reservado. Como resultado de este análisis, se determinó que el tamaño del archivo que contendrá el documento XML con información personal del usuario sea de 2 Kbytes.

Anteriormente se mencionó que las tarjetas *ACOS2* almacenan la información en archivos conformados por registros, los cuales pueden medir un máximo de 32 bytes. Como la cantidad de registros que requerirá cada usuario, dependerá de la cantidad de información que incluya, la aplicación que lea esta información, tendrá un mecanismo

sencillo para saber cuantos registros debe leer. Si definimos el tamaño de estos registros a su capacidad máxima (32 bytes), entonces el documento XML para el usuario del ejemplo del anexo D, requerirá un total de 37 de estos registros. Para hacer más sencillo el proceso de lectura del documento XML con la información personal del usuario, se determinó que el número de bytes que éste requiera, se almacene en el primer registro del mismo archivo, tal como lo muestra la figura 4.11. De esta manera, las aplicaciones que requieran leer la información personal del usuario, podrán saber cuantos registros y cuantos bytes de ese archivo en particular se deben leer. Los registros que aparecen en la figura 4.11 están basados en el ejemplo del anexo D. Los dos primeros bytes del primer registro (registro 0) están asignados para almacenar el número de bytes que requieren los datos personales. La aplicación que lee la información, utilizará este número para calcular cuantos registros y cuántos bytes del último registro se deben leer. En el ejemplo, el registro 37 requirió solamente 9 bytes. El resto debe ser ignorado por la aplicación.

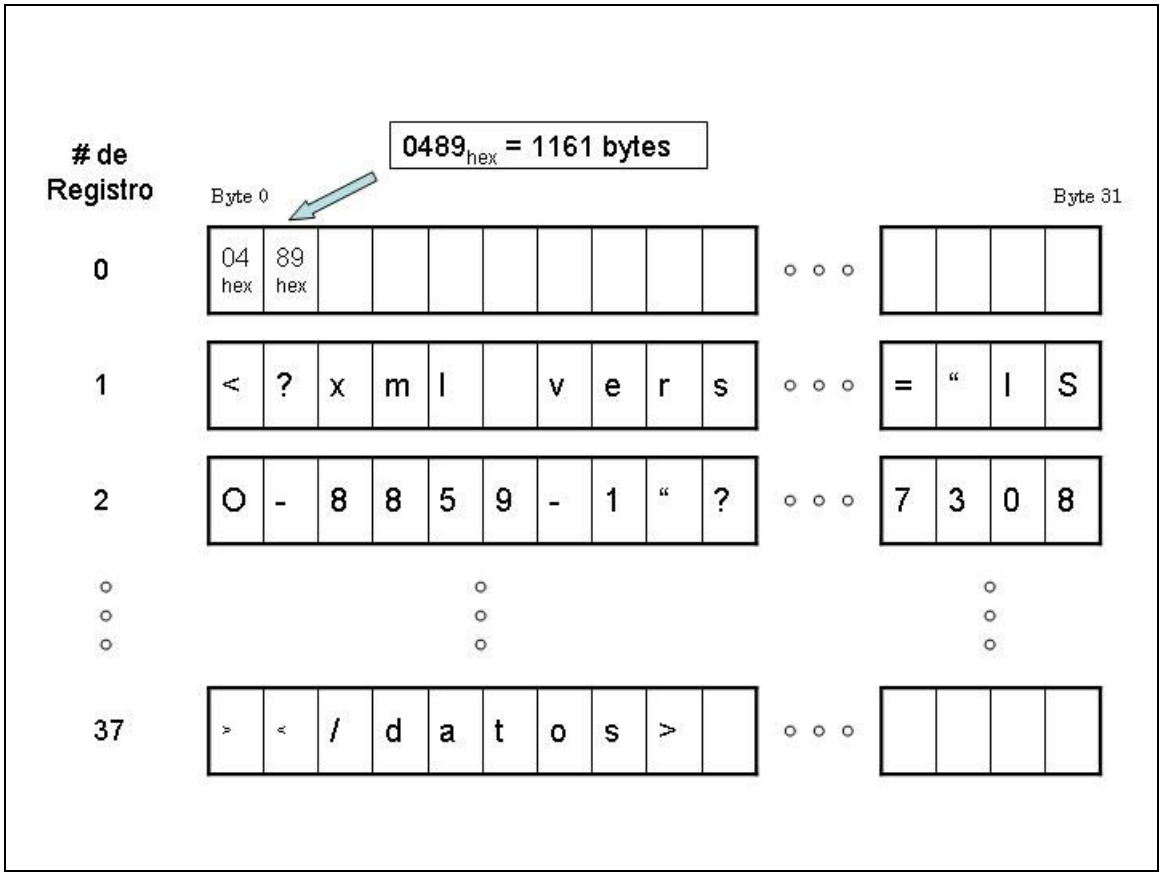

Figura 4.11 – Almacenamiento de datos personales en los registros de la tarjeta inteligente

Para poder asegurar que el documento XML cumpla con la estructura definida, se requiere contar con un mecanismo de validación. El uso de esquema similar a los archivos DTD (Definición de Tipo de Documento) para documentos XML resolverá esta necesidad. La aplicación que lea, despliegue o manipule esta información, deberá utilizar este mecanismo para asegurar que los datos han sido almacenados de manera adecuada. Esto es, que además de verificar que el documento está bien formado, que también cumpla con la definición de su estructura, como se mencionó anteriormente.

El DTD se almacenará en un archivo de la tarjeta de la misma manera en que se almacenará el documento XML con los datos personales. Esto es, almacenando la información en registros de 32 bytes cada uno y utilizando el primer registro para almacenar la cantidad de bytes que utiliza. Tal archivo tendrá los mismos atributos que el archivo que contiene los datos personales del usuario. Es decir, será de sólo lectura y para poder ser modificado se requerirá autenticarse al sistema de una entidad de certificación, junto con la introducción de la clave PIN y los privilegios necesarios de operador del sistema cliente para realizar tal modificación. Además sólo se permitirá la modificación del DTD si existe uno más actualizado. La aplicación que acceda tanto el documento XML como el DTD, se encargará de realizar el proceso de validación.

El DTD que se propone incluir en la tarjeta inteligente tiene una longitud de 933 bytes. Debido a que esta información pudiera incrementarse en futuras versiones, se determinó que el archivo que lo almacena tenga una capacidad de 2 Kbytes, brindando así suficiente espacio para almacenar versiones posteriores. La primera versión del DTD propuesto se muestra en la figura 4.12. Este archivo DTD define la estructura que debe tener el documento XML que contiene los datos personales del usuario. En su definición se determina el orden en que deben aparecer los campos que contiene el documento, así como la cantidad de veces que deben aparecer. Como se observa en el listado de la figura 4.12, algunos campos como la clave CURP, datos del usuario y fecha de actualización, son obligatorios y deben aparecer una sola vez, mientras que la información sobre contactos que el usuario quiera agregar, así como números telefónicos y grados académicos, son opcionales y sin límite de la cantidad a incluir.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!-- DTD - Datos personales - ACOS2 -->
<!-- V.1.0 - 12mayo2006 -->

