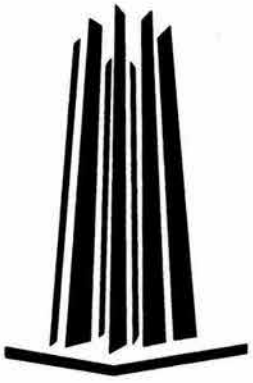
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

"TARJETAS INTELIGENTES, SU TECNOLOGÍA Y LA PROPUESTA DE SU APLICACIÓN PARA CONTROLAR LA SEGURIDAD EN EL DEPARTAMENTO DE INGENIERÍA EN COMPUTACIÓN"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA
P R E S E N T A:
JOSÉ GUADALUPE ROMO MÉNDEZ



DIRECTOR DE TESIS: M. I. JORGE VALERIANO ASSEM

MÉXICO, D.F. 2004

Agradezco a Dios.

Por la vida y el permitirme vivirla plenamente, por los padres, por los hijos y familia que me dio.

A mi madre.

Francisca Méndez León.

Por su amor, por su ejemplo; Mamá en este trabajo como en cualquier otra meta que logre cristalizar su nombre estará implícito en el.

A mi padre.

José Luis Romo Reynoso.

Por que su recuerdo me ha acompañado siempre.

A mis hermanos.

Pili, Raúl y Lulú.

Por su cariño y su incondicional apoyo.

A mi esposa.

Claudia López Guevara.

Por su amor, apoyo y el impulso a ser mejor cada día.

A mis hijos.

Luis y Martha.

Por que son la razón de mi vida.

A mis sobrinos.

Isaac Vega, Alan Romo, Fernanda Romo, porque los quiero como hijos míos.

A la familia López Guevara.

Sr. Joel López, Sra. Beatriz Guevara, Xóchitl, y Beatriz por su cariño.

Al Sr. Felipe Real (QEPD).

Quién me enseñó a trabajar, a ser responsable y siempre apoyo mi educación.

A la empresa Red Color, S.A. de C.V.

A los Ingenieros Alberto, Bernardo y Guillermo Bremer Gutiérrez y al Lic. José Antonio Bremer Cantú por la formación que he recibido trabajando a su lado y por las facilidades queme dieron para realizar este trabajo.

A Miguel, Miguel Angel, Tania y Jorge por su ayuda.

Índice

ÍNDICE

Introducción

INTRODUCCIÓN

La tarjeta con banda magnética ha sido un medio ampliamente utilizado como dispositivo para grabar datos del usuario. Las aplicaciones más conocidas son la tarjeta de identificación, control de acceso y la tarjeta de débito/crédito. Sin embargo, su reducida capacidad para almacenar información y, sobre todo, la vulnerabilidad que presenta al permitir su reproducción de manera ilícita, lleva a la necesidad de tener dispositivos que cubran estas deficiencias.

La tecnología de Tarjetas Inteligentes (TI's), sustentada en el desarrollo de la microelectrónica, viene a reemplazar el uso de tarjetas con código de barras o con banda magnética. La capacidad para almacenar mayor información que sus predecesoras, la facilidad de incorporar mecanismos sofisticados de seguridad como los algoritmos de encriptado y desencriptado, el manejo de llave pública y privada y, principalmente, la capacidad de procesamiento, la convierten en el dispositivo ideal para controlar el manejo de dispositivos, acceso a equipos, servicios e instalaciones.

El Departamento de Ingeniería en Computación de la Facultad carece de sistemas automatizados que controlen el acceso, además está expuesto a la presencia de personas ajenas a sus actividades, por lo que es necesario contar con un sistema eficiente para proteger los recursos humanos, materiales y de información que integran su patrimonio ya que cuenta con una importante infraestructura de equipo, indispensable para desarrollar sus labores académicas y de investigación. En este sentido, una posible solución es la implementación de un sistema basado en la tecnología de tarjetas inteligentes.

Esta tesis presenta las bases teóricas para entender la tecnología de TI's y una propuesta enfocada al desarrollo de un modelo de aplicación que permita cubrir los siguientes aspectos:

- Contar con un medio de identificación seguro y confiable.
- Controlar el acceso a las instalaciones del departamento.
- Reducir los costos originados por daños al patrimonio.

El presente trabajo está estructurado de la siguiente manera:

- Marco Teórico. Proporciona una panorámica de la teoría utilizada en las tarjetas inteligentes como son las memorias y microprocesadores.
- Tarjetas Inteligentes. Presenta el estado del arte de las tarjetas inteligentes, su clasificación, características físicas y técnicas.
- Sistemas Operativos para Tarjetas Inteligentes. Explica su sistema operativo, así como la estructura de archivos y la seguridad de la información.
- Dispositivos de Interfaz. Detalla algunos tipos de lectores y terminales existentes, su clasificación y características principales; además, menciona los protocolos de comunicación.
- Aplicaciones. Muestra un resumen de algunas de las aplicaciones de esta tecnología a nivel mundial y en nuestro país.
- Modelo para la Aplicación de la TI. Propone el modelo conceptual para la aplicación de esta tecnología en la Facultad de Ingeniería y el Departamento de Computación. Asimismo, la recomendación de incluir este tópico para la asignatura Temas Especiales.

Marco Teórico

- El transistor
- El circuito integrado
- Memorias
- Dispositivos lógicos programables (PLD's)
- Microprocesadores

Capítulo 1

CAPÍTULO 1. MARCO TEÓRICO

Desde sus orígenes, el ser humano ha dedicado gran parte de su tiempo a desarrollar mecanismos que faciliten su vida diaria. La innovación permanente que existe en todos los campos de la electrónica se debe, sin duda alguna, a la introducción de los dispositivos de estado sólido o semiconductores. Un material semiconductor es aquel cuya resistencia eléctrica es intermedia entre los materiales aislantes y los conductores. Ya en el año 1906 se utilizaban gran variedad de cristales semiconductores como detectores de aparatos de radio. Los materiales empleados eran la galena, el silicio, las ferritas y el carborúndum.

1.1 EL TRANSISTOR

1.1.1 Los tubos de vacío

Durante el periodo de 1904 a 1947, el tubo de vacío o bulbo fue el dispositivo electrónico de interés, objeto de investigación y desarrollo. En 1904, el diodo de tubo de vacío fue introducido por J. A. Flemming. Poco después, en 1906, Lee De Forest agregó un tercer elemento denominado rejilla de control al tubo de vacío, lo que originó el primer amplificador denominado tríodo. En los años siguientes, la radio y la televisión brindaron un gran impulso a la industria de los tubos electrónicos, también conocidos como bulbos. La producción aumentó de casi 1,000,000 de tubos en 1922 hasta aproximadamente 100,000,000 en 1937. A principios de la década de los treintas el tetrodo de cuatro elementos y el pentodo de cinco elementos se distinguieron en la industria de los tubos electrónicos. Durante los años subsecuentes este sector se convirtió en uno de los más importantes de la industria logrando avances rápidos en el diseño, las técnicas de manufactura, las aplicaciones de alta potencia y alta frecuencia.

1.1.2 El transistor

El 23 de diciembre de 1947, William B. Shockley, Walter H. Brattain y John Bardeen, premio Nobel en Física para el año 1956, demostraron el efecto amplificador del primer transistor en los laboratorios de Bell Telephone. Las ventajas de este dispositivo de estado sólido de tres terminales sobre el tubo de vacío fueron evidentes. Su designación es abreviatura del inglés **tran**sfer re**sistor**; fue el primer dispositivo de estado sólido capaz de amplificar señales eléctricas. Puede decirse que desde entonces los semiconductores se han introducido como elementos imprescindibles en todos los campos de la electrónica.

Las ventajas que aportaron los transistores al reemplazar a los tubos de vacío, se pueden sintetizar en los puntos siguientes:

- Tamaño reducido.
- Bajo consumo de energía.
- Gran estabilidad.
- Reducido nivel de alimentación.
- Simplicidad en el diseño de circuitos electrónicos.
- Reducción de costos.
- Respuesta inmediata, debido a que no requieren tiempo de calentamiento.

Todas estas características han hecho posible la creación de equipos miniaturizados. La carrera por la miniaturización no se detuvo con la invención del transistor, por el contrario, solamente marcó el inicio. Posteriormente el papel protagónico le correspondió al circuito integrado (IC).

