

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 utilizarse 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 borrrable), mientras que las alemanas utilizaban EEPROM (memoria de sólo lectura, programable y borrrable 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 ciento 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 las 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 (Breunese, 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

Las 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):

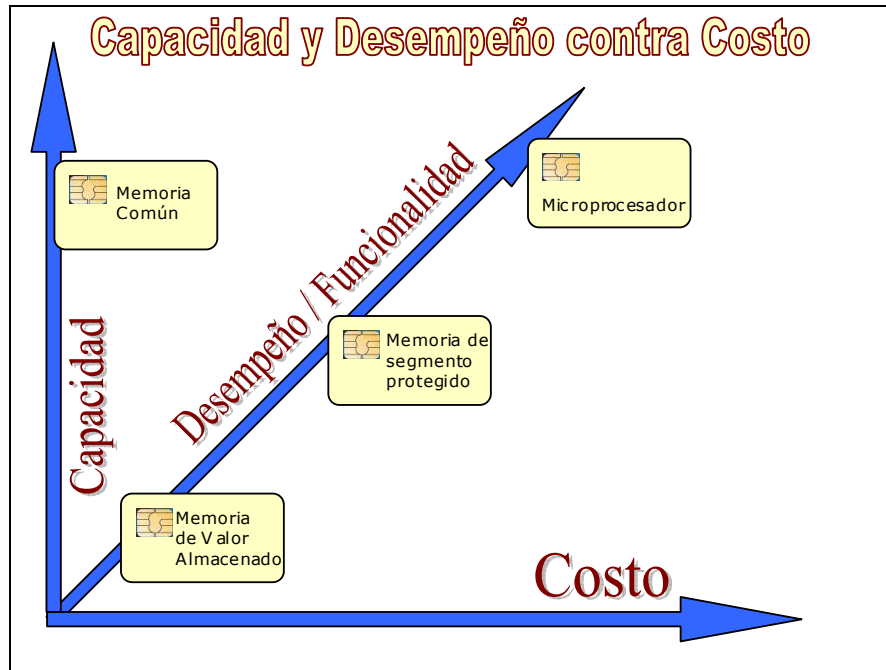


Figura 2.1 Gráfica de capacidad y desempeño vs. costo

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 “Acknowledge 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.