<!ELEMENT datos (curp,usuario,contacto*,actualizacion)>
<!ELEMENT usuario
(nombre,paterno,materno?,nacimiento,sexo,domicilio,tel*,sangre?,grado*)>
<!ELEMENT nacimiento (fecha,ciudad,estado,pais)>
<!ELEMENT domicilio (ciudad,estado,pais,colonia,calle,num)>
<!ELEMENT tel (tipo,numtel,ext*)>
<!ELEMENT contacto (nombre,paterno,materno?,domicilio,tel*)>
<!ELEMENT curp (#PCDATA)>
<!ELEMENT nombre (#PCDATA)>
<!ELEMENT paterno (#PCDATA)>
<!ELEMENT materno (#PCDATA)>
<!ELEMENT sangre (#PCDATA)>
<!ELEMENT grado (#PCDATA)>
<!ELEMENT fecha (#PCDATA)>
<!ELEMENT ciudad (#PCDATA)>
<!ELEMENT estado (#PCDATA)>
<!ELEMENT pais (#PCDATA)>
<!ELEMENT colonia (#PCDATA)>
<!ELEMENT calle (#PCDATA)>
<!ELEMENT num (#PCDATA)>
<!ELEMENT sexo (#PCDATA)>
<!ELEMENT tipo (#PCDATA)>
<!ELEMENT numtel (#PCDATA)>
<!ELEMENT ext (#PCDATA)>
<!ELEMENT actualizacion (#PCDATA)>
```

Figura 4.12 - Archivo DTD para validación del documento XML

4.3.7 Diseño de la estructura de expedientes curriculares electrónicos

Anteriormente se mencionó que el sistema propuesto, el cual brindará una alternativa en la verificación de la validez de documentos probatorios tanto de estudios como de experiencia laboral, requerirá el almacenamiento de los mismos en formato digital, utilizando una estructura bien definida y estandarizada para que las distintas empresas, instituciones y usuarios en general, que tengan acceso a esta información, puedan interpretarla de manera eficaz. Como parte del diseño del sistema de almacenamiento de expedientes curriculares electrónicos, se propone el diseño de la estructura de un expediente curricular implementado en el lenguaje de marcado XML. Tal expediente se

almacenará en distintos archivos XML que contendrán datos personales, documentos probatorios de estudios y comprobantes de experiencia laboral.

Antes de comenzar con el diseño del expediente curricular electrónico, se mencionan algunas definiciones para que a partir de estas, se determine que es lo que se almacenará en tales expedientes.

4.3.7.1 Certificado de estudios

Un certificado de estudios es un documento de carácter oficial que acredita la completa superación de una persona en un ciclo de estudios oficiales, expedido por una autoridad competente de acuerdo con la legislación del estado a cuyo sistema educativo pertenezcan dichos estudios (Ibarra, Flores & Castillo, 2005).

4.3.7.2 Expediente curricular

Un expediente curricular integra la información registrada por las organizaciones implicadas en la formación profesional, académica y laboral de una persona, garantizando oficialmente su experiencia, habilidades y conocimientos adquiridos (Ibarra, Flores, Castillo & Castro, 2006).

4.3.7.3 Expediente curricular electrónico

Aunque no se conoce una definición formal para un expediente curricular electrónico, se ha definido, en el contexto de esta investigación, como el conjunto de todos los documentos que conforman un expediente curricular, en un formato que pueda ser almacenado y manipulado por medios electrónicos.

4.3.7.4 Diseño del expediente curricular electrónico

El diseño del expediente curricular está basado en el trabajo realizado por Kelly, Christensen & Miller (2002), al cual nombraron *XMLrésumé* que trata sobre un sistema que utiliza XML y XSL para marcar, agregar metadatos y darle formato a résumés y currículums vitae. Aunque muchas personas tienden a usar los términos résumé y currículum vitae indistintamente, en realidad son dos cosas distintas. El primero se refiere a un resumen de una o dos páginas de las habilidades, experiencia laboral y educación de una persona. En cambio un currículum vitae incluye más detalles sobre el área académica como experiencia en investigación y docencia, publicaciones, presentaciones, afiliaciones, reconocimientos y otro tipo de detalles (Doyle, 2006).

Newfield (2006) menciona que un résumé es un resumen académico y de experiencia laboral elaborado con el propósito de resaltar las habilidades y experiencia orientado a obtener un empleo, mientras que un currículum vitae es una lista para documentar todos los empleos que ha tenido y todos los estudios que ha recibido en su vida.

Como en el diseño de este sistema se pretende almacenar información a detalle relacionada con el área tanto académica como laboral de las personas, utilizaremos el término "expediente curricular" para referirnos al documento que será almacenado en el sistema. Este se asemeja más a la definición de currículum vitae. Cabe mencionar que como este sistema se enfoca a comprobar la validez de documentos probatorios, no se utilizará para almacenar documentación orientada a un perfil en particular, como lo es el caso de los résumés, en los cuales la persona enfoca el contenido a un área en específico, resaltando sus habilidades y experiencia para obtener un empleo, lograr un ascenso, etc. El expediente curricular que se almacenará en este sistema contendrá únicamente documentación oficial expedida por las instituciones educativas y cartas de las empresas donde la persona ha laborado. El diseño del expediente curricular electrónico de este trabajo es un subconjunto del *XMLRésumé*, debido a que se eliminan elementos que no se consideraron necesarios para incluirse en un expediente curricular, además de agregar otros que son requeridos para su administración en el sistema propuesto.

El documento DTD que se publica en el sitio Web de *XMLRésumé*, define varias secciones que se pueden incluir en un résumé o currículum vitae. Entre las secciones se encuentran las siguientes:

- **Objetivo -** Se indica un objetivo para el cual fue elaborado el currículum vitae. Por ejemplo, el obtener un empleo en cierto puesto de una empresa.

- **Historial** – Contiene el historial laboral de la persona. Para cada trabajo que desempeñó (y posiblemente el que aún desempeña) se puede especificar el nombre del patrón, nombre de la empresa, período, proyectos y logros realizados.

- **Grados académico**s – Contiene los grados académicos que ha recibido. Para cada grado recibido se puede especificar la institución donde lo obtuvo, la puntuación obtenida, resultados, nivel y algunas notas.

- **Habilidades** – Permite incluir un conjunto de habilidades que tiene la persona, divididas por áreas.

- **Publicaciones** – Si la persona ha escrito libros o artículos, en esta sección se mencionan.

- **Referencias** – Se menciona información sobre contactos que sirvan de referencia de la persona. Se incluye nombre, dirección, organización y puesto que desempeña.

- **Palabras clave** – Permite incluir palabras que se utilizarán para facilitar las búsquedas en bases de datos.

- **Membresías** – Se mencionan las organizaciones a las que pertenece o ha pertenecido, incluyendo la dirección, período y descripción de actividades.

- **Intereses** – Se mencionan los intereses profesionales que tiene la persona.

- **Reconocimientos** – Se incluyen los reconocimientos que ha obtenido, especificando el título del reconocimiento, organización de donde lo obtuvo, período y descripción.

Además, este DTD permite incluir varios résumés o currículums vitae en un solo documento. Para un listado completo de los elementos que se incluyen en *XMLRésumé*, favor de consultar Kelly, Christensen & Miller (2002).
El expediente curricular electrónico de este trabajo consiste en un documento XML, parecido a *XMLRésumé,* pero en este caso se omite información que oriente el documento hacia un perfil en particular. Esto es, puede contener todos los documentos probatorios digitalizados de la persona, siguiendo un formato único por cada tipo de documento probatorio. Los elementos como objetivos, habilidades, referencias, membresías e intereses que define *XMLRésumé*, no serán relevantes para el objetivo del expediente curricular que se almacenará en las bases de datos de las entidades de certificación.

Tomando como referencia el trabajo realizado por los autores de *XMLrésumé*, junto con un análisis sobre los datos que se incluyen en la mayoría de los documentos probatorios existentes, se determinó que el expediente curricular conste de dos grupos de elementos. El primero contendrá elementos que definen los datos personales del usuario, mientras que el segundo contendrá aquellos que conforman cada documento probatorio. Como no todos los documentos probatorios incluyen la misma información, se determinó crear subconjuntos de elementos para cada tipo de documento probatorio. Cabe mencionar que en este expediente solamente se incluirá información sobre los documentos probatorios que sean reconocidos y validados por alguna entidad de certificación. Los conjuntos de elementos que se incluirán se presentan a continuación:

Datos personales – Son los datos que identifican al usuario. Contiene los siguientes elementos:

- Clave Única de Registro de Población (CURP)
- Nombre completo
- Fecha y lugar de nacimiento
- Sexo
- Domicilio actual
- Números telefónicos
- Tipo de sangre
- Información de contactos (ya sean familiares o amigos)
- Fecha de actualización

Podrá existir duda de porqué se repiten los datos personales que se almacenan en la tarjeta inteligente y en el expediente curricular electrónico. Esto se hizo con la finalidad de que estos datos estén siempre disponibles en las bases de datos y no se requiera presentar la tarjeta inteligente para poder acceder a ellos, en caso de que se realicen búsquedas, estadísticas o mantenimiento de la información. Además sirve como mecanismo para corroborar que los datos sean los correctos, en caso de que exista la duda de que la tarjeta inteligente ha sido alterada. Por otro lado, como se mencionó en la sección 4.3.5, el hecho de almacenar datos personales del usuario en la tarjeta inteligente, permite que se utilice como identificación en sistemas que no tengan conexión a las bases de datos.

Documentos probatorios - Dentro del expediente curricular electrónico se encuentra un conjunto de elementos que muestran información sobre los documentos probatorios que ha presentado el usuario ante una entidad de certificación y que han sido validados. Estos documentos han sido estructurados de tal manera que permiten presentar todo tipo de información relacionada a ellos. Sin embargo, esto no implica que el sistema tenga que desplegar todos los elementos que contienen, sino que el sistema de despliegue determinará cuales presentar de acuerdo al tipo de información que se le solicitó. Por ejemplo, si una empresa requiere conocer únicamente el último grado de estudios de cierta persona, podrá seleccionar esa opción y el sistema se encargará de buscar en el

expediente curricular electrónico los elementos que conforman la descripción del título de grado académico.

Como parte del diseño de la estructura del expediente curricular electrónico, se determinaron los elementos a incluir en cada documento probatorio. Además, cada documento probatorio tiene una clave única que lo identifica en el sistema, tal como se menciona en la sección 4.3.2.4. Como no todos los documentos probatorios presentan el mismo tipo de información, se diseñó una estructura para cada tipo, como se presenta a continuación:

- **Títulos de grado académico** - Estos documentos determinan el grado académico de la persona, esto es, el valor académico en base a la profundidad y la amplitud de los conocimientos y habilidades adquiridas al cumplir con ciertos créditos, dependiendo de la institución donde se adquiere. Los elementos que contiene son:

    - Institución que lo expide.
    - Fecha y lugar de expedición.
    - Grado y descripción del título de grado adquirido.
    - Información de registro por el departamento de administración escolar de la institución que lo otorga, lo cual incluye número de registro, libro y fojas del registro de títulos profesionales, fecha de registro y nombre de quien firma.
    - Datos de revisión por la Dirección General de Profesiones de la Secretaría de Educación Pública (SEP). Entre estos datos se incluyen el libro, fojas, número de grado académico, número de cédula y fecha de revisión.
    - Nombres de las autoridades de la institución que firman el título.

- **Certificados académicos** – Son aquellos que comprueban que la persona cursó y acreditó las asignaturas que cubre un programa de estudios, ya sea de licenciatura u otro grado como especialidad, maestría o doctorado. El hecho de presentar un certificado de estudios no equivale a tener el grado de estudios para el cual se cumplieron los créditos. Solamente con el título de grado académico se podrá registrar

tal grado. Estos documentos contienen los mismos elementos que los títulos de grado académico, pero además se anexa el kardex que contiene los nombres de las asignaturas junto con las calificaciones, escala de evaluación, créditos obtenidos y observaciones.

- **Constancias de diplomados y seminarios** - Son documentos que hacen constar que la persona cursó y acreditó las materias que conforman los programas de diplomados y seminarios. Este tipo de estudios no tiene valor en grado académico. Sin embargo, representan habilidades y conocimientos de la persona.

- **Constancias y exámenes de idiomas** – Son documentos probatorios que hacen constar que la persona cursó programas para el aprendizaje de idiomas, así como exámenes para comprobar el conocimiento de algún idioma. Por ejemplo, el Examen de Inglés como Lengua Extranjera (TOEFL).

- **Publicaciones** - Son documentos probatorios de las publicaciones que ha hecho la persona, como por ejemplo, libros, artículos científicos y revistas.

- **Reconocimientos** - Aquellos que reconocen a la persona por alguna aportación académica o trabajo realizado. Por ejemplo, impartición de conferencias, exposiciones, y seminarios.

- **Experiencia laboral** – Son aquellos documentos que comprueban el desempeño de la persona en el ambiente laboral. Estos documentos podrán ser expedidos por las empresas donde la persona laboró, en forma de constancias o cartas oficiales. La entidad de certificación se encargará de comprobar los datos que incluya, para agregarlos al expediente curricular electrónico del usuario. Los elementos que conforman cada comprobante de experiencia laboral incluyen:

    - Puesto de trabajo (incluye descripción del puesto)
    - Empresa o institución

- Departamento
- Jefe inmediato
- Período en que laboró en esa empresa o institución
- Responsabilidades
- Reconocimientos

- **Otros** – Documentos que no se incluyen en las categorías anteriores, pero que debido al valor que representan, pueden anexarse al expediente curricular electrónico del usuario.

4.3.7.5 Archivo DTD

En base a la definición de los elementos que contiene cada documento probatorio que conforman el expediente curricular electrónico, se diseñó el archivo de validación DTD. Este define la estructura que debe tener el documento XML, incluyendo el orden y la cantidad de veces en que deben aparecer los elementos del documento. Aunque el expediente curricular electrónico de un profesionista podrá estar fragmentado y distribuido entre distintas entidades de certificación, se presenta en la figura 4.2 la primera versión del conjunto de elementos que conformaría el DTD como si estuviera integrado en un solo archivo. Esto con el objetivo de presentar una idea clara sobre los elementos que contiene. Por otro lado, se omiten los elementos que identifican a cada documentos probatorio, ya que estos no estarán almacenados en el contenido del documento, sino en estructuras propias de las bases de datos.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- DTD de Expediente Curricular Electrónico V.1.0  22octubre2006 -->

<!ELEMENT expediente
(datos,titulos_grado?,certificados?,diplomados?,seminarios?,experiencia?,p
ublicaciones?,idiomas?)>
<!ATTLIST expediente curp ID #REQUIRED>

<!-- Datos Personales y de Contactos-->

<!ELEMENT datos (usuario,contacto*,actualizacion)>
<!ELEMENT usuario (nombre,nacimiento,sexo,domicilio,tel*,email*,sangre?)>
<!ELEMENT nacimiento (fecha,localidad)>
```

```
<!ELEMENT domicilio (calle,num,colonia,localidad)>
<!ELEMENT tel (clave_pais,clave_area,numtel,ext*)>
<!ATTLIST tel tipo (casa | trabajo | fax | movil | otro) #IMPLIED>
<!ELEMENT contacto (nombre,domicilio,tel*,email*)>
<!ELEMENT sangre (#PCDATA)>
<!ELEMENT colonia (#PCDATA)>
<!ELEMENT calle (#PCDATA)>
<!ELEMENT num (#PCDATA)>
<!ELEMENT clave_pais (#PCDATA)>
<!ELEMENT clave_area (#PCDATA)>
<!ELEMENT numtel (#PCDATA)>
<!ELEMENT ext (#PCDATA)>
<!ELEMENT actualizacion (fecha)>

<!-- Títulos de Grado Académico -->

<!ELEMENT titulos_grado (titulo_grado+)>
<!ELEMENT titulo_grado
(titulo,institucion,clave_institucion,autoridades,fecha,localidad,registro
_institucion,registro_sep)>
<!ATTLIST titulo_grado clave_documento ID #REQUIRED>
<!ATTLIST titulo_grado grado (Licenciatura | Especialidad | Maestría |
Doctorado) #REQUIRED>
<!ELEMENT registro_institucion (num_registro,libro,fojas,fecha,autoridad)>
<!ELEMENT num_registro (#PCDATA)>
<!ELEMENT fojas (#PCDATA)>
<!ELEMENT registro_sep
(libro,fojas,numero_grados,cedula,fecha,registrador)>
<!ELEMENT numero_grados (#PCDATA)>
<!ELEMENT cedula (#PCDATA)>
<!ELEMENT registrador (nombre)>

<!-- Certificados Académicos -->

<!ELEMENT certificados (certificado+)>
<!ELEMENT certificado
(institucion,campus,escuela,clave_institucion,programa,grado?,autoridades,
fecha,localidad,matricula,calificaciones,registro_institucion)>
<!ATTLIST certificado clave_documento ID #REQUIRED>
<!ELEMENT programa (#PCDATA)>
<!ELEMENT calificaciones
(escala,minima_aprobatoria,asignatura+,total_creditos?,promedio_general?)>
<!ATTLIST calificaciones tipo_periodo (bimestral | trimestral | semestral
| anual) #REQUIRED>
<!ELEMENT escala (minima,maxima)>
<!ELEMENT minima (#PCDATA)>
<!ELEMENT maxima (#PCDATA)>
<!ELEMENT minima_aprobatoria (#PCDATA)>
<!ELEMENT asignatura
(periodo_asig,nombre_asig,etapa?,calificacion,creditos)>
<!ATTLIST asignatura tipo_examen (Ordinario | Extraordinario |
Regularización) #REQUIRED>
<!ATTLIST asignatura tipo_asignatura (Obligatoria | Optativa |
Curso_Tutorial) #IMPLIED>
<!ELEMENT periodo_asig (año,parte?)>
<!ELEMENT parte (#PCDATA)>
<!ELEMENT nombre_asig (#PCDATA)>
```

```
<!ELEMENT etapa (#PCDATA)>
<!ELEMENT calificacion (#PCDATA)>
<!ELEMENT creditos (#PCDATA)>
<!ELEMENT total_creditos (#PCDATA)>
<!ELEMENT promedio_general (#PCDATA)>

<!-- Constancias de Diplomados -->

<!ELEMENT diplomados (diplomado+)>
<!ELEMENT diplomado
(institucion,clave_institucion,campus?,escuela?,departamento?,titulo,perio
do,modulos,total_creditos,escala,minima_aprobatoria,registro,autoridades)>
<!ATTLIST diplomado clave_documento ID #REQUIRED>
<!ELEMENT modulos (modulo+)>
<!ELEMENT modulo (numero,titulo,horas,calificacion,creditos?)>
<!ELEMENT numero (#PCDATA)>
<!ELEMENT horas (#PCDATA)>
<!ELEMENT registro (num_registro,folio,libro,autoridades?)>
<!ELEMENT folio (#PCDATA)>

<!-- Constancias de Seminarios -->

<!ELEMENT seminarios (seminario)+>
<!ATTLIST seminario clave_documento ID #REQUIRED>
<!ELEMENT seminario (institucion,
clave_institucion,campus?,escuela?,departamento?,titulo,(fecha |
periodo),registro?,autoridades)>

<!-- Experiencia Laboral -->

<!ELEMENT experiencia (empleo+)>
<!ELEMENT empleo (puesto,supervisor,(empresa |
institucion),responsable?,domicilio,periodo,responsabilidades?,logros?,rec
onocimientos?)>
<!ATTLIST empleo clave_documento ID #REQUIRED>
<!ELEMENT puesto (nombre_puesto,descripcion?,departamento)>
<!ELEMENT nombre_puesto (#PCDATA)>
<!ELEMENT supervisor (nombre,puesto,tel)>
<!ELEMENT responsable (nombre,puesto)>
<!ELEMENT responsabilidades (responsabilidad+)>
<!ELEMENT responsabilidad (#PCDATA)>
<!ELEMENT logros (logro+)>
<!ELEMENT logro (descripcion)>
<!ELEMENT reconocimientos (reconocimiento+)>
<!ELEMENT reconocimiento (titulo,(fecha |
periodo),descripcion?,institucion?,localidad?,autoridades?)>

<!-- Publicaciones -->

<!ELEMENT publicaciones (publicacion+)>
<!ELEMENT publicacion (pub_libro | pub_articulo | exposicion |
hoja_tecnica | pub_periodica)>
<!ATTLIST publicacion clave_documento ID #REQUIRED>
<!ELEMENT pub_libro (titulo,(autor+ |
autor_institucional+)+,editorial,fecha_pub,paginas?,ISBN_obra?,ISBN_volume
n?)>
<!ELEMENT autor_institucional (#PCDATA)>
```

```
<!ELEMENT editorial (siglas?,nom_editorial,ciudad,pais)>
<!ELEMENT siglas (#PCDATA)>
<!ELEMENT nom_editorial (#PCDATA)>
<!ELEMENT fecha_pub (dia?,mes?,año)>
<!ELEMENT paginas (#PCDATA)>
<!ELEMENT ISBN_obra (#PCDATA)>
<!ELEMENT ISBN_volumen (#PCDATA)>
<!ELEMENT pub_articulo (titulo,autor+,url_texto?,url_indice?,fecha,ISSN?)>
<!ELEMENT url_texto (url)>
<!ELEMENT url_indice (url)>

<!-- Exámenes de Idiomas -->

<!ELEMENT idiomas (idioma+)>
<!ELEMENT idioma (toefl_itp | toefl)>
<!ATTLIST idioma clave_documento ID #REQUIRED>
<!ELEMENT toefl_itp (institucion,
clave_institucion,grado,veces_tomado,pais_nativo,lenguaje_nativo,resultado
s,fecha)>
<!ELEMENT veces_tomado (#PCDATA)>
<!ELEMENT pais_nativo (#PCDATA)>
<!ELEMENT lenguaje_nativo (#PCDATA)>
<!ELEMENT resultados (listening,structure,reading,total)>
<!ELEMENT listening (score)>
<!ELEMENT structure (score)>
<!ELEMENT reading (score)>
<!ELEMENT total (score)>
<!ELEMENT score (#PCDATA)>

<!-- Elementos comunes -->

<!ELEMENT nombre (nom,paterno,materno?)>
<!ELEMENT nom (#PCDATA)>
<!ELEMENT paterno (#PCDATA)>
<!ELEMENT materno (#PCDATA)>
<!ELEMENT sexo (#PCDATA)>
<!ELEMENT fecha (dia,mes,año)>
<!ELEMENT dia (#PCDATA)>
<!ELEMENT mes (#PCDATA)>
<!ELEMENT año (#PCDATA)>
<!ELEMENT localidad (ciudad,estado,pais)>
<!ELEMENT ciudad (#PCDATA)>
<!ELEMENT estado (#PCDATA)>
<!ELEMENT pais (#PCDATA)>
<!ELEMENT titulo (#PCDATA)>
<!ELEMENT descripcion (#PCDATA)>
<!ELEMENT institucion (#PCDATA)>
<!ELEMENT empresa (#PCDATA)>
<!ELEMENT campus (#PCDATA)>
<!ELEMENT escuela (#PCDATA)>
<!ELEMENT matricula (#PCDATA)>
<!ELEMENT periodo (desde,hasta)>
<!ELEMENT desde (dia?,mes?,año)>
<!ELEMENT hasta ((dia?,mes?,año) | actual)>
<!ELEMENT actual EMPTY>
<!ELEMENT grado (#PCDATA)>
<!ELEMENT clave_institucion (#PCDATA)>
```

```
<!ELEMENT departamento (#PCDATA)>
<!ELEMENT autoridades (autoridad+)>
<!ELEMENT autoridad (nombre,cargo)>
<!ELEMENT cargo (#PCDATA)>
<!ELEMENT libro (#PCDATA)>
<!ELEMENT autor (nombre,institucion?,localidad?,email*)>
<!ELEMENT email (#PCDATA)>
<!ELEMENT url (#PCDATA)>

<!-- Fin del documento -->
```