1.2 EL CIRCUITO INTEGRADO

1.2.1 Características

Un circuito integrado, también conocido como chip, es un elemento compacto producido en una pequeñísima placa de silicio que cumple con las funciones de un circuito electrónico completo, en él se integran diversos componentes activos y pasivos. Se fabrica como un conjunto inseparable de elementos dentro de una pequeña y única estructura la cual no puede ser dividida pues perdería su función electrónica. El primer circuito integrado fue desarrollado en 1950 por Jack Kilby de Texas Instruments y Robert Noyce de Fairchild Semiconductor.

Para lograr un menor tamaño, los investigadores siguieron desarrollando nuevas técnicas que condujeron a la microelectrónica. La microelectrónica puede dividirse en dos partes, una perteneciente a los circuitos integrados monolíticos, componentes activos y pasivos formados en una placa de silicio, y otra que comprende los circuitos peliculares.

1.2.2 Clasificación de los circuitos integrados

Los circuitos integrados son clasificados por el nivel de integración, término que se usa para proporcionar una medida del número de transistores y otros componentes electrónicos que contienen, esto se detalla en la Tabla 1.1. También de acuerdo con sus aplicaciones, los circuitos integrados se pueden dividir en analógicos y digitales.

Clasificación	Descripción	Características	Ejemplo
SSI	Integración de pequeña escala (*Small Scale Integration*)	Hasta 100 componentes	Compuertas 7400
MSI	Integración de mediana escala (*Medium Scale Integration*)	De 100 a 3,000 componentes	Decodificador 7442
LSI	Integración de gran escala (*Large Scale Integration*)	De 3,000 a 100,000 componentes	PLA 82S100
VLSI	Integración de escala muy grande (*Very Large Scale Integration*)	De 100,000 a 1,000,000 componentes	Intel 486
ULSI	Integración de escala ultra grande (*Ultra Large Scale Integration*)	Aprox. un billón de componentes	Intel Itanium

Tabla 1.1 *Clasificación de circuitos integrados por el número de componentes*

1.2.3 Tipos de encapsulados

Los circuitos integrados se fabrican sobre grandes obleas circulares de silicio, sobre ellas se crean muchos circuitos individuales al mismo tiempo. El circuito integrado está formado por muchas capas de materiales diferentes, donde cada una tiene su propio patrón y

características eléctricas distintivas. El proceso de creación del patrón sobre una capa se llama litografía óptica. Esta técnica permite crear patrones con un ancho menor de 0.5 µm.

La capacidad para crear circuitos tan pequeños ha permitido construir el nivel VLSI. La importancia de la distribución física es una característica del proceso litográfico ya que debe tener tamaños medibles, los aspectos más importantes son:

- El ancho de la línea metálica.
- El espaciamiento de una línea a otra entre líneas metálicas adyacentes.

En la fabricación de circuitos integrados con tecnología MOSFET el ancho mínimo de una línea es 0.8 µm, mientras que el espacio de las líneas adyacentes es de 1.2 µm.

Los avances en la formación litográfica de patrones han reducido el tamaño del transistor, esto era imposible hace algunos años. Las líneas de producción actuales fabrican transistores con longitudes de canal tan pequeñas como 0.13 µm, y se espera llegar a valores menores que 0.1 µm en la siguiente generación de plantas de producción. En la Figura 1.1 se muestra el avance en la disminución de la longitud de canal en los últimos años y su tendencia.

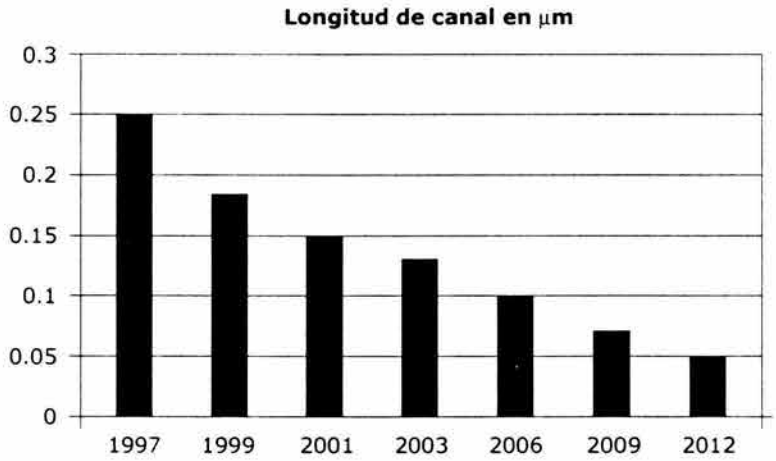


Figura 1.1 *Reducción de la longitud de canal (Fuente: Intel)*

Los chips vienen en diferentes encapsulados como se puede apreciar en la Figura 1.2. Los más comunes son:

- SIP (*Single In-line Packages*). Estos chips cuentan con una sola hilera de conectores.
- DIP (*Dual In-line Packages*). Son los chips tradicionales, pueden tener de 8 a 40 patas acomodadas en dos hileras por ambos extremos del chip.
- LCC (*Leadless Chip Carrier*). Este tipo de encapsulado no tiene pines de conexión externos y deben ser colocados en un receptáculo para su conexión.
- SOP (*Small Outline Packages*). Este empaque rectangular para montaje de superficie tiene dos filas de conectores.

- FLATPACK. Este tipo de encapsulado es el comúnmente utilizado para circuitos montados en la superficie.
- PGA (*Pin-Grid Arrays*). Son chips cuyas terminales están alineadas en cuadros concéntricos.

En adición a estos tipos existen los llamados SIMM's (*Single In-line Memory Modules*) y los DIMM's (*Dual In-line Memory Module*). Los SIMM's consisten en un arreglo de hasta nueve chips ensamblados en una tarjeta y cuyo comportamiento es como si fueran una sola unidad. Los módulos de memoria DIMM, se parecen bastante a la memoria de tipo SIMM. Al igual que los SIMM's, la mayoría de los DIMM's se instalan verticalmente en las ranuras de expansión. La diferencia principal entre los dos consiste en que, en un chip SIMM, los contactos de cada fila se unen con los contactos correspondientes de la otra fila para formar un sólo contacto eléctrico; en un chip DIMM, los contactos opuestos permanecen eléctricamente aislados para formar dos contactos separados.

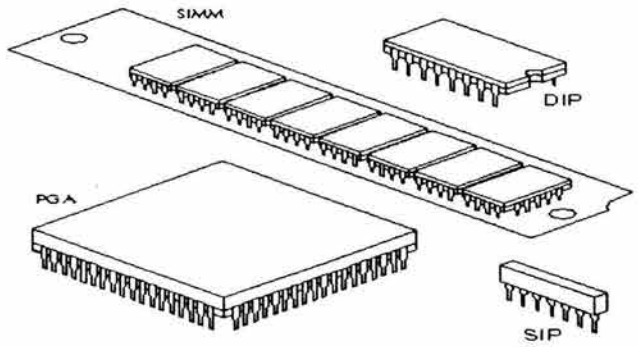


Figura 1.2 *Tipos de chips*

1.2.4 Uso de los circuitos integrados

En la electrónica de consumo, los circuitos integrados han hecho posible el desarrollo de nuevos productos como las computadoras, las calculadoras digitales, los relojes digitales y los videojuegos. Se han utilizado también para mejorar y reducir el costo de otros existentes como los televisores, los receptores de radio y los equipos de alta fidelidad. Su uso está muy extendido en la industria, la medicina, el control de tráfico aéreo y terrestre, el control ambiental y las comunicaciones.

1.3 MEMORIAS

También se han desarrollado, a partir de semiconductores, otros dispositivos electrónicos que día con día toman mayor relevancia: las memorias, cuya función es el almacenamiento de datos binarios a corto o largo plazo.

Las computadoras y otros sistemas requieren el almacenamiento temporal o permanente de un gran número de datos binarios. Los sistemas basados en microprocesadores necesitan

memoria para almacenar programas y/o datos generados durante el procesamiento, de tal manera que puedan accesarlos cuando sea necesario.

Las memorias se clasifican de acuerdo a la tecnología empleada en su fabricación en memorias semiconductoras, magnéticas y ópticas. Para los fines que persigue esta investigación, este trabajo sólo se centrará en las memorias semiconductoras.