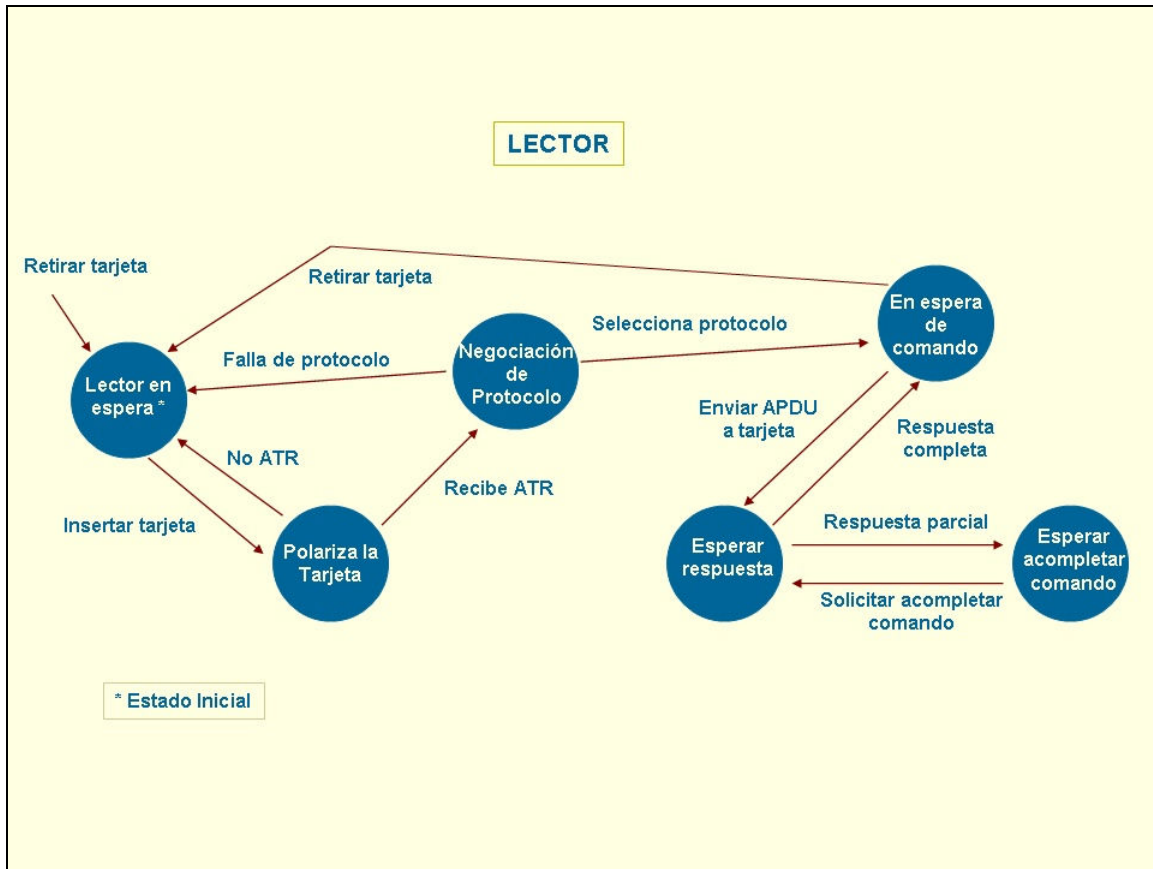


Figura 2.2 Diagrama de estados del lector

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.

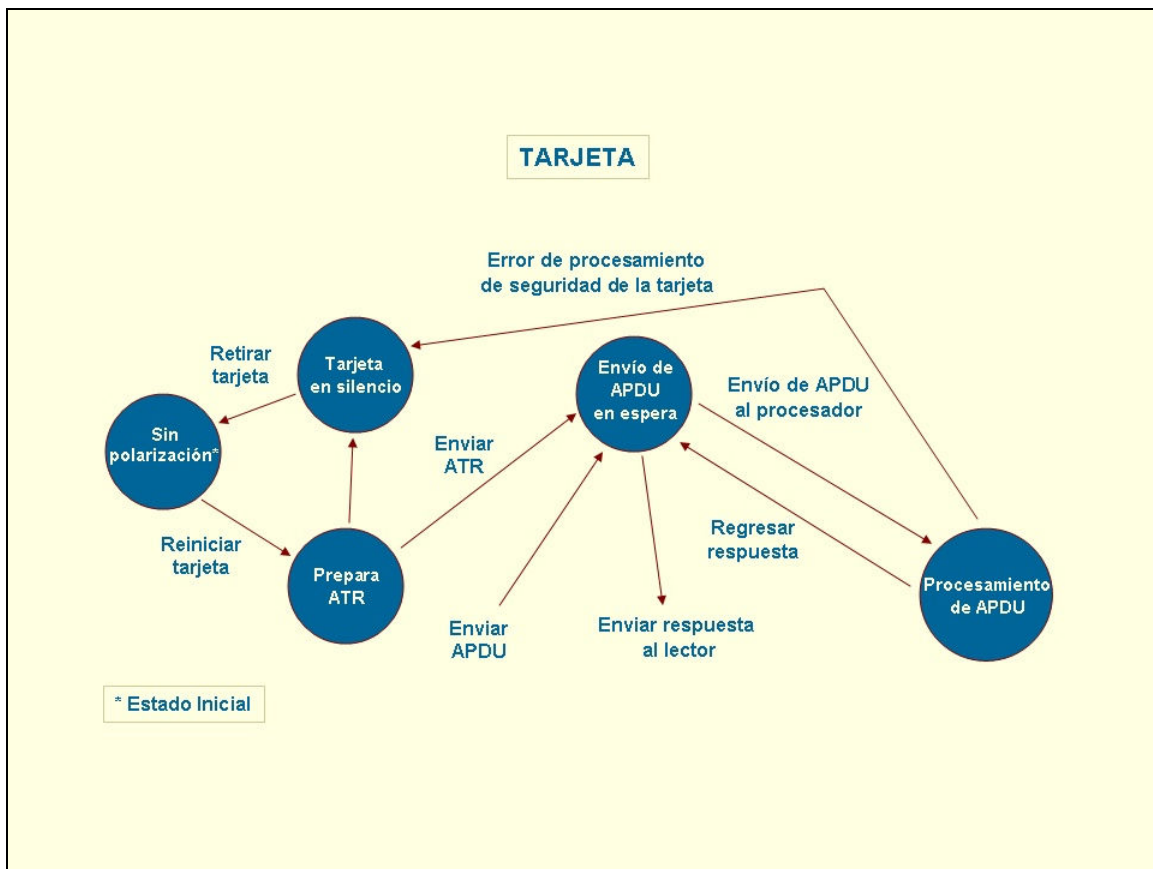


Figura 2.3 Diagrama de estados de la tarjeta inteligente

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 tarjetas 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 autenticación, 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.