Figura 4.13 – Archivo DTD para validación del documento XML del expediente curricular

Esta primera versión se diseñó para presentar una idea clara sobre la manera en que el expediente curricular está estructurado. Sin embargo, se estima que surjan nuevas versiones del mismo, conforme se lleva a cabo el proceso de adaptación de los documentos probatorios existentes con el sistema. En la página Web del sitio del Grupo de Investigación en Tarjetas Inteligentes (GRINTAIN) se encuentra publicada la versión más reciente del archivo DTD, junto con un ejemplo del expediente curricular en XML. Para la descarga de estos archivos consulte la página Web que se encuentra en la siguiente liga: http://www.grintain.com/proyectos/expediente/dtd

En el diseño se observa que la cantidad de información que contiene el documento puede variar, ya que no se fija un límite en la cantidad de documentos probatorios que puede incluir. Por otro lado, el servidor de aplicaciones será quien se encargue de extraer de los servidores de bases de datos, los documentos XML y procesarlos, para que las aplicaciones cliente desplieguen la información de los expedientes curriculares de manera adecuada para el usuario del sistema.

Capítulo V. Conclusiones

La problemática que ha surgido debido a la falsificación, duplicado y comercio ilegal de comprobantes de estudios, motivó el planteamiento de una alternativa en la validación de la autenticidad de dichos documentos. Tal alternativa consiste en la implementación de un sistema de bases de datos distribuidas para almacenar, recuperar y administrar información sobre los comprobantes de estudios y experiencia laboral de todas las personas con nivel de estudios de nivel profesional que residen en el país. Este sistema, además de ayudar a minimizar los inconvenientes de la problemática mencionada, aprovecha las ventajas que brindan los dispositivos actuales de almacenamiento y recuperación de información para hacer más eficiente los procesos involucrados en la gestión de los comprobantes de estudios y experiencia laboral.

Para la elaboración de este trabajo se planteó como objetivo general, diseñar un sistema basado en tarjetas inteligentes que permita almacenar y recuperar de manera segura y eficiente, expedientes curriculares electrónicos. Esto derivó en cuatro objetivos específicos que se fueron cumpliendo conforme se avanzó en la investigación. El proceso que se llevó a cabo para cumplir con estos objetivos incluyó conocer a detalle, los aspectos que involucran el brindar una solución segura y eficiente para el manejo de información sensible. Dentro de estos aspectos se encuentra el uso de tarjetas inteligentes como mecanismo seguro de autenticación e identificación con algún sistema. Esto motivó la realización de una investigación a profundidad sobre tarjetas inteligentes, lo cual permitió conocer su desarrollo, abarcando desde sus antecedentes y evolución, hasta lo más reciente de esta tecnología. De igual manera, se documentó sobre la forma en que estas se clasifican, así como la gran variedad de aplicaciones donde se han utilizado y se utilizan actualmente.

Lo anterior amplió en gran parte el panorama sobre estos dispositivos y permitió tener certeza de la confiabilidad de utilizar esta tecnología como mecanismo seguro para acceso al sistema que almacena los expedientes curriculares electrónicos. Se observó que las distintas definiciones de tarjetas inteligentes encontradas en las fuentes bibliográficas se orientaban a contextos específicos. Esto motivó a plantear una nueva definición que abarcara un contexto general. Se espera que esta nueva definición, así

como el material recopilado, sirva como referencia para otros trabajos de investigación donde se haga uso de tarjetas inteligentes. Además, el proceso de recopilación de información sobre tarjetas inteligentes derivó otros temas que fueron de gran importancia para la realización de este trabajo. Entre estos se encuentran la seguridad de la información y los mecanismos que se emplean para proporcionarla.