1.3.1 Memorias semiconductoras

Las memorias semiconductoras están formadas por matrices de elementos de almacenamiento que pueden ser circuitos digitales latches o flip-flops, capacitores, o cualquier otro elemento que permita almacenar una carga eléctrica.

La información se almacena en unidades conocidas como bits cuyo valor puede ser 0 ó 1 solamente; es decir, con carga o sin carga. Las memorias guardan datos en unidades que van de uno a ocho bits. Una unidad completa de información se conoce como palabra y generalmente se forma con grupos de 8 bits.

Las memorias semiconductoras están constituidas por celdas organizadas en forma matricial, cada celda representa un bit que puede tener el valor 0 o señal baja o bien el valor 1 o señal alta. Cada bloque de la matriz de memoria representa una celda de almacenamiento y su ubicación puede ser determinada mediante la fila y columna correspondiente.

La Figura 1.3 (a) muestra una matriz de 8 filas por 8 columnas, ésta se puede interpretar como una memoria de 64 bits (8 x 8 = 64) o bien como una memoria de 8 bytes. La Figura 1.3 (b) corresponde a una matriz de 32 x 4 equivalente a una memoria de 128 bits o bien de 16 bytes. La última Figura, 1.3 (c), corresponde a una matriz de 32 x 1, es decir una memoria de 32 bits. La memoria se identifica mediante el número de palabras que puede almacenar, multiplicado por el tamaño de la palabra.

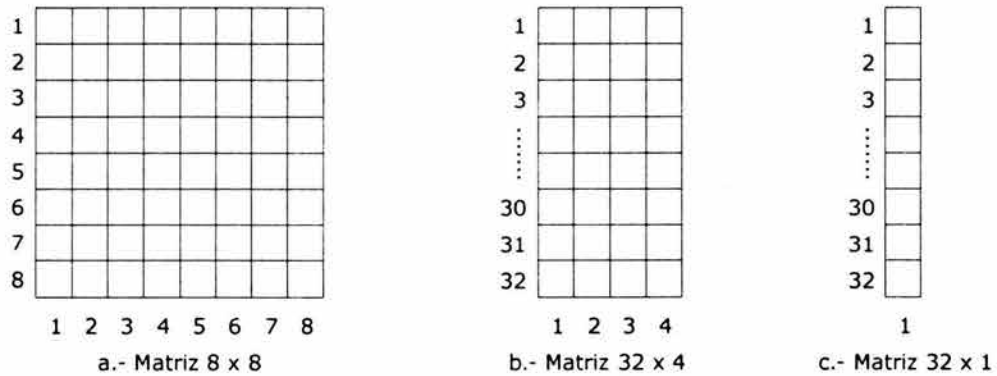


Figura 1.3 *Distintos arreglos de memoria*

Una memoria está formada por el bus de direcciones, el bus de control, el bus de datos y la matriz de memoria, como se muestra en la Figura 1.4.

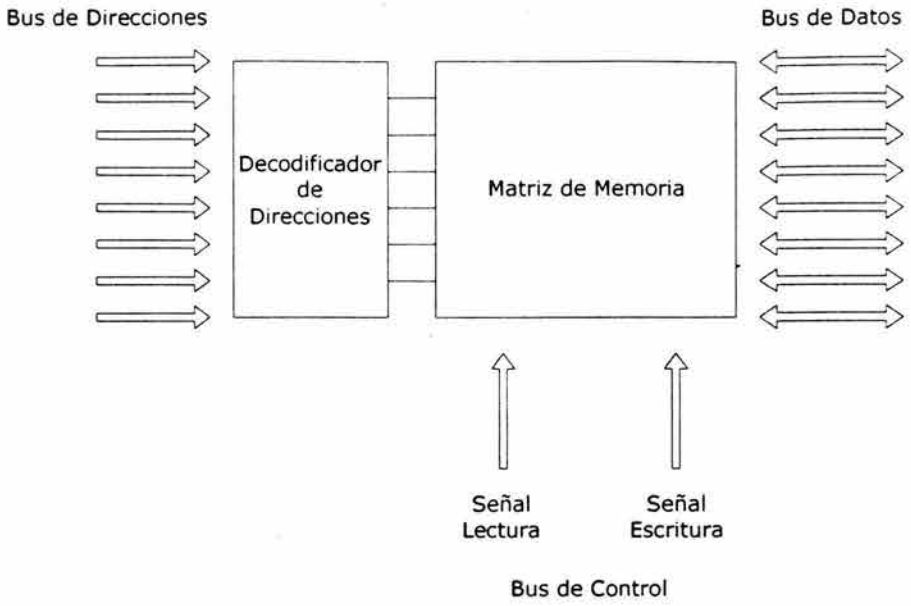


Figura 1.4 *Diagrama de bloques de una memoria*

Para efectuar una lectura se indica en el bus de direcciones la dirección de la palabra de memoria que se desea leer, entonces se activa la señal de lectura. Después de cierto tiempo, el tiempo de latencia de la memoria, aparece en el bus de datos el contenido de la dirección buscada.

Cuando el proceso es de escritura, se deposita en el bus de datos la información que se quiere almacenar y en el bus de direcciones la dirección donde se desea guardar; a continuación, se habilita la señal de escritura. Una vez que pasa el tiempo de latencia la memoria escribe los datos en el área designada.

Las memorias semiconductoras se dividen en dos categorías principales en función de su capacidad de lectura y/o escritura: ROM y RAM.

1.3.1.1 Memoria ROM

Una memoria ROM (*Read Only Memory*, memoria de sólo lectura) mantiene de forma permanente o semipermanente los datos almacenados en ella. Estos pueden ser leídos pero no modificados, aunque en algunos casos es posible hacerlo mediante el uso de equipo especial. Las ROM's almacenan información que se utiliza repetidamente en las aplicaciones, tales como tablas, instrucciones programadas para la inicialización y el funcionamiento del sistema, etc. La memoria ROM mantiene su contenido incluso cuando se desconecta la fuente de energía que la alimenta, en virtud de esta característica también se le conoce como memoria no volátil.

Las memorias ROM's se subdividen en ROM de Máscara, PROM, EPROM, UV EPROM y EEPROM, Figura 1.5.

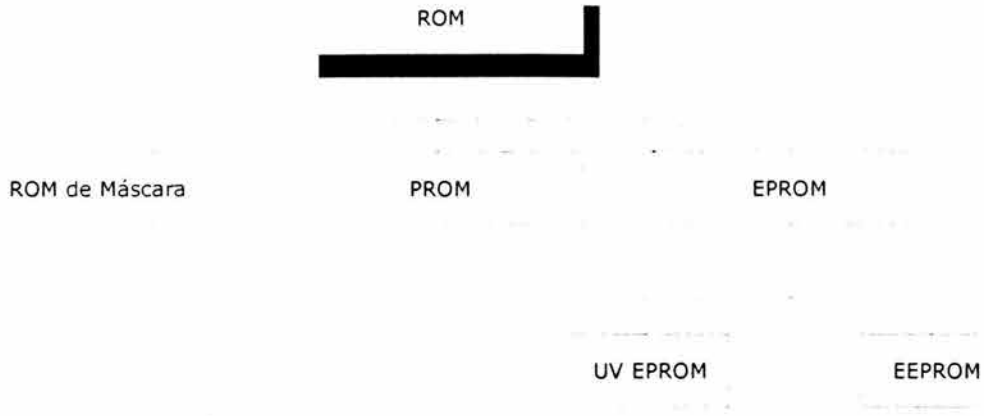


Figura 1.5 *Familia de memorias ROM's*

La ROM de máscara, denominada simplemente ROM, es una memoria programada de forma permanente durante el proceso de fabricación para proporcionar funciones estándar de uso generalizado. Una vez programada, su contenido no puede cambiarse. La mayoría de los circuitos integrados ROM utilizan la presencia o ausencia de un transistor en una unión fila/columna para representar un 1 o un 0.

La memoria ROM se utiliza en computadoras personales para almacenar el BIOS (*Basic Input/Output Services*, Servicios básicos de entrada/salida). Estos son programas que se utilizan para realizar tareas fundamentales de control y soporte en las computadoras como por ejemplo, controlar ciertas funciones del monitor de vídeo, permitir el formateo de los discos, explorar si se ha pulsado el teclado, controlar ciertas funciones de impresión, permitir pasar el control al sistema operativo, etc.

Las PROM's son similares a las memorias ROM's de máscara. La diferencia es el hecho de no ser programadas de fábrica sino por el usuario quien lo realiza de acuerdo a sus necesidades. La programación se lleva a cabo insertando la memoria PROM en un dispositivo especial conocido como programador de PROM's, el cual se controla por software.

Una EPROM es una PROM con capacidad de borrado. A diferencia de una PROM, una EPROM puede reprogramarse después de borrar el programa residente en la matriz de memoria. Existen dos tipos de EPROM's, las que son borradas por rayos ultravioleta UV EPROM's y las EEPROM's que se pueden borrar eléctricamente.

Una UV EPROM se reconoce por la ventana de cuarzo transparente de su encapsulado. El borrado se realiza mediante la exposición del chip de la matriz de memoria a una radiación ultravioleta a través de la ventana, en un periodo de tiempo que va desde unos minutos hasta una hora de exposición.

Las EEPROM's se pueden borrar y programar mediante impulsos eléctricos. Su ventaja es la facilidad de poderlas reprogramar dentro del propio circuito final, sin tener que sacarlo del mismo. Esto permite cambiar la configuración de cualquier sistema fácil y rápidamente.

1.3.1.2 Memoria RAM

La memoria RAM (*Random Access Memory*, memoria de acceso aleatorio) es un tipo de memoria de acceso directo; mejor dicho, el tiempo que tarda en accesar cualquier dirección de memoria es el mismo y estas direcciones se pueden seleccionar en cualquier orden, tanto en una operación de escritura como de lectura.

Tiene como característica la destrucción de la información previamente almacenada cuando realiza la escritura, cosa que no sucede con la lectura. Las memorias RAM's se utilizan para almacenar datos a corto plazo, ya que estos se pierden cuando se desconecta la alimentación de la memoria, por esta razón son denominadas memorias volátiles.

Los principales tipos de memoria RAM son las RAM's estáticas o SRAM (*Static RAM*) y las RAM's dinámicas o DRAM (*Dynamic RAM*), Figura 1.6.

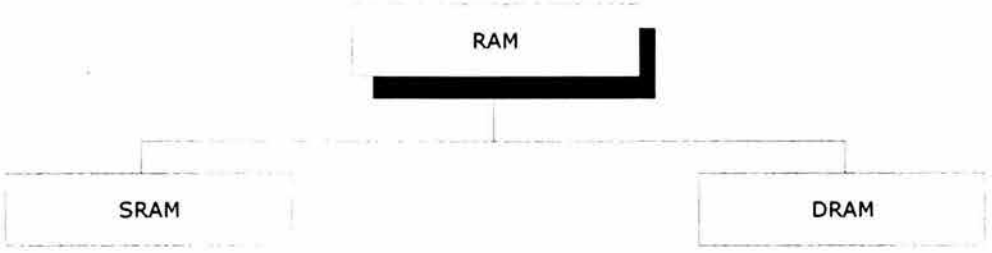


Figura 1.6 *Familia de memorias RAM's*

Las SRAM's utilizan latches como elementos de almacenamiento, pueden guardar información durante un periodo de tiempo indefinido mientras esté conectada la alimentación o, hasta que se escriba un nuevo bit de datos.

Las memorias DRAM's almacenan los datos en capacitores, requieren recargarse (refrescarse) periódicamente para mantener la información. Este tipo de celda es muy sencillo, lo que permite construir matrices de memorias muy grandes en un chip a un costo por bit más bajo que las memorias estáticas; sin embargo, el ciclo de refrescado de datos requiere circuitos de memoria adicional que complican el funcionamiento de la DRAM. Además, para acceder a una dirección de memoria es necesario esperar a que concluya el ciclo de refresco.

Generalmente, una DRAM se actualiza cada 8 ms o 16 ms, en algunos dispositivos puede exceder los 100 ms. Una operación de lectura refresca automáticamente todas las direcciones de la fila seleccionada aunque no siempre se puede predecir que tan a menudo

se producirá un ciclo de lectura, por lo tanto, no se puede depender del ciclo de lectura para recargar la información.

1.3.1.3 Memoria FLASH

También existen las memorias FLASH, son memorias de lectura/escritura de alta densidad (gran capacidad de almacenamiento de bits) no volátiles, lo que significa que los datos se pueden guardar indefinidamente sin necesidad de alimentación. Por alta densidad se entiende la capacidad de empaquetar en una pequeña superficie del chip una gran cantidad de celdas. Esto implica que a mayor densidad, mayor cantidad de bits.

La memoria FLASH es la memoria ideal porque posee una capacidad de almacenamiento alta, es no volátil, tiene capacidad de lectura/escritura, rapidez de operación comparativamente alta y buena relación calidad/precio. Las tecnologías tradicionales de memoria como la ROM, PROM, EPROM, EEPROM, SRAM y DRAM, poseen una o más características pero ninguna de ellas tiene todas, excepto las memorias FLASH.

Actualmente se utilizan en la fabricación de BIOS para computadoras, denominadas FLASH BIOS. Esta tecnología ofrece la ventaja de actualizar el BIOS con software proporcionado por el fabricante, sin necesidad de desmontar el chip del circuito final ni usar otros aparatos.

1.4 DISPOSITIVOS LÓGICOS PROGRAMABLES (PLD's)

Un dispositivo lógico programable, o PLD (*Programmable Logic Device*), es un dispositivo cuyas características pueden ser modificadas y almacenadas mediante programación.

La mayoría de los PLD's están formados por una matriz de conexiones, una matriz de compuertas AND, y una matriz de compuertas OR, y algunos, además, incluyen registros. Las matrices pueden ser fijas o programables. Con estos recursos se implementan las funciones lógicas deseadas mediante un software especial y un programador de dispositivos. La estructura general de un PLD se muestra en la Figura 1.7.

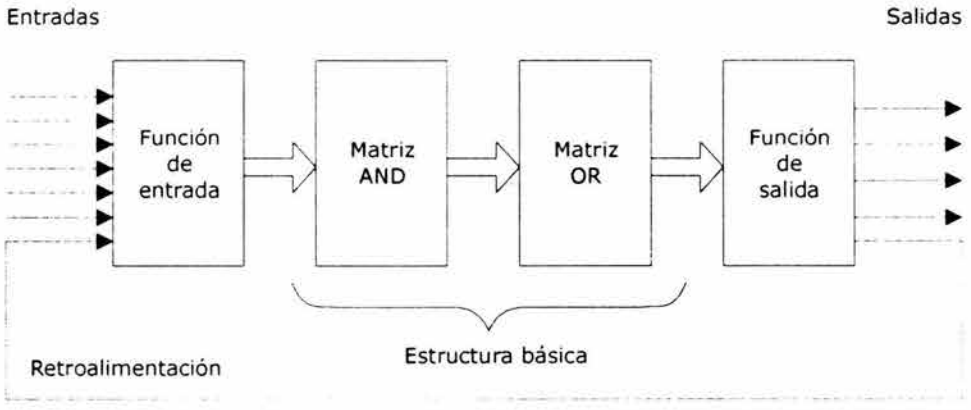


Figura 1.7 *Estructura general de un PLD*

1.4.1 Tecnologías de programación

Las tecnologías de programación enfocadas al control de las conexiones utilizadas en estos dispositivos son las siguientes:

- Programación por fusible. Cada punto programable consiste en una conexión formada por un fusible. Cuando un voltaje considerablemente más grande que el voltaje de la fuente es aplicado a través del fusible, la intensidad de la corriente produce que se rompa la conexión fundiendo el fusible. Los dos estados de conexión existentes son cerrado y abierto representados por un fusible intacto y uno fundido respectivamente.

- Programación por máscara. Esta programación es llevada a cabo por el fabricante del semiconductor durante los últimos pasos del proceso de fabricación. Las conexiones son realizadas o no en las capas de metal sirviendo como conductores en el circuito. La estructura de estas capas es determinada por la función deseada para el circuito.

- Programación por "antifusible". Como el nombre lo sugiere el antifusible tiene un comportamiento opuesto al fusible. El antifusible consiste de un área pequeña en la cual dos conductores están separados por un material de alta resistencia, por lo tanto actúa como un camino abierto antes de la programación. Con la aplicación de un voltaje más alto que el normal de operación, a través de los conductores, el material que los separa es fundido cambiando a un valor de resistencia baja, esto lo convierte en conductor proporcionando un camino cerrado.