Durante la revisión de fuentes bibliográficas, se encontró que existen diversos mecanismos que, al ser utilizados en conjunto, permiten brindar seguridad en el manejo de la información. Para la elaboración del diseño propuesto se tomaron en cuenta dichos mecanismos y además fue de relevancia considerar el valor de la información que se deseaba proteger y conocer el impacto económico y social que representaría si esta fuera interceptada y alterada por personas ajenas al sistema. En primera instancia, si se hubieran implementado mecanismos de seguridad de un nivel muy básico, como por ejemplo, el uso de contraseñas de acceso, sin utilizar cifrado de datos, ni mecanismos de autenticación mutua, hubiera hecho vulnerable al sistema para que personas ajenas a éste, lograran acceder fácilmente a la información, por medio del uso de herramientas de bajo costo. El exponer esta información a tales personas, tendría un impacto social más que económico, ya que se perdería credibilidad y se volvería susceptible a fraudes que, posiblemente, tendrían mayores consecuencias que las que resultan de utilizar los procesos actuales para la verificación de documentos probatorios. Por otro lado, no fue necesario implementar mecanismos de seguridad más avanzados y costosos que los propuestos en este trabajo, como por ejemplo el uso de tarjetas inteligentes del tipo JavaCard con infraestructura de llave pública para autenticación. Tales mecanismos son más adecuados para aplicaciones donde el robo o alteración de la información representaría grandes pérdidas económicas. Por lo tanto, el uso de tarjetas inteligentes tipo ACOS2 con autenticación simétrica es la solución adecuada para el sistema propuesto. El conocimiento adquirido durante esta investigación, permitió elaborar un diseño que cumple con los requisitos del sistema, dando como resultado una alternativa viable y segura para la validación de la autenticidad de documentos probatorios, así como para su almacenamiento y administración.

El diseño del sistema de expedientes curriculares electrónicos implicó incluir servidores de bases de datos distribuidos en distintas localidades, los cuales almacenarán en formato electrónico, la información relacionada con los estudios y experiencia laboral

de los profesionistas del país. Un hecho importante que motivó la utilización de un diseño de bases de datos distribuido basado en el uso de réplicas, fue el descubrir la existencia de la plataforma de bases de datos *Berkeley DB* de la empresa *Oracle*. Esto permitió contar con un antecedente confiable, con aplicaciones exitosas, para el diseño de bases de datos distribuidas que brindan alta disponibilidad y confiabilidad de los datos. A su vez, permitió diseñar el sistema para que los expedientes curriculares se fraccionaran y se distribuyera su almacenamiento entre las distintas entidades de certificación, dependiendo del lugar donde se realizó su verificación. Esto brindó la ventaja de poder delegar la responsabilidad a cada entidad de certificación, sobre el almacenamiento y administración de los documentos probatorios que cada una valida. De esta manera, se evitó caer en los problemas que conlleva el centralizar tanto el almacenamiento como la administración de los datos.

Durante el análisis de requisitos del sistema se consideraron varios aspectos para proveer una solución viable, en cuanto a costo y seguridad para el almacenamiento y recuperación de expedientes curriculares electrónicos. El utilizar tarjetas inteligentes con criptografía 3-DES como mecanismo de autenticación y enlaces VPN basados en SSL para proveer comunicación entre clientes y servidores, así como enlaces VPN basados en IPSec para comunicación entre las entidades de certificación, permitió hacer uso de la infraestructura de la red pública Internet de una manera que brindara integridad y privacidad de los datos.

El conocimiento adquirido sobre los avances tecnológicos de las tarjetas inteligentes motivó la intención de almacenar una copia del expediente curricular electrónico en la memoria de la tarjeta inteligente del usuario. Esto brindaría la característica de que el expediente curricular pudiera ser consultado desde dispositivos lectores sin la necesidad de contar con conexión al sistema de expedientes curriculares electrónicos. Sin embargo, conforme se fueron conociendo las características de las tarjetas inteligentes que se incluyen en los paquetes de desarrollo existentes, se encontraron limitantes en cuanto a sus capacidades de almacenamiento. El tipo de tarjeta inteligente seleccionado para este trabajo no proporciona suficiente espacio de memoria para garantizar el almacenamiento de un expediente curricular electrónico que tiende a crecer conforme el usuario incrementa tanto sus estudios como experiencia laboral. Sin embargo, se concluyó que el hecho de no poder almacenar una copia del expediente curricular en la

memoria de la tarjeta inteligente, sino solamente en las bases de datos distribuidas, aumentaba la confiabilidad del sistema. El usar la modalidad *offline* para la consulta de expedientes curriculares electrónicos, representaba un riesgo de seguridad ya que, al no llevarse a cabo el proceso autenticación entre la tarjeta y el sistema, hubiera puesto en juicio la confiabilidad de la información contenida en las tarjetas inteligentes. La aplicación que leyera el expediente curricular electrónico de la tarjeta inteligente no tendría forma de autenticar la validez de esa tarjeta y por lo tanto, tampoco la validez de la información almacenada en ella. Sin embargo, para el caso de la información personal del usuario que se almacena en la tarjeta inteligente y que puede ser consultada en modalidad *offline*, no representa ningún riesgo, ya que esa información es sólo para identificación personal en aplicaciones que no requieran su validación.

Cabe mencionar que, aunque se diseñe y se implemente este sistema con todas las medidas de seguridad necesarias para proteger información valiosa, el factor humano siempre será determinante en el grado de seguridad y confiabilidad que se brinde. Será necesario definir, implementar y hacer que se cumplan las políticas de seguridad donde se consideren aspectos humanos, incluyendo un manejo eficaz de privilegios de acceso y uso de la información, códigos de ética, administración de responsabilidades y conflicto de intereses, entre otros. Esto nos lleva a considerar que, aunque el sistema cuente con medidas de seguridad extrema en todos los aspectos técnicos, el factor humano sigue siendo un punto débil en cuanto a la seguridad y confiabilidad del sistema, si no se toman las medidas adecuadas para evitarlo.

Un aspecto importante que se consideró en este trabajo fue el proponer y desarrollar un modelo para el almacenamiento y representación de la información referente a los expedientes curriculares, que tuviera una estructura bien definida y pudiera servir como estándar para su uso por las diversas instituciones educativas y empresas del país. Esto motivó la búsqueda de antecedentes en cuanto a modelos de representación de datos de este tipo, para que sirviera de base a la elaboración del modelo mencionado. La existencia del proyecto *XMLRésumé*, el cual tiene como objetivo brindar un modelo para estructurar información electrónica referente a currículums vitae y resúmenes académicos, permitió contar con un antecedente para utilizarse como punto de partida en la elaboración del expediente curricular electrónico y adaptarlo a las necesidades de este trabajo. El modelo de almacenamiento y representación de los expedientes

curriculares electrónicos en lenguaje XML que se diseñó, será de gran importancia, ya que permitirá contar con un estándar a nivel nacional para el intercambio de información tanto académica como de experiencia laboral con que cuentan las personas. Esto hará posible contar con un lenguaje común en donde se minimice la ambigüedad y por lo tanto, los esfuerzos para interpretar la información que contengan los documentos probatorios que los profesionistas presenten. Se espera que lo anterior sirva de modelo para que las empresas cuenten con una estructura de almacenamiento de información sobre el historial de las actividades que desempeñan sus empleados, facilitando así, la elaboración de documentos que demuestren experiencia laboral.

El implementar este sistema con todos los aspectos mencionados, cumple con los objetivos definidos en la introducción de esta investigación. Sin embargo, es importante anticipar y estudiar también los problemas que se pueden encontrar durante su implementación. De esta manera se podrá realizar una planeación adecuada para minimizar los inconvenientes. Uno de los problemas que se anticipa de antemano es la resistencia de las instituciones y empresas para adaptarse a esta nueva forma de verificar la validez de la documentación presentada por los profesionistas, así como la complejidad en la reestructuración de los sistemas que llevan a cabo los procesos de expedición de títulos en las instituciones educativas, para adaptarlos a los requerimientos del sistema de expedientes curriculares. La incorporación de nuevas tecnologías implica un proceso de adaptación que requiere de tiempo y esfuerzo por parte de todos los involucrados. Vivimos en una sociedad en la cual muchos de los procesos que involucran almacenamiento y validación de información, se llevan a cabo utilizando técnicas tradicionales que son vulnerables a actos delictivos como lo es la falsificación de comprobantes de estudios. La migración de estos procesos a una forma más segura y eficiente, representará un gran avance, no solamente en el sector educativo, sino en todos los demás sectores de nuestra sociedad ya que, al validar los comprobantes de estudios y de experiencia laboral de los profesionistas, se garantiza que tienen las habilidades para desempeñarse en el cumplimiento de las funciones que su profesión les demanda. El sector educativo, en conjunto con el sector laboral y otras dependencias involucradas, deberán realizar una planeación adecuada para que este cambio se lleve a cabo de manera eficaz.

Por otro lado, la implementación de este sistema implicará cubrir con otras actividades muy importantes entre las que se encuentra la creación de entidades de certificación que pudieran ser organismos federales, con facultades para realizar los procesos de validación y administración de estos documentos, que cuenten con infraestructura robusta tanto de comunicaciones como de los sistemas de bases de datos de clase corporativa para asegurar su buen funcionamiento.

Se espera que el resultado de esta investigación, además de aportar las bases fundamentadas para el diseño e implementación de un sistema de información distribuido con un mecanismo seguro de autenticación e identificación, sea el primer paso de una solución eficaz para resolver los inconvenientes asociados a la gestión actual de los expedientes curriculares en papel y que ayude a minimizar el problema de la falsificación de comprobantes de estudios.

Referencias

ACS - Advanced Card Systems Ltd. (2006). *ACOS2 Reference Manual*. Consultado el 20 de marzo de 2006, de http://www.acs.com.hk/downloads_datasheet/REF_ACOS2_V2.3.pdf

ACS - Advanced Card Systems Ltd. (2006). *PC-Linked Readers*. Consultado el 3 de mayo de 2006, de http://www.acs.com.hk/Products_PC_Linked_SmartCard_Readers.asp

Arvay, T., Tafel, A., Ford L. (1997). *Smart Cards: Big-Time Puch in a Byte-Sized Package.* Quartermaster Professional Bulletin – U.S. Army Quartermaster Corps. Consultado el 25 de febrero de 2006, de http://www.quartermaster.army.mil/OQMG/Professional_Bulletin/1997/Winter/smartcard.html

Axalto (2006). *Cyberflex Access – The Java Card for Information Security*. Consultado el 30 de mayo de 2006, de http://www.axalto.com/access/smartcards/cyberflexaccess.asp

Barr, M. (2001, Mayo). *Memory Types*. CMP Media LLC. Embedded Systems Programming. Vol 5, No. 114. Pp. 103-104.

Bergin, J. (2003). *Building Graphical User Interfaces with the MVC Pattern*. Pace University. Consultado el 10 de octubre de 2006, de http://csis.pace.edu/~bergin/mvc/mvcgui.html

Berson, A. (1996). *Client/Server Architecture* (2ª ed). New York, NY: McGraw-Hill.

Bezakova, I., Pashko, O., Surendran, D. (2000). *Smartcards Survey*. Department of Computer Science, The University of Chicago. Consultado el 30 de mayo de 2006, de http://people.cs.uchicago.edu/~dinoj/smartcard/

Bradley, T. (2007). *VPN's: IPSec vs. SSL*. About.com – Internet Network Security. Consultado el 20 de enero de 2007, de http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm

Breunesse, C., Jacobs, B., Oostdijk, M. (2002). *Voting using Java Card smart cards: A case study*. Nijmegen Intitute for Information and Computer Sciences. University of Nijmegen, The Netherlands.

Bunn, J. (2001). *Distributed Databases*. Center for Advanced Computing Research – CALTEC. California Institute of Technology.

Cardlogix Corp. (2001). *Smart Card and Security Basics.* Consultado el 21 de marzo de 2005, de http://www.smartcardbasics.com/pdf/SmartCardBasics.pdf

Cardlogix Corp. (2001). *Smart Card Families*. Consultado el 20 de mayo de 2006, de http://www.cardlogix.com/product_smart.asp

CardWerk, SM. (1999). *History of Smart Cards.* Smarter Card Solutions. Consultado el 10 de marzo de 2005, de http://www.cardwerk.com/smartcards/smartcard_history.aspx

Castillo, J., Sosa, L. (2001*). La Tecnología Embedded Internet como un Resultado de la Tendencia en los Dispositivos a la Conectividad Global.* Facultad de Ingeniería, Universidad Autónoma de Baja California. México. Consultado el 6 de junio de 2005, de http://www.tataware.com/embedded_internet/

Clark, A. (1990). *Smart Cards. A paper to be presented to the London Chapter of the EDP Auditors Association*. Secure Systems Group. Consultado el 28 de mayo de 2006, de http://www.primarykey.co.uk/Andy/Papers/smartc02.pdf

Clark, D. (2003). *Enterprise Security. The Manager's Defense Guide*. Boston: Addison-Wesley.

Corum, C. & Wehr, J. (2004, Mayo 1). *Contactless card standards: Making sense of 10536, 14443, and 15693.* ContactlessNews. Consultado el 6 de marzo de 2006, de http://www.contactlessnews.com/library/2003/05/01/contactless-card-standards-making-sense-of-10536-14443-and-15693/

Coulouris, G., Dollimore, J. & Kindberg, T. (2001). *Sistemas Distribuidos – Conceptos y Diseño* (3ª ed.). Madrid: Addison Wesley.

Daley, W. & Kammer, R. (1999, Octubre 25). *Data Encryption Standard (DES) FIBS PUB 46-3*. Federal Information Processing Standard Publication (FIPS PUB). U.S. Department of Commerce / National Institute of Standards and Technolgy.

Di Giorgio, R. (1997). *Smart Cards: A Premier.* Java World-Java Developer Section. Consultado el 12 de abril de 2005, de http://www.javaworld.com/javaworld/jw-12-1997/jw-12-javadev

Diners Club International. (2005). *Dinners Club history overview and timeline*. Consultado el 28 de mayo de 2006, de http://www.dinersclubnewsroom.com/anniversary.cfm?submenu=history

Doyle, A. (2006). *Curriculum Vitae vs. Resume?-- FAQs for Jor Searching*. About.com. Consultado el 1º de junio de 2006, de http://jobsearch.about.com/cs/curriculumvitae/f/cvresume.htm

eGov (2006). *Smart Card Tutorial*. U.S. General Services Administration. Consultado el 26 de febrero de 2006, de http://www.smartcard.gov/tutorial/tutorial_text.doc

Elmasri, R. & Navathe, S. (2002). *Fundamentos de Sistemas de Bases de Datos* (3ª ed.). Madrid: Addison-Wesley.

Erlwein, M. (2003). *Programa liderazgo para las américas: Juventud y transformaciones socioculturales*. Universidad Mayor. Santiago, Chile.

Everett, D. (1994). *Tutorial: Introduction to Smart Cards.* Smart Card Group. Consultado el 2 de abril de 2005, de http://www.smartcard.co.uk/tutorials/sct-itsc.pdf

Finkenzeller, K. (2004). *Radio Frequency Identification: Standarization of RFID.* Consultado el 15 de abril de 2005, de http://www.rfid-handbook.de

Frost & Sullivan (2005). *Americas Smart Card Market Analysis*. Smart Card Alliance. Pallo Alto, CA. Consultado el 29 de mayo de 2006, de http://www.smartcardalliance.org/alliance_activities/SCA_Executive_Summary_Final_092605.pdf

Fúster, A., Martínez, D., Hernández, L., Montoya, F., Muñoz, J. (2001). *Técnicas Criptográficas de Protección de Datos* (2ª. ed.). España: Alfaomega Ra-Ma.

García de Fanelli, A. (2002). *La educación superior trasnacional: Tipología y regularización estatal.* Centro de Estudios de Estado y Sociedad (CEDES). Buenos Aires, Argentina.

Gobierno del Estado de Colima (2007). *La CURP en Colima*. Consultado del 10 de enero de 2007, de http://www.colima-estado.gob.mx/e-gobierno/curp/curpcolima.php

Health Smart Card (1999). *Health Smart Card Introduction*. Consultado el 3 de diciembre de 2005, de http://www.healthsmartcard.net/intro.html

Hernández, R., Fernández, C., Baptista, P. (1999). Metodología de la Investigación. México: McGraw Hill.

Hive Minded, Inc (2002, Noviembre 5). *Hive Minded Announces Smartcard.NET.Press*. Consultado el 13 de agosto de 2006, de http://www.hiveminded.com/pr/Hive_Minded_Announces_Smartcard.pdf

ID Edge (2002). *Learning Center: Types of Smart Cards*. Consultado el 15 de abril de 2005, de http://www.idedge.com/ID_Card_Learning_Center/Smart_Cards/Smart_Cards.cfm
Inside Contactless (2003, Septiembre 18). *ISO Communication Standard 13.56 MHz*. Creating a Contactless World. Consultado el 15 de agosto de 2006, de http://www.insidecontactless.com/pdf/ISOStandards.pdf

Ibarra, J., Flores, B., Castillo, J. & Castro, U. (2006). *Diseño de una Arquitectura para el Manejo de Expedientes Curriculares Electrónicos Utilizando Tarjetas Inteligentes*. XXVIII Congreso Internacional de Ingeniería Electrónica ELECTRO 2006. Sección Sistemas Inteligentes. Vol. XXVIII. Pp. 323-328. ISSN. 1405-2172. Chihuahua, México.

Ibarra, J., Flores, B. & Castillo, J. (2005). *La Problemática del Comercio Electrónico en Comprobantes Curriculares*. 1er. Simposium Internacional de Educación. Nuevas Tecnologías y Gestión del Conocimiento. Sección Educación a Distancia. Num. 48. Memoria académica electrónica. Facultad de Ciencias Humanas, UABC. Mexicali, México.

ISO – International Organization for Stardarization (2006). *ISO/IEC 7816 1-11*. Consultado el 15 de abril de 2005, de http://www.iso.org

Johnson, B., Gossels, J. & Davis, D. (2004). *The SSL Handshake. A Perspective on Practical Security*. Systems Experts Corporation. Consultado el 28 de septiembre de 2006, de http://www.systemexperts.com/literature.html

Jurgensen, T. M. & Guthery, S. B. (2002). *Smart Cards, The developer's Toolkit*. Upper Saddle River, NJ: Prentice Hall PTR.

Kelly, S., Christensen, B., Miller, M. (2002). *XMLRésuméLibrary.* Consultado el 12 de abril de 2005, de http://xmlresume.sourceforge.net

Maturana, A. (2003). *Aspectos legales del comercio electrónico – Criptografía.* Portal Eurociber. Consultado el 18 de abril de 2005, de http://www.eurociber.es/index.php?mostrar=hackers8

McManus, J., Kinsman, C. (2002). *Visual Basic® .NET Developer's Guide to ASP .NET, XML and ADO.NET*. IN: Addison Wesley.

Menezes, A., Van Oorschot, P. & Vanstone, S. (2001). *Handbook of Applied Cryptography* (5ª ed.). Boca Ratón, FL: CRC Press.

MOREnet (2003). *An introduction to Network Firewalls and the Firewall selection Process*. Technical Support : Network Design and Process. Consultado el 18 de enero de 2007, de http://www.more.net/technical/netserv/tcpip/firewalls/

Nash, A., Duane, W., Joseph, C. & Brink, D. (2002). *PKI: Infraestructura de Claves Públicas* (1ª ed.). Bogotá: Osborne McGraw-Hill.

Newfield, P. (2006). *Resumes and C.V.s -- What's the Difference?*. Career Builder. Consultado el 25 de mayo de 2006, de http://www.careerbuilder.com/JobSeeker/CareerBytes/hints0600.htm

NIST- National Institute of Standards and Technology. (2006). *Personal Identity Verification (PIV) of Federal Employees / Contractors*. Computer Secutiry Resource Center. Consultado el 12 de agosto de 2006, de http://csrc.nist.gov/piv-program

Norton, M. (2001). *Layer 3 Switching -- Introducing the Router*. Networking as a 2nd language. Consultado el 10 de noviembre de 2006, de http://www.oreillynet.com/pub/a/network/2001/04/13/net_2nd_lang.html

Notimex (2004, Noviembre 23). *La Cédula Profesional contará con un Chip para evitar Falsificación*. Diario La Crónica de Hoy. Consultado el 20 de mayo de 2006, de http://www.cronica.com.mx/nota.php?id_nota=154552

Oberthur (2006, Febrero 15). *Orange, M-Systems and Oberthur Card Systems unveil World's first 512 MB SIM Card*. Press Releases. Oberthur Card Systems. Consultado el 28 de febrero de 2006, de http://www.oberthurcs.com/press_page.aspx?id=38

Open Card Consortium (1998). *General Information Web Document* (2ª ed.). Consultado el 2 de mayo de 2006, de http://www.opencard.org/docs/gim/ocfgim.html

Oracle (2006). *Sleepycat Software – Berkeley DB*. Sitio Web. Consultado el 2 de diciembre de 2006, de http://sleepycat2.inetu.net/products/bdb.html

Orlin, J. (1997-2000). *Digital Signatures Ilustrated.* Consultado el 2 de junio de 2005, de http://www.aci.net/kalliste/digsig.htm

PC/SC Workgroup (2006). *PC/SC workgroup specification 2.01.3*. Consultado el 5 de mayo de 2006, de http://www.pcscworkgroup.com

Petri, S. (1999). *An Introduction to Smart Cards*. Messaging Magazine, September/October. Consultado el 28 de mayo de 2006, de http://www.opengroup.org/comm/the_message/magazine/mmv5n5/SmartCards.htm

Poynder, R. (2001). *A guide to Smart Cards.* Smartex Limited. Consultado el 2 de mayo de 2005, de http://www.smartex.com/smartcards_guide.html

Raghu K. (2006, Junio 18). *Sex workers go smart with cards*. DNA – Daily News & Analysis. Consultado el 13 de agosto de 2006, de http://www.dnaindia.com/report.asp?NewsID=1036385

Red Hat Inc. (2005). *Apéndice B – Ataques y agresiones comunes*. Red Hat Enterprise Linux 4: Manual de seguridad. Consultado el 20 de febrero de 2006, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/index.html

Rodríguez L., Perovich D., Varela M., Martínez L. (2001). *Historias Clínicas en Tarjetas Inteligentes*. Jornadas Argentinas de Informática e Investigación Operativa. Argentina.