- Programación por bit de SRAM. Esta programación se realiza manejando la compuerta de un transistor MOS en el punto de programación. Si el bit SRAM almacena un 1, el transistor es encendido y la conexión entre su fuente (*source*) y drenador (*drain*) forman un camino cerrado. Para el bit SRAM igual a 0, el transistor está apagado y la conexión entre la fuente y el drenador es un camino abierto.

Las tres primeras tecnologías de conexión fusible, máscara y antifusible son permanentes, los dispositivos no pueden ser reprogramados porque la programación ha generado cambios físicos irreversibles. En la tecnología de bit SRAM el contenido de la programación puede ser cambiado electrónicamente. Para almacenar el bit SRAM, la fuente de energía suministrada debe estar disponible, esto la hace de tipo volátil, es decir, la programación lógica se pierde en ausencia de la energía suministrada.

1.4.2 Clasificación de los PLD's

Los dispositivos lógicos programables se pueden clasificar de acuerdo con su arquitectura, la cual es básicamente la ordenación funcional de los elementos internos que proporcionan al dispositivo sus características específicas. Dentro de esta clasificación se encuentran:

- Las memorias de sólo lectura (ROM)
- Los arreglos lógicos programables (PLA)
- La lógica de arreglos programables (PAL)
- La lógica de arreglos genéricos (GAL)
- Los dispositivos lógicos programables complejos (CPLD)
- Los arreglos de compuertas programables en campo (FPGA)

1.4.2.1 Memoria de sólo lectura (ROM)

La memoria ROM, explicada en el punto 1.3.1.1, cuenta con una estructura general que incluye un decodificador a la entrada y una matriz de compuertas OR a la salida. Las entradas dan la dirección para la memoria y las salidas proporcionan los bits de datos de la palabra de almacenamiento que ha sido seleccionada por la dirección. En la Figura 1.8 se muestra la lógica interna de una memoria de 32 palabras de 8 bits cada una (ROM de 32 x 8). Existen diferentes tipos de memorias ROM's las cuales se mencionan en la sección 1.3.1.1

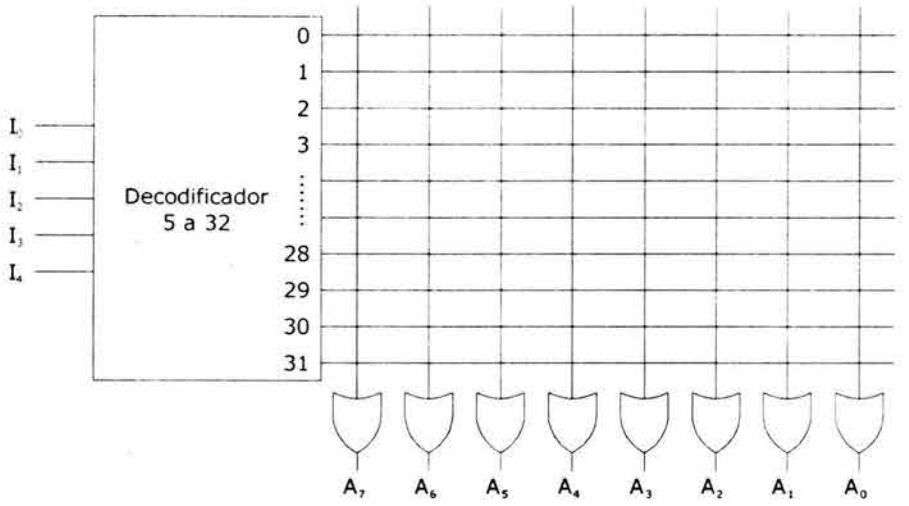


Figura 1.8 *Lógica interna de una ROM de 32 x 8*

1.4.2.2 Arreglo lógico programable PLA (*Programmable Logic Array*)

EL arreglo o matriz lógico programable, PLA, es un PLD formado por una matriz de compuertas AND programable y por una matriz OR también programable. Se le denomina FPLA (*Field Programmable Logic Array,* arreglo lógico programable en campo) debido a que es el usuario y no el fabricante el encargado de realizar su programación.

El PLA fue desarrollado para superar algunas limitaciones de las memorias PROM's, aunque es similar en su concepto el PLA no provee una decodificación completa de las variables y no genera todos los mintérminos. El decodificador es reemplazado por un arreglo de compuertas AND que pueden ser programadas para generar términos de productos de las variables de entrada. Los términos de productos son entonces selectivamente conectados a compuertas OR para proveer la suma de productos requeridos para las funciones Booleanas.

1.4.2.3 Lógica de arreglo programable PAL (*Programmable Array Logic*)

Este PLD se desarrolló para superar ciertas desventajas del PLA tales como los largos retardos debidos a los fusibles adicionales que resultan de la utilización de dos matrices programables en serie y la mayor complejidad del circuito.

El PAL básico está formado por una matriz de compuertas AND programable y una matriz OR fija con la lógica de salida, es el PLD más comúnmente utilizado cuando el programa se escribe una sola vez.

1.4.2.4 Arreglo lógico genérico GAL (*Generic Array Logic*)

Un GAL en su forma básica es un PLD con una matriz AND reprogramable, una matriz OR fija y una lógica de salida programable mediante una macrocelda. Esta estructura permite implementar cualquier función lógica en forma de suma de productos con un número de términos definido.

En los PLD's no reprogramables la síntesis de las ecuaciones lógicas se realiza mediante la quema de fusibles en cada punto de intersección de los pines de entrada con las compuertas. En un GAL el fusible se reemplaza por una celda CMOS eléctricamente borrable (EECMOS) y mediante programación se activa o desactiva cada celda EECMOS. Una celda activada conecta su correspondiente intersección de fila y columna, y una celda desactivada desconecta dicha intersección. Con esta estructura se puede aplicar cualquier combinación de variables de entrada, o sus complementos, a una compuerta AND para generar cualquier operación producto que se desee.

Las dos principales diferencias entre los dispositivos GAL y PAL son que los GAL son reprogramables y que tienen configuraciones de salida programables.

1.4.2.5 Dispositivos lógicos programables complejos CPLD (*Complex Programmable Logic Device*)

Este concepto se utiliza para definir a un PLD con un grado de integración mayor ya que permite implementar sistemas más eficientes porque utilizan menos espacio, mejoran la confiabilidad del circuito y reducen costos. Un CPLD se forma con múltiples bloques lógicos, cada uno similar a un PLD. Los bloques lógicos se comunican entre sí utilizando una matriz programable de interconexiones que proporciona un mejor desempeño.

La matriz de interconexiones programables, PIM (*Programmable Interconnect Matrix*), permite unir los pines de entrada/salida a las entradas del bloque lógico, o las salidas del bloque lógico a las entradas de otro bloque lógico, o inclusive a las entradas del mismo bloque. La mayoría de los CPLD's usan una de dos configuraciones para esta matriz: interconexión mediante arreglo o interconexión mediante multiplexores.

La primera se basa en una matriz de filas y columnas con una celda EECMOS en cada intersección. Al igual que en el GAL esta celda puede ser activada para conectar/desconectar la correspondiente fila y columna. Esta configuración permite una total interconexión entre las entradas y salidas de los bloques lógicos. Sin embargo, estas ventajas provocan que disminuya el desempeño del dispositivo además de aumentar el consumo de energía y el tamaño del componente.

En la interconexión mediante multiplexores, existe un multiplexor por cada entrada al bloque lógico. Las vías de interconexión programables son conectadas a las entradas de un número fijo de multiplexores por cada bloque lógico. Las entradas de selección de estos multiplexores son programadas para permitir que sea seleccionada únicamente una vía de la matriz de interconexiones por cada multiplexor, la cual se propaga hacia el bloque lógico.

Cabe mencionar que estos multiplexores no tienen acceso a todas las vías de la matriz por lo que el número de rutas se incrementa usando multiplexores de mayor tamaño, permitiendo así que cualquier combinación de señales de la matriz de interconexión pueda ser enlazada hacia cualquier bloque lógico. Sin embargo, el uso de grandes multiplexores incrementa el tamaño de dispositivo y reduce su desempeño.