Rohde, L. (2000, Febrero 9). *Smart Cards to Contain Biometric Data*. CNN.com-Cable News Network. Consultado el 13 de agosto de 2006, de http://archives.cnn.com/2000/TECH/computing/02/09/biometrics.card.idg/index.html

RSA Security (2004). *Techniques in Cryptography*. Crypto FAQ: Chapter 3. RSA Laboratories. Consultado el 17 de septiembre de 2006, de http://www.rsasecurity.com/rsalabs/node.asp?id=2212

SECTRA, Secretaría Interministerial de Planificación de Transporte (2000). *Sistemas Inteligentes de Transporte: Glosario de términos.* Chile. Consultado el 12 de abril de 2005, de http://www.sectra.cl/its/glosario/terminos.htm

SEGOB, Secretaría de Gobernación (2006). *Clave Única de Registro de Población*. Preguntas más frecuentes. Consultado el 20 de noviembre de 2006, de http://www.segob.gob.mx/templetas/blank.php?idCont=182

Smart Card Alliance (2004). *Industry information – Standards*. Consultado el 1de junio de 2006, de http://www.smartcardalliance.org/industry_info/standards.cfm

Smart Card Trends (2004, Abril 27). *Visa Launches Visa Wave for Contacless Card Payments*. SCT news. Consultado el 13 de agosto de 2006, de http://www.smartcardstrends.com/det_atc.php?idu=679

Smart Card Trends (2005, Mayo 13). *USB Backbone becomes Ubiquitous*. STC News. Consultado el 12 de agosto de 2006, de http://www.smartcardstrends.com/det_atc.php?idu=2171

Smart Card Trends (2006, Agosto 4). *Gemalto Receives Order for U.S. Electronic Passport*. SCT News. Consultado el 13 de agosto de 2006, de http://www.smartcardstrends.com/det_atc.php?idu=3956

SSL.com (2005). *What is SSL?*. Knowledge base – Frequently Asked Questions. Consultado el 20 de septiembre de 2006, de http://info.ssl.com/article.aspx?id=10241

STMicroelectronics (2005). *Contactless Memories for RFID Solutions*. Consultado el 20 de abril de 2005, de http://www.st.com/stonline/press/news/back2005/b990m.htm

STMicroelectronics (2006). *25 years of smartcard ICs experience*. Consultado el 4 de octubre de 2006, de http://www.st.com/stonline/products/families/smartcard/sc_history.htm

Sun Microsystems (2002). *Model-View-Controller*. Java Blueprints. Consultado el 10 de diciembre de 2006, de http://java.sun.com/blueprints/patterns/MVC-detailed.html

Sun Microsystems (2006). *Java Card Technology*. Consultado el 1º de junio de 2006, de http://java.sun.com/products/javacard

Tropical Software (2004). *Triple DES Encryption Overview*. Strong Encryption Package. Consultado el 12 de septiembre de 2006, de http://www.tropsoft.com/strongenc/tripledes.htm

UC - Universidad de Cantabria (2003). *Cerca de 200 establecimientos ofrecen descuentos a los usuarios de la Tarjeta Universitaria Inteligente.* Noticias. Consultado el 10 de abril de 2005, de http://www.unican.es/WebUC/Internet/Noticias_y_novedades/historico/2003/1trimestre/20030123+c.htm

UPM - Universidad Politécnica de Madrid (2005). *Diseño y Optimización de Bases de Datos*. Departamento de Organización y Estructura de la Información. Consultado el 20 de octubre de 2006, de http://www.oei.eui.upm.es/Asignaturas/BD/DYOBD/DISTRIBUIDAS.pdf

WLAN Smart Card Consortium (2003). *WLAN-SIM Specification Version 1.0*. Consultado el 13 de agosto de 2006, de http://www.wlansmartcard.org/specs/WLAN-SIM-V1.pdf

ANEXO A - Proceso de personalización de la tarjeta inteligente

En base al manual de referencia de la tarjeta inteligente ACOS2 de la compañía Advanced Card Systems Ltd. (ACS, 2000), se detalla a continuación el procedimiento para llevar a cabo la personalización de estas tarjetas para su aplicación en el sistema de almacenamiento y recuperación de expediente curriculares electrónicos, sistema propuesto en este trabajo.

El ciclo de vida de las tarjetas ACOS2 consta de cuatro etapas, como se muestra en la figura A1. Estas van desde su fabricación hasta la etapa donde el usuario final las utiliza en su operación normal.

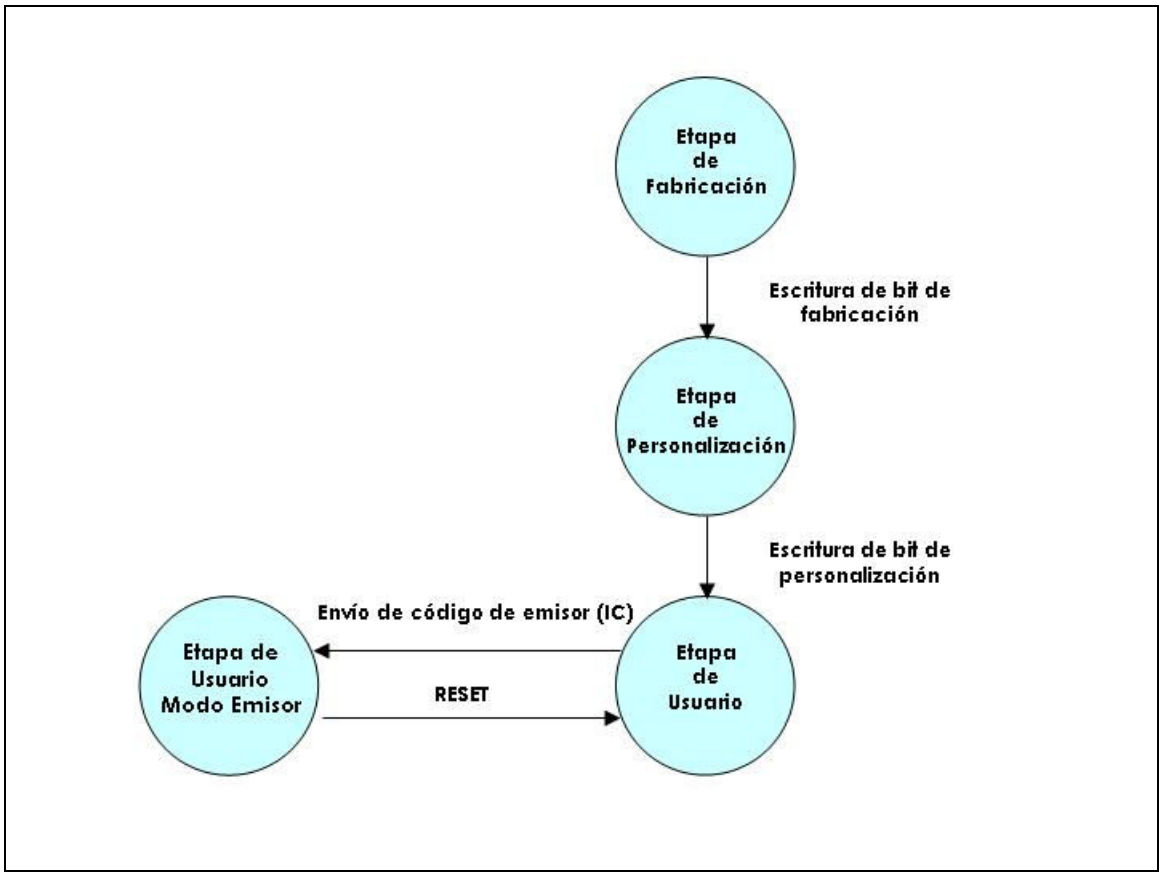

Figura A1 – Etapas del ciclo de vida de la tarjeta inteligente ACOS2

La tarjeta siempre se encuentra en alguna de estas cuatro etapas y su cambio a otra etapa depende de si se escriben ciertos bits en los registros internos de la tarjeta. Las etapas se detallan a continuación:

1. **Etapa de fabricación**. Esta etapa es efectiva desde el momento de la fabricación del chip de la tarjeta hasta que se realice la escritura de cierto bit de un registro interno de la tarjeta (llamado "fusible de fabricación"), el cual determina el cambio a la siguiente etapa. Durante esta etapa se programa en la tarjeta la siguiente información que quedará almacenada de manera definitiva y que determinará varios aspectos del funcionamiento de la misma:

    a. **Identificador del fabricante** – Es un número de 8 bytes que representa información sobre el fabricante así como la versión de la tarjeta.
    b. **Número de serie**. Es un número de 8 bytes el cual es único para cada tarjeta.
    c. **Código del emisor de la tarjeta (IC code) -** Es un número de 8 bytes proporcionado por el fabricante, el cual se utilizará para tener acceso a personalizar la tarjeta.

2. **Etapa de personalización**. Esta etapa comienza en el momento en que se escribe cierto bit durante la etapa de fabricación. Una vez llegada a esta etapa, no se puede volver a la etapa de fabricación. Esta es la etapa que le corresponde programar en la tarjeta a los desarrolladores de la aplicación, ya que es aquí donde se personaliza. Durante esta etapa se escriben los siguientes elementos en la tarjeta:

    a. **Códigos de Aplicación (ACs)**. Son 5 números de 8 bytes de longitud cada uno, los cuales serán utilizados para proporcionar privilegios de acceso de lectura y escritura de los archivos de usuario de la tarjeta. Las aplicaciones hacen uso de estos códigos para poder leer o escribir en los archivos de la tarjeta. Los códigos pueden ser introducidos por la aplicación en forma

normal o encriptada, dependiendo de la configuración previa en la tarjeta.

b. **Llaves de Encriptación**. Es un par de llaves que se utilizan para el proceso de autenticación mutua, en el cual tanto la tarjeta como la aplicación verifican que su respectiva contraparte sea genuina. Estas llaves pueden tener una longitud de 8 o 16 bytes, dependiendo si utilizan el proceso de encriptación del tipo DES o 3-DES, el cual se especifica durante esta misma etapa.

c. **Clave PIN**. Es una cadena de 8 bytes que se utiliza para controlar los derechos de lectura y escritura de los archivos de usuario de la tarjeta, tal como sucede con los 5 códigos de aplicación (ACs). La diferencia radica en que los ACs no pueden ser modificador una vez programados, en cambio la clave PIN puede ser cambiada por el usuario durante el uso normal de la tarjeta. Esta funciona como un mecanismo de identificación de usuario, en donde el usuario introduce un número que se sabe de memoria, el cual está almacenado en la tarjeta, comprobando de esta manera que es el dueño de la tarjeta. El número es verificado por la tarjeta para proveer privilegios ya sea de lectura o escritura de los archivos.

d. **Bloques de Definición de Archivos**. Son registros que definen la manera en que estarán organizados los archivos de usuario. Cada archivo de usuario se asocia a uno de estos bloques de configuración. Aquí se especifican parámetros como la cantidad de registros por archivo, la longitud de los registros, atributos de lectura, atributos de escritura e identificadores de archivos.

e. **Otros datos** – Se almacenan otros datos específicos a la tarjeta, como velocidad de transmisión, identificador del emisor de tarjetas, tipo de encriptación, etc.

3. **Etapa de usuario**. Esta etapa designa el modo normal operacional de la tarjeta. Esta etapa es efectiva una vez finalizada la configuración de la etapa de personalización. En esta etapa ya no se puede volver a 2 anteriores, pero si se puede pasar a la etapa del emisor de tarjeta si se introduce el código de emisor (IC), el cual debe estar solamente en manos de este y no del usuario final.

4. **Etapa de usuario – Modo del Emisor**. Esta etapa es similar a la etapa de usuario, con la única diferencia de que cuenta con privilegios para acceder a ciertas áreas de la memoria que no pueden ser accedidas en la etapa del usuario.

Una vez conocido el ciclo de vida de la tarjeta inteligente ACOS2, podemos determinar como llevar a cabo el proceso de programación y personalización de la tarjeta para la aplicación.

Debido a que cada tarjeta es entregada por el fabricante con un código de emisor (IC), el cual fue almacenado previamente en la etapa de fabricación como se mencionó anteriormente, se deben tomar las medidas necesarias para evitar que estos códigos sean utilizados por personas ajenas al departamento que se encarga de este proceso de personalización. Lo más indicado sería contar con una terminal o consola con privilegios de acceso a la base de datos de la entidad certificadora para acceder a información de los usuarios para el cual se expedirá la tarjeta. Con esta información en mano se puede empezar a realizar la "personalización" de la tarjeta

Basándonos en lo mencionado anteriormente, se puede definir los pasos que se deben seguir en el proceso de personalización. Tal proceso lo llevará a cabo el personal encargado de emitir las tarjetas a los usuarios. Estas personas recibirán las tarjetas en blanco directamente del fabricante o proveedor, con su respectiva clave de emisor (IC) y serán quienes tendrán privilegios de acceso al sistema para realizar tal proceso.

A continuación se presentan una serie de pasos que se han definido para llevar a cabo la personalización de la tarjeta inteligente.