Un bloque lógico es muy similar a un PLD, cada uno de ellos poseen generalmente una matriz de compuertas AND, una matriz de compuertas OR y una configuración para la distribución de los productos en las diferentes macroceldas del bloque.

El tamaño del bloque lógico es una medida de la capacidad del CPLD, ya que de esto depende el tamaño de la función booleana que pueda ser implementada dentro del bloque. Los bloques lógicos usualmente tienen de cuatro a veinte macroceldas. La cantidad de bloques lógicos que puede poseer un CPLD depende de la familia y fabricante del dispositivo.

1.4.2.6 Arreglo de compuertas programables en campo FPGA (*Field Programmable Gate Arrays*)

Existe una gran variedad de FPGA's que por su tipo de tecnología se pueden considerar de tres clases, FPGA's programables mediante antifusibles, FPGA's programables mediante EEPROM's y FPGA's programables mediante celdas de memoria SRAM.

La arquitectura de un FPGA consiste en arreglos de varias celdas lógicas las cuales se comunican unas con otras mediante canales de conexiones verticales y horizontales.

Cada celda lógica es funcionalmente similar a los bloques lógicos de un CPLD. La diferencia está en que un FPGA normalmente utiliza generadores de funciones en vez de compuertas. Cada uno de estos generadores es como una memoria en donde en vez de implementar la función lógica mediante compuertas, se precalcula el resultado y lo almacena en el generador.

Las entradas al generador funcionan como un bus de direcciones, y mediante las diferentes combinaciones de las entradas al generador se selecciona el resultado correcto. Esto le da una gran densidad al dispositivo ya que se maneja un gran número de generadores, pero el tiempo de propagación al implementar una función lógica en estos generadores es menor al que se necesitaría si se utilizaran compuertas.

La estructura de las celdas lógicas y las formas en que estas pueden ser interconectadas, tanto salidas como entradas de la celda, varían de acuerdo al fabricante.

En general, una celda lógica tiene menos funcionalidad que la combinación de sumas de productos y macroceldas de un CPLD, pero como cada FPGA tienen una gran cantidad de celdas lógicas es posible implementar grandes funciones utilizando varias celdas lógicas en cascada.

1.5 MICROPROCESADORES

Al microprocesador se le denomina el CPU (*Central Process Unit,* Unidad Central de Proceso) y es el cerebro de una computadora personal. Es un chip, en cuyo interior existen miles (o millones) de elementos electrónicos como los transistores, cuya combinación permite realizar el trabajo que tenga encomendado.

Los microprocesadores suelen tener la forma de un cuadrado o rectángulo negro. Están recubiertos por una carcasa de protección (o encapsulado) que rodea a la oblea de silicio en sí, para darle consistencia e impedir su deterioro (por ejemplo, por oxidación con el aire). Los conductores que sobresalen del procesador, como se puede ver en la Figura 1.9, se conectan a unas pequeñas patillas metálicas que se sueldan a las placas del circuito integrado para permitir el enlace con los conectores externos que lo acoplarán a su zócalo (*socket*), a la placa base o al circuito impreso.

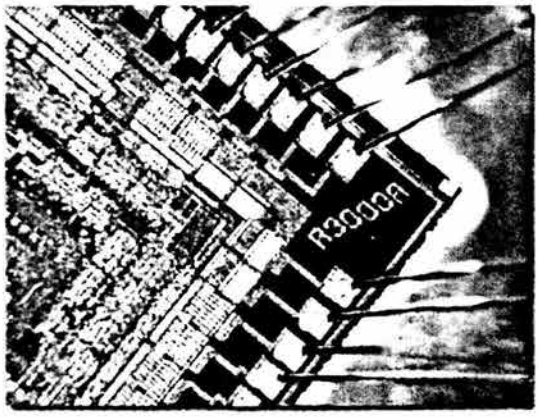


Figura 1.9 *Microprocesador*

En el chip existen millones de interruptores y circuitos que ayudan a la computadora en la toma de decisiones y en la realización de tareas. El microprocesador también se encuentra en otros dispositivos como equipo electrónico, teléfonos, automóviles, etc.

1.5.1 Partes de un microprocesador

En general, el CPU está compuesto por las siguientes partes principales:

- La Unidad Aritmético-Lógica (ALU, *Arithmetic and Logic Unit*). Es un circuito digital que efectúa y controla la velocidad de los cálculos numéricos (suma, resta) y operaciones lógicas (AND, OR y comparaciones). La magnitud de la ALU define el tamaño del microprocesador.
- Unidad de control. El propósito principal de este elemento es el de leer e interpretar las instrucciones del programa que se encuentra en la memoria; dirige la operación de los componentes internos del microprocesador, proporcionando el tiempo y la señal de control adecuada para indicar cómo se deben llevar a cabo las instrucciones. Además, permite controlar el flujo de las señales entre la memoria principal, la ALU y los dispositivos de entrada/salida.

- Registros. Son áreas de almacenamiento temporal, localizadas en la ALU, que permiten que los datos sean procesados a una velocidad más rápida que la convencional.
- Bus de control o de resultados. Selecciona la dirección de la información marcando la secuencia de los pasos a seguir para dicha transferencia.
- Bus de datos. Intercambia los datos entre las distintas partes del microprocesador de forma bidireccional.
- Bus de direcciones. Ejecuta la localización de la memoria que se requiere leer o escribir e identifica los puertos de entrada/salida.

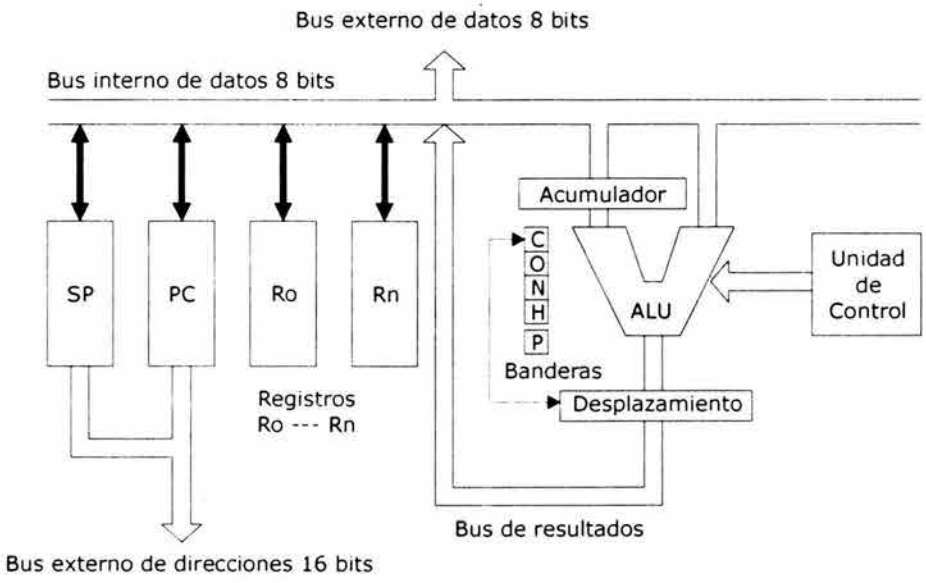


Figura 1.10 *Arquitectura básica del microprocesador*

La forma básica de operar del microprocesador en su conjunto, es direccionar una posición de la memoria en busca de una instrucción mediante el bus de direcciones, llevar la instrucción a la unidad central de proceso (CPU) por medio del bus de datos, señalando la secuencia de la transferencia por medio del bus de control.

Normalmente, a los microprocesadores se les suelen agregar dispositivos para su adecuada operación, tales como:

- Memoria caché. Es una memoria ultrarrápida que le sirve al CPU para tener inmediatamente ciertos datos que previsiblemente serán utilizados en las siguientes operaciones, sin tener que acudir a la memoria RAM, reduciendo el tiempo de espera. También se le conoce como caché de primer nivel.
- Coprocesador matemático. La FPU (*Floating Point Unit*, Unidad de Punto Flotante) es la parte del microprocesador especializada en esa clase de cálculos matemáticos; puede estar en el interior del microprocesador o en otro chip.
- Oscilador de cristal. Proporciona la señal de sincronización o señal de reloj para coordinar todas las actividades del microprocesador. La velocidad del microprocesador se mide en Megahertz (MHz). Debido a la extrema dificultad de

fabricar componentes electrónicos que funcionen a las inmensas velocidades de MHz habituales hoy en día, todos los microprocesadores modernos tienen dos velocidades:
  - Velocidad interna. La velocidad a la que funciona el microprocesador internamente.
  - Velocidad externa o de bus. La velocidad con la que se comunica el microprocesador y la placa base.
- Memoria adicional. El microprocesador no es capaz, por si solo, de albergar la cantidad de memoria necesaria para almacenar instrucciones y datos de programa. Con esta finalidad se utilizan otros circuitos integrados llamados chips de memoria.