1. El usuario emisor de tarjetas (aquel que se encarga de programarlas) se autentica en el sistema para obtener privilegios de acceso a la información de los usuarios, así como para programar las tarjetas. Este paso es crítico y se debe contar con un buen esquema de seguridad, ya que si alguna otra persona logra tener acceso a estas opciones del sistema, pudiera programar nuevas tarjetas poniendo en riesgo la seguridad del sistema en general. Lo recomendable para realizar este proceso en forma segura, es contar con una aplicación cliente que se encuentre en la misma red local del servidor de aplicaciones de la entidad certificadora.

2. El usuario emisor extrae del sistema una relación de usuarios nuevos que acaban de registrarse para obtener su tarjeta. Entre esta lista de usuarios también pueden encontrarse aquellos que perdieron su tarjeta y la reportaron o que tuvieron algún otro problema que implicó darle de baja la tarjeta actual. Esta relación de usuarios se puede utiliza para realizar el proceso de impresión que incluye el logotipo del sistema, su profesión, nombre completo, fecha de emisión, e información adicional que se requiera tener impresa en ella.

3. Una vez que las tarjetas estén impresas, el usuario emisor hace una búsqueda del usuario final en la base de datos y selecciona la opción de programar una nueva tarjeta. Esto lo hará con cada nueva tarjeta. El sistema debe estar validado para comprobar que no se ha expedido previamente otra tarjeta para el mismo usuario. Esto con la finalidad de asegurarse de que no existan tarjetas duplicadas. De lo contrario, dos o más personas pudieran identificarse con tarjetas idénticas. Este punto crítico se puede comparar a la problemática que surgiría en un banco si se expidieran tarjetas duplicadas. El usuario pudiera de alguna manera conseguir la clave PIN de la persona y lograr extraer dinero de los cajeros o realizar otras transacciones. De manera similar, si se duplica una tarjeta curricular, otra persona pudiera identificarse en establecimientos afiliados, y en el peor de los casos, al adivinar o robar la clave PIN, pudiera otorgar acceso al expediente curricular o realizar cambios en el mismo.

4. Una vez seleccionado al usuario de la tarjeta, se procede a seleccionar la opción de programar la tarjeta. Durante este proceso, la aplicación del sistema genera en forma aleatoria las llaves de autenticación mutua y los códigos de aplicación (AC) que se almacenarán en la tarjeta y en el sistema. Este proceso de almacenamiento de llaves y códigos se realiza en forma automática sin que ni siquiera el usuario emisor tenga acceso a ellas. A su vez, se genera en forma aleatoria el número de identificación personal (PIN) el cual podrá ser cambiado posteriormente por el usuario final. Este número no se almacena en el sistema, solamente en la tarjeta, ya que funciona como mecanismo para identificar al usuario portador de la tarjeta. Posterior a esto, la aplicación procede a programar la tarjeta para que esta pase a la etapa de usuario final y no se pueda volver a personalizar. A partir de este paso, tanto las llaves de autenticación mutua, como los códigos de aplicación de esta tarjeta en específico, no deben volver a transferirse, sino solamente quedar almacenados en ella y en la base de datos del servidor de la unidad certificadora. Como se verá más adelante, para el proceso de autenticación mutua, las llaves almacenadas nunca salen de la tarjeta, sino que se emplea un mecanismo de comprobación de llaves por medio de envío de mensajes aleatorios. Los códigos de aplicación (ACs) tampoco se expondrán durante la operación normal de la tarjeta (por ejemplo, al realizar una consulta del expediente curricular) debido a que estos códigos viajarán en forma cifrada utilizando llaves de encriptación distintas para cada sesión.

5. En este momento la tarjeta ya está relacionada con el usuario en específico. El siguiente paso consiste en almacenarle los datos personales, lo cual lo realiza la misma persona. Esto lo hace autenticándose al sistema usando la tarjeta inteligente e introduciendo la clave PIN. Este proceso le sirve también para comprobar si la tarjeta quedó programada correctamente. Una vez que el sistema identifica al usuario, el emisor selecciona la opción de actualizar los datos personales y estos se almacenan en la tarjeta.

6. Una vez personalizada la tarjeta, esta debe entregársele al usuario final junto con la clave PIN en un sobre a prueba de alteraciones, tal como lo realizan los bancos cuando entregan tarjetas de crédito a sus cuenta habientes. De esta manera se puede comprobar si el PIN fue leído por otra persona, y tomar las medidas necesarias en caso de que esto ocurra (por ejemplo, cancelar la tarjeta y entregarle otra). El portador de la tarjeta (usuario final) debe acudir a una oficina de la entidad certificadora para que por medio de la tarjeta inteligente le almacenen en el sistema sus documentos probatorios, los cuales forman parte de su expediente curricular.

ANEXO B - Estándares ISO/IEC 7816

Es una serie de estándares internacionales para tarjetas con circuito integrado (tarjetas inteligentes). El objetivo de estos estándares es lograr la interoperabilidad entre distintos fabricantes de tarjetas inteligentes y lectores de las mismas, en lo que respecta a características físicas, comunicación de datos y seguridad. Estos estándares son basados en los ISO 7810 e ISO 7811, los cuales definen características físicas de tarjetas de identificación. Las características de comunicación de las tarjetas que no tienen contactos, tales como las que utilizan radio frecuencia (RF) son definidas en otros estándares como por ejemplo, el ISO / IEC 14443.

La tabla B1 muestra las partes que comprenden el estándar ISO / IEC 7816 (ISO,2006).

Estándar	Descripción
7816-1	Define las características físicas de la tarjeta inteligentes, tales como sus dimensiones, tensión mecánica, radiación electromagnética, etc.
7816-2	Define las dimensiones, la posición y la función de los contactos del circuito integrado (chip).
7816-3	Define las señales electrónicas incluyendo niveles de voltaje, de corriente y velocidad, así como los procedimientos de operación, mecanismos de comunicación y transmisión de datos entre la tarjeta y el lector, uso de paridad y formato de "Contestación de Reset".
7816-4	Define: ▪ El contenido de los pares comando-respuesta que se intercambian a nivel de interfaz. ▪ Estructuras para aplicaciones y datos en la tarjeta

	▪ La estructura y contenido de los caracteres históricos de la respuesta de Reset, los cuales describen las características de operación de la tarjeta inteligente. ▪ Métodos para extracción de objetos y elementos de datos de la tarjeta. ▪ Mecanismos para la identificación y direccionamiento de aplicaciones en la tarjeta. ▪ Estructuras de archivos y métodos de acceso. ▪ Arquitectura de seguridad para derechos de acceso a los archivos y datos en la tarjeta. ▪ Comandos orientados a objetos de datos. ▪ Métodos de acceso a los algoritmos que procesa la tarjeta inteligente (no describe los algoritmos). ▪ Métodos para el intercambio seguro de mensajes. El estándar 7816-4 es independiente de la tecnología de interfaz física que se implemente en la tarjeta inteligente.
7816-5	Define como utilizar un identificador de aplicaciones para detectar la presencia y realizar la extracción de aplicaciones en la tarjeta. También muestra como obtener la unicidad en los identificadores de aplicaciones a través de un registro internacional y define el proceso del registro de estos identificadores,
7816-6	Define los elementos de datos (DEs) de intercambio entre las industrias, para tarjetas de contacto y sin contacto. Define el identificador, nombre, descripción, formato, codificación y estructura de cada DE y define los medios para la extracción

	de éstos desde la tarjeta.
7816-7	Define los comandos de intercambio entre industrias para el Lenguaje de Consultas Estructurado para Tarjetas (SCQL)
7816-8	Define los comandos de intercambio entre industrias para operaciones criptográficas (seguridad). Estos comandos son complementos de los definidos en el estándar ISO 7816-4.
7816-9	Define los comandos de intercambio entre industrias para el administración de la tarjeta y los archivos (como crearlos, borrarlos, etc.). Especifica una descripción y codificación del ciclo de vida de la tarjeta y de objetos relacionados. También especifica una descripción y codificación de los atributos de seguridad, como llevar a cabo la verificación en la descarga de información a la tarjeta para proteger los datos que se transmiten.
7816-10	Define las señales eléctricas y la respuesta de Reset para tarjetas que requieren señales de sincronización.
7816-11	Especifica comandos y objetos de datos de intercambio entre industrias, relacionados con la verificación personal a través de métodos biométricos. También presenta aspectos de seguridad en el uso de estos comandos.

Tabla B1 Estándar ISO/IEC 7816

Anexo C – Especificación PC/SC

Introducción

PC/SC es una especificación desarrollada por un grupo de trabajo el cual se conforma de varias empresas, entre ellas fabricantes de tarjetas inteligentes como Bull, Schlumberger, Gemplus y de otras empresas como Microsoft, Toshiba, Sun Microsystems, HP e IBM. Este grupo se inició para desarrollar una especificación que facilite la interoperabilidad necesaria para el uso efectivo de la tecnología de las tarjetas con circuito integrado (ICCs, por sus siglas en inglés de "*Integrated Circuit Card"*) en computadoras personales (PC). Además del desarrollo de esta especificación, el grupo se encarga de la implementación de hardware y componentes de software necesarios para la validación del diseño.

Actualmente, el uso de tarjetas con chip en ambientes de PCs se encuentra obstaculizado por la falta de interoperabilidad en varios niveles. Primero, la industria carece de estándares para interfaces entre PCs y lectores de tarjetas (IFDs, por sus siglas en inglés de "*Interface Device")*. Esto ha hecho difícil el desarrollo de aplicaciones que puedan trabajar con lectores de distintos fabricantes. Segundo, no existe una interfaz de programación de alto nivel para funciones comunes de las tarjetas con chip que sea aceptada ampliamente. Por último, no se han definido mecanismos para permitir que múltiples aplicaciones compartan de manera efectiva los recursos de las tarjetas con chip. Esto es crítico debido a la tendencia que existe de contar con varias aplicaciones en una sola tarjeta con chip. Sin el uso de estándares para compartir dispositivos, será imposible que los desarrolladores de aplicaciones aseguren la ejecución correcta de los servicios de las tarjetas con chip.

Objetivos

La especificación PC/SC se encuentra actualmente en su versión 2.01.3 [PC/SC, 2006]. Esta describe la funcionalidad mínima requerida para las ICCs, IFDs, y PCs para permitir

la interoperabilidad entre elementos de los distintos fabricantes. La especificación busca cumplir los siguientes objetivos:

- Mantener consistencia con los estándares existentes para ICCs y para PCs.
- Permitir la interoperabilidad entre componentes que se ejecuten en distintas plataformas (neutralidad entre plataformas).
- Permitir a las aplicaciones aprovechar las ventajas de los productos y componentes de los distintos proveedores (neutralidad entre proveedores).
- Permitir el uso de los avances tecnológicos sin necesidad de volver a escribir software a nivel de aplicación (neutralidad entre aplicaciones).
- Facilitar el desarrollo de estándares de interfaces a nivel de aplicación para servicios de las ICCs para incrementar la disponibilidad de aplicaciones basadas en tarjetas en ambientes de PCs.
- El soporte de ambientes que promuevan lo más posible el uso de tarjetas con chip como un elemento adicional de los ambientes de PCs.

Organización de la especificación

La especificación PC/SC se compone de nueve partes. Estas partes describen los requerimientos específicos para la interoperabilidad entre dispositivos compatibles, información de referencia para diseño, interfaces de programación y requerimientos de compatibilidad funcional. Las nueve partes se mencionan a continuación:

- **Parte 1.** Introducción y vista general de la arquitectura.
- **Parte 2**. Requerimientos de interfaz para tarjetas con chip (ICC) y lectores (IFD) compatibles.
- **Parte 3.** Requerimientos para dispositivos de interfaz de conexión a PC.
- **Parte 4**. Consideraciones de diseño de IFDs e información de referencia. Provee recomendaciones para la implementación de IFDs en teclados con interfaz PS/2.