Un microprocesador no es una computadora completa. Carece de grandes cantidades de memoria y no es capaz de comunicarse con los dispositivos de entrada/salida.

Un tipo diferente de circuito integrado llamado microcontrolador es de hecho una computadora completa situada en un único chip; contiene todos los elementos del microprocesador básico además de otras funciones especializadas.

1.5.2 Desarrollo de los microprocesadores

La tecnología de los microprocesadores y la fabricación de circuitos integrados han evolucionado vertiginosamente en últimas fechas. Existen varios factores, con los cuales se puede identificar su desarrollo:

- Arquitectura interna. Capacidad de procesamiento de la información, es decir, el movimiento de datos e instrucciones entre los registros, la unidad de control y la ALU.
- Bus de datos externos. Trayecto común a través del cual, el microprocesador envía o recibe datos y comandos de almacenamiento.
- Velocidad del reloj. Frecuencia de la ejecución de las instrucciones dentro del microprocesador, regulada por el oscilador de cristal.
- Número de transistores, tipo de tecnología, etc.

En la Tabla 1.2 se muestra una lista de la evolución de los procesadores junto con sus características principales y sistemas que los han utilizado.

Procesador	Año	Arquitectura Interna	Bus de Datos Externo	Velocidad del Reloj (MHz)	Características
Intel 4004	1971	4 bits	4 bits		- Bajo costo, velocidad lenta - Baja salida de corriente - Incompatible con TTL - 2,300 transistores (PMOS)
Intel 8008	1974	8 bits	8 bits		- Baja densidad vs. PMOS - Compatible con TTL - 3,000 transistores (NMOS)
Intel 8086	1978	16 bits	16 bits	4, 7, 8, 10	- Lenguaje Ensamblador - Protección de las bases de segmento. - 29'000 transistores (HMOS)
Intel 8088	1979	16 bits	8 bits	4, 5, 8	- Semejante al 8086, pero con un bus de 8 bits. - IBM, PC, XT
Motorola 6800	1979	16 bits	16 bits	8, 16	- Macintosh Plus, SE, Commodore Amiga
Intel 80186	1982	16 bits	16 bits	8, 10, 12.5	- Funciones de componentes externos integrados en el chip. 56,000 transistores (HMOS)

Intel 80286	1982	16 bits	16 bits	8, 10, 12.5	- Diferentes niveles de protección - Comunicación de tareas - Modo protegido o virtual - IBM, PC/AT, PS/2, Model 50/60, Compaq Deskpro 286 - 130,000 transistores (HMOS)
Motorola 68020	1984	32 bits	32 bits	16, 33	- Macintosh II
Sun Microsystems	1985	32 bits	32 bits	20, 25	- Sun Sparcstation 1, 300
Intel 80386	1985	32 bits	32 bits	16, 20, 25, 33	- Tecnología VLSI - Ampliación a 32 bits - Paginación ampliada - Gestión de direccionado integrado en el chip - Modo virtual - IBM PS/2, IBM compatibles AT - 275,000 transistores (HCMOS)
Motorola 68030	1987	32 bits	32 bits	16, 50	- Macintosh IIx series, SE/30
Intel 80486	1989	32 bits	16 bits	25, 33, 50, 66	- Memoria Caché y coprocesador matemático integrados. - Direccionamiento Tubular (*Pipeline*) - Ciclos de ráfaga (*Burst*) - Instrucciones más utilizadas ejecutadas en un ciclo de reloj - IBM PS/2, IBM compatibles - 1,200,000 transistores (HCMOS)
Motorola 68040	1989	32 bits	32 bits	25, 40	- Macintosh Cuadras
IBM Risc 6000	1990	32 bits	32 bits	25, 40	- IBM Risc/6000 Workstation
Sun Microsystems	1992	32 bits	32 bits	20, 50	- Sun Sparcstation LX
Pentium	1993	32 bits	32 bits	60, 66, 75, 90, 100, 120, 133, 150, 166	- Caché de datos y coprocesador matemático integrados - Control de errores - Ampliación de las posibilidades integradas de prueba y depuración - Unidad de punto flotante mejorada - Ejecución de dos instrucciones simultáneamente (superescalar) - Aumento de rendimiento vs. Incremento en consumo de energía - 3,100,000 transistores (BICMOS)
Pentium Pro	1995	32 bits	64 bits	100, 150, 180, 200	- Reducción en consumo de energía - Error en división con punto flotante - 5,500,000 transistores
Pentium II	1997	32 bits	64 bits	233, 266, 300, 450	- Mejoramiento para aplicaciones multimedia - Doble Bus Independiente - Ejecución Dinámica - Tecnología MMX (*MultiMedia eXtensions*) - 7,500,000 transistores(CMOS-silicio)
Pentium Celeron	1998	32 bits	64 bits	500, 600, 700, 850, 1000, 900, 950, 1100, 1200, 1400, 1700, 1800, 2000, 2300, 2400	- Optimización de acceso y ejecución de datos e instrucciones - Bajo costo - 19,000,000 de transistores
Pentium III	1999	32 bits	64 bits	500, 600, 733, 800, 866, 933, 1000, 1130, 1200, 1400	- Desarrollo de aplicaciones en Internet - 28,100,000 transistores

Pentium 4	2000	32 bits	64 bits	1700, 2400, 2660, 2800, 3060, 3200	- Mejora de rendimiento y flexibilidad en entornos multitarea - Máximo rendimiento en multimedia - 55,000,000 de transistores
Pentium Itanium	2001	64 bits	64 bits	1300, 1400, 1500	- Recursos de cálculo masivo - Capacidad de ejecución de múltiples instrucciones simultáneamente - Incremento de seguridad en Comercio Electrónico e Internet - 120,000,000 de transistores

Tabla 1.2. *Evolución de los microprocesadores*

La ITRS (*International Technology Roadmap for Semiconductors*) estima que para el año 2011 se integrarán más de un billón de transistores en un mismo circuito. Se considera que el factor limitante en la velocidad de los microprocesadores acabará siendo el comportamiento de los propios electrones al circular por los transistores. Cuando las dimensiones se hacen muy pequeñas, los efectos cuánticos debidos a la naturaleza ondulatoria de los electrones podrían dominar el comportamiento de los transistores y circuitos. Puede que sean necesarios nuevos dispositivos y diseños de circuitos a medida que los microprocesadores se aproximen a dimensiones atómicas. Para producir las generaciones futuras de microchips se necesitaran técnicas como la epitaxial por haz molecular, en la que los semiconductores se depositan átomo por átomo en una cámara de vacío ultra elevado, o la microscopía de barrido de efecto de túnel, que permite ver incluso el desplazamiento de átomos individuales con precisión.

Por último, es importante mencionar que el desarrollo de la microelectrónica hizo posible la incorporación de microprocesadores en las tarjetas inteligentes, por lo que además de la capacidad de almacenamiento se agregó el procesamiento de la información contenida. Uno de los logros más importantes con esta mejora fue la posibilidad de implementar en la propia tarjeta algoritmos de encriptación de datos, lo cual será ampliamente tratado en los siguientes capítulos.

Tarjetas Inteligentes

- Tarjeta de Banda Magnética
- Tarjeta Inteligente
- Desarrollo Histórico
- Tipos de Tarjetas Inteligentes
- Tipos de Interfaz
- Ciclo de Vida
- Fabricantes
- Estándares
- Aplicaciones
- Evolución del Mercado
- Costo de una Tarjeta Inteligente

Capítulo 2

CAPÍTULO 2. TARJETAS INTELIGENTES

2.1 TARJETA DE BANDA MAGNÉTICA

La tarjeta magnética es uno de los medios más utilizados en operaciones financieras, como tarjetas de crédito y de acceso a cajeros, y en aplicaciones donde se requiere una tarjeta de bajo costo no reutilizable, por ejemplo, en acceso a espectáculos, estacionamientos, medios de transporte, etc.