- **Parte 5.** Describe las interfaces y funcionalidad que provee el administrador de recursos de las ICCs.
- **Parte 6.** Describe el modelo del proveedor de servicios del ICC, identifica las interfaces requeridas e indica como estas se pueden extender para cumplir con los requerimientos de aplicaciones de dominio específico.
- **Parte 7.** Describe las consideraciones para el diseño de aplicaciones y como hacer uso de los demás componentes.
- **Parte 8.** Recomendaciones para la implementación de ICCs de seguridad y privacidad.
- **Parte 9.** Describe el manejo de IFDs con algunas capacidades extendidas.
- **Parte 10.** Describe el manejo de IFDs con capacidades de entrada segura de PIN.

Arquitectura de PC/SC

La arquitectura que define la especificación PC/SC se compone básicamente de los siguientes elementos:

- **Tarjeta con circuito integrado (ICC)** – Se refiere a la tarjeta inteligente. Esta especificación es compatible con ICCs que cumplen con estándares ISO 7816-1,2,3 y 10 para tarjetas de contacto síncronas y asíncronas. También es compatible con tarjetas sin contacto que cumplen con estándares ISO/IEC 14443 (de proximidad), ISO/IEC 15693 (de vecinidad) y similares.

- **Dispositivo lector (IFD)** – Se refiere al lector de tarjetas, el cual es la interfaz física por medio del cual el ICC se comunica con la PC. Un IFD puede tener una o más ranuras para tarjetas y pueden también permitir ciertas funciones adicionales como pantallas de despliegue, lector de huella digital y teclado. Además los lectores pueden tener diferentes puertos de conexión con la PC, como por ejemplo USB, serial, puerto de teclado, PCMCIA, etc.

- **Controlador del lector** - Es un software de bajo nivel que se encuentra en la PC y controla los canales de entrada y salida utilizados para conectar el IFD a la PC. Este provee acceso a funciones específicas del IFD y esconde las diferencias entre IFDs que tienen varias funciones y los que son sencillos.

- **Administrador de recursos del ICC** – Este es un componente clave de la arquitectura PC/SC. Se encuentra a nivel del sistema y es el responsable de administrar los otros recursos relevantes al ICC dentro del sistema, además de controlar el acceso a los IFDs y, a través de ellos, el acceso a ICCs en particular. Lo provee el vendedor del sistema operativo y debe existir solamente un controlador de recursos por sistema. Administración el acceso entre múltiples IFDs e ICCs de la siguiente manera:

    1. Es el responsable de la identificación y rastreo de los recursos, lo cual incluye:

        - Rastrear los IFDs instalados y presentar información respecto a ellos a las demás aplicaciones.
        - Rastrear los tipos de ICC conocidos, junto con sus proveedores de servicios asociados e interfaces que soporta, haciendo disponible esta información a las demás aplicaciones.
        - Rastrear los eventos de inserción y retiro de ICCs para mantener información exacta sobre los ICCs que están insertados en los IFDs disponibles.

    2. Es el responsable de controlar la localidad de los IFDs y sus recursos a través de múltiples aplicaciones.

    3. Soporta transacciones para el acceso a servicios disponibles dentro de un ICC, permitiendo ejecutar varios comandos dentro de una misma función.

- **Proveedores de servicios del ICC** – Son componentes que encapsulan funcionalidad expuesta por cierto ICC para hacerla accesible a través de interfaces de programación de alto nivel. Estas funcionalidades se dividen en servicios del sistema operativo del ICC y en servicios específicos del dominio de la aplicación.

- **Proveedor de servicios criptográficos** – Encapsula acceso a funciones criptográficas del ICC a través de interfaces de programación de alto nivel. Entre las funciones se encuentran la generación de llaves, administración de llaves, firmas digitales, algoritmos Hash, servicios de cifrado, importación y exportación de llaves.

En la figura C1 se muestra el diagrama de la arquitectura que define la especificación PC/SC, en términos de elementos de hardware y software.

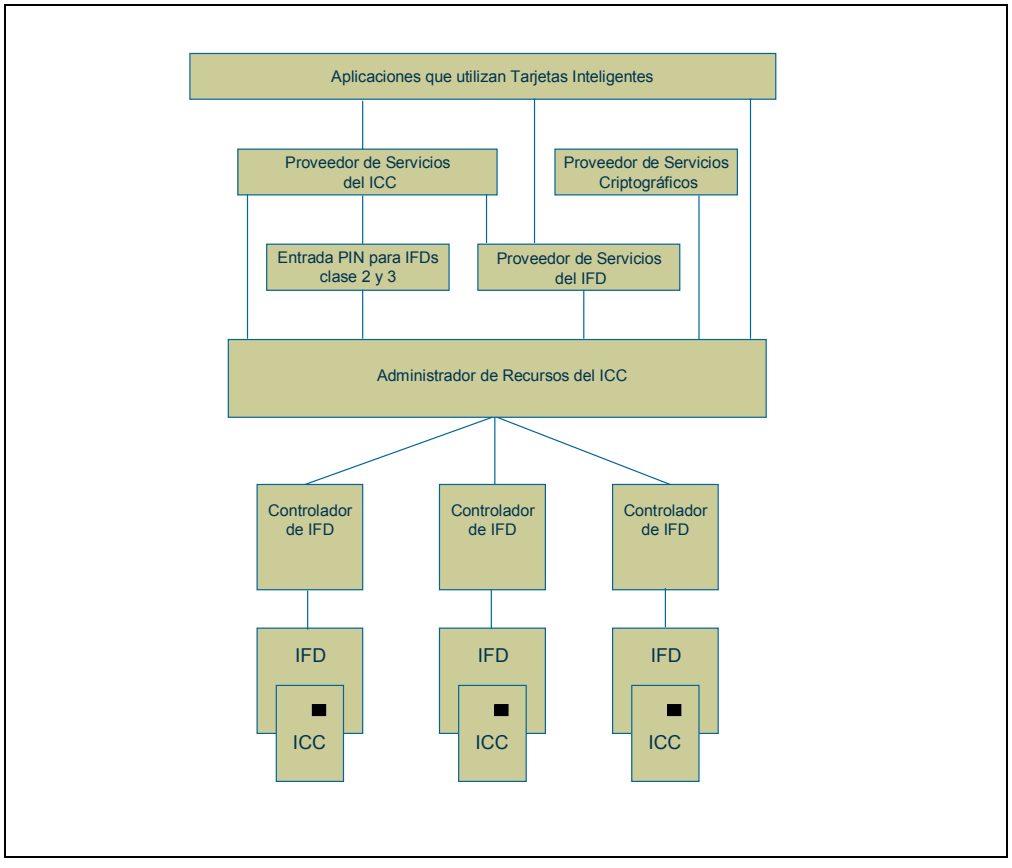

Figura C1 - Arquitectura de la especificación PC/SC

ANEXO D - Información personal del usuario en la tarjeta inteligente

Los datos personales del usuario, los cuales incluyen su nombre, dirección, clave CURP, teléfono, tipo de sangre, y datos de contactos, se almacenarán en un documento XML en un archivo de la tarjeta inteligente. Este documento podrá ser leído por el sistema de expedientes curriculares, así como por otras aplicaciones sin necesidad de autenticación o claves de acceso, como se detalló en el capítulo IV. El listado de la figura D1 muestra un ejemplo del documento XML que contiene información personal de un usuario.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<datos>
    <curp>
        CARJ730814HBCSML09
    </curp>
    <usuario>
      <nombre>
        Julio César
      </nombre>
      <paterno>
        Castillo
      </paterno>
      <materno>
         Ramírez
      </materno>
      <nacimiento>
        <fecha>
          14081973
        </fecha>
        <ciudad>
          Mexicali
        </ciudad>
        <estado>
          Baja California
        </estado>
        <pais>
            MX
        </pais>
      </nacimiento>
      <sexo>
        H
      </sexo>
      <domicilio>
        <ciudad>
          Mexicali
        </ciudad>
```

```
        <estado>
          Baja California
        </estado>
        <pais>
          MX
        </pais>
        <colonia>
           Residencias
        </colonia>
        <calle>
           Olga
        </calle>
        <num>
           84-C
        </num>
      </domicilio>
      <tel>
        <tipo>
          casa
        </tipo>
        <numtel>
          (686)566-42-98
        </numtel>
      </tel>
      <tel>
        <tipo>
          celular
        </tipo>
        <numtel>
          (686)135-9211
        </numtel>
      </tel>
      <tel>
        <tipo>
          Oficina
        </tipo>
        <numtel>
          (686)557-16-22
        </numtel>
        <ext>
           132
        </ext>
      </tel>
      <sangre>
        O+
      </sangre>
    <grado>
      Ingeniero en Computación
    </grado>
    <grado>
      Maestro en Ciencias e Ingeniería en Computación
    </grado>
    </usuario>
    <contacto>
       <nombre>
           Luis Alfredo
       </nombre>
```

```
        <paterno>
             Sosa
        </paterno>
        <materno>
            Quiróz
        </materno>
        <domicilio>
           <ciudad>
               Mexicali
           </ciudad>
           <estado>
               Baja California
           </estado>
           <pais>
               MX
           </pais>
           <colonia>
               Villas del Cedro
           </colonia>
           <calle>
               Gredos
           </calle>
           <num>
               28-C2
           </num>
       </domicilio>
       <tel>
           <tipo>
              casa
           </tipo>
           <numtel>
              (686)841-34-91
           </numtel>
        </tel>
    </contacto>
    <actualizacion>
         13042006
    </actualizacion>
</datos>
```

Figura D1 – Ejemplo de documento XML con información personal del usuario

Anexo E. Productos generados del proyecto de investigación

1. Castillo, J., Flores, B., Ibarra, J. (2006, Octubre 20). *Tarjetas Inteligentes y sus Aplicaciones*. Taller impartido en el VI Simposium Internacional de Ingeniería Decivel. Facultad de Ingeniería, UABC. Mexicali, B.C., México.

2. Castillo, J., Flores, B., Ibarra, J. (2006, Mayo 9). *Grupo de Investigación en Tarjetas Inteligentes (GRINTAIN) – Estrategias y Resultados*. Conferencia impartida durante la Semana de Computación e Informática en el XXV aniversario del Instituto de Ingeniería, UABC. Mexicali, B.C., México.

3. Ibarra, J., Flores, B., Castillo, J. & Castro, U. (2006). *Diseño de una Arquitectura para el Manejo de Expedientes Curriculares Electrónicos Utilizando Tarjetas Inteligentes.* Congreso Internacional de Ingeniería en Electrónica ELECTRO 2006. Sección Sistemas Inteligentes. Vol. XXVIII. P.p 323-328. ISSN. 1405-2172. Creel, Chi., México.

4. Flores, B., Ibarra, J. & Castillo, J. (2005, Noviembre) *La Problemática del Comercio Electrónico en Comprobantes Curriculares*. Primer Simposium Internacional de Educación. Sección Educación a Distancia. Num. 48. Facultad de Ciencias Humanas, UABC. Mexicali, B.C., México.

5. Castillo, J., Ibarra, J., Flores, B., *"Introducción a las Tarjetas Inteligentes"*. V Simposium Internacional Decivel. Facultad de Ingeniería, UABC. Mexicali, México. Octubre de 2005.

6. Julio Castillo. Conferencia *"Introducción a las Tarjetas Inteligentes y sus Aplicaciones"*. Semana de Informática, CESUES. San Luis Río Colorado, Sonora.

Octubre de 2005.

7. Castillo, J., Ibarra, J. & Flores, B. Publicación de cartel *"Diseño de un Sistema para el Almacenamiento y Recuperación de Expedientes Curriculares Electrónicos utilizando Tarjetas Inteligentes"*. Semana de Moprosoft. Facultad de Ingeniería, UABC. Mexicali, México. Junio de 2005.

8. Sitio Web del grupo de Investigación en Tarjetas Inteligentes
   http://www.grintain.com