Los datos son almacenados en la banda magnética, la cual está separada 5.54 mm del borde superior y tiene un ancho de 10.28 mm. Ésta se encuentra dividida en tres sub-bandas de un ancho de 2.54 mm, separadas entre sí por 0.76 mm, como se puede apreciar en la Figura 2.1.

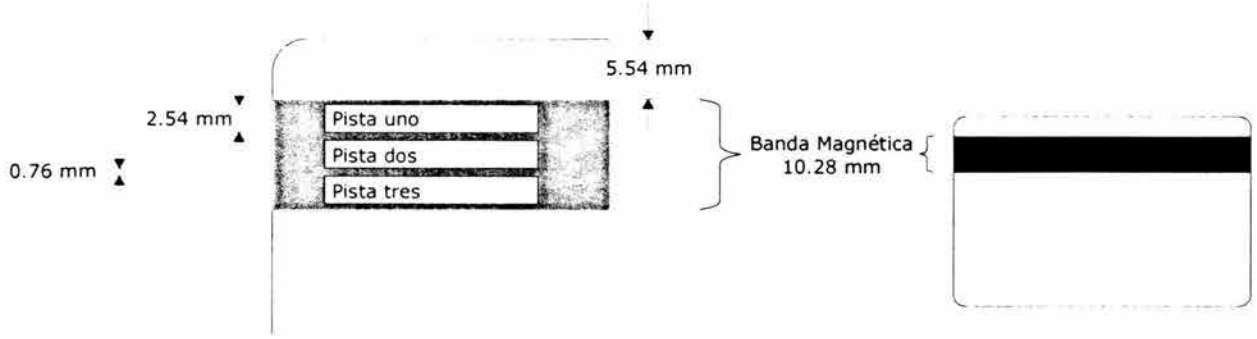


Figura 2.1 *Sub-bandas de una tarjeta magnética*

La primera sub-banda, que es la más cercana al borde, tiene una capacidad de 210 bpi (bits por pulgada) y puede almacenar hasta 79 caracteres. Los primeros 18 se usan para almacenar el número de cuenta o identificación, los siguientes 26 codifican el nombre del propietario y el resto se emplea para datos adicionales tales como fecha de expedición, restricciones, tipo de tarjeta, etc. Esta sub-banda suele utilizarse en operaciones como el registro de la entrada y salida de un empleado.

La segunda sub-banda tiene una capacidad de 75 bpi, con lo que puede almacenar hasta 40 caracteres. Los primeros 19 se usan para almacenar el número de cuenta y el resto para datos adicionales. Esta sub-banda tiene aplicaciones en campos tales como las transacciones financieras de modo en línea.

La tercera sub-banda también se utiliza para transacciones de carácter financiero, aunque ésta suele incorporar mecanismos de seguridad. La información como número de cuenta, identidad del usuario, unidad monetaria, cantidad máxima que se puede retirar, etc., es encriptada junto con un número de identificación personal o PIN (*Personal Identification Number*) que se le pide al usuario en las operaciones que realiza. La última banda contiene un máximo de 107 caracteres, teniendo una capacidad de 210 bpi y es la única que puede ser alterada cada vez que se usa la tarjeta.

El procedimiento para almacenar datos en la banda magnética es análogo al usado con las cintas de audio. Consiste en esparcir sobre un soporte una serie de partículas que se pueden polarizar y que mantienen la polaridad con el tiempo. Al aplicar un campo magnético a lo largo del soporte se pueden polarizar las partículas en una dirección u otra. Esto se consigue, por ejemplo, pasando un inductor sobre la cinta al mismo tiempo que se cambia el sentido de la corriente, dependiendo si es un bit cero o uno. El proceso de lectura se realiza colocando una bobina sobre la cinta, con lo que se consiguen pequeñas corrientes que indican la presencia de un cero o uno almacenado.

Las garantías de seguridad que ofrecen las tarjetas magnéticas dependen en gran medida del PIN del usuario. Aunque, el punto más débil de este sistema se presenta cuando el propietario utiliza un lector no confiable o que es distinto al de su compañía. Si esto sucede, se puede obtener el contenido de la banda magnética, al igual que el PIN, y con dicha información se podrá realizar una copia exacta para utilizarla indebidamente.

Muchos cambios tecnológicos han marcado el desarrollo de las tarjetas usadas en general como medio de identificación. Las primeras tarjetas que almacenaron datos accesibles fueron las de banda magnética, las cuales han sido ampliamente utilizadas hasta la aparición de las tarjetas con electrónica integrada o tarjetas inteligentes.

2.2 TARJETA INTELIGENTE

Es una tarjeta plástica del tamaño de una tarjeta de crédito que cuenta con un circuito integrado incrustado que la hace inteligente. El circuito integrado le da la habilidad para realizar algoritmos y toma de decisiones, también es capaz de almacenar información y cuenta con mecanismos de seguridad extremadamente efectivos; incluso una sola tarjeta puede tener diferentes aplicaciones con un código de acceso diferente para cada una de ellas. En la Figura 2.2 se muestran los principales componentes para un tipo de tarjeta inteligente.

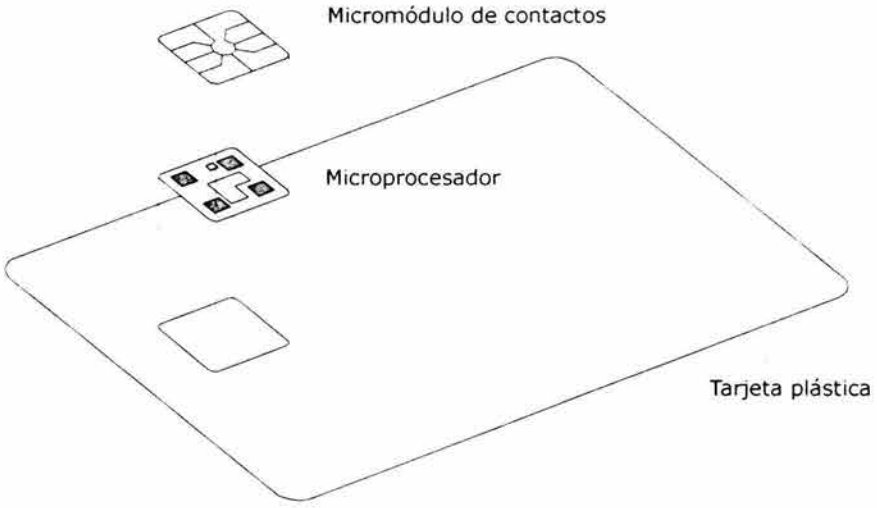


Figura 2.2 *Componentes de una Tarjeta Inteligente*

Las Tarjetas Inteligentes (TI's) son de alguna manera la evolución de las tarjetas de banda magnética y de código de barras y, a diferencia de éstas, el hecho de contar con un microprocesador las hace mucho más versátiles y les confiere una capacidad de procesamiento que anteriormente no existía. A continuación, en la Tabla 2.1 se tiene un cuadro comparativo entre las tarjetas inteligentes y magnéticas.

Tarjetas inteligentes	Tarjetas magnéticas
Gran capacidad de almacenamiento	Baja capacidad de almacenamiento
Seguridad de datos mediante encriptación, parámetros biométricos y/o PIN	Los datos almacenados pueden cambiarse y/o duplicarse con relativa facilidad
Aplicaciones diversas en una misma tarjeta	Diseñadas para funciones simples y repetitivas
Procesamiento on-line y off-line	Modo de operación on-line
Almacenamiento permanente de datos en memorias no-volátiles	La banda magnética puede perder magnetismo con el uso
Construcción resistente al uso	Proclive al desgaste

Tabla 2.1 *Comparación entre tarjetas inteligentes y magnéticas*

2.2.1 Ventajas

Algunas de las ventajas de las tarjetas inteligentes son:

- Capacidad de procesamiento de información en modo fuera de línea (*off-line*).
- Seguridad de datos a través de mecanismos de encriptación.
- Posibilidad de ser reprogramadas.
- Posibilidad de uso de la misma tarjeta en diferentes aplicaciones.
- Portátil y móvil: identifica al usuario.

Las tarjetas inteligentes juegan un papel creciente como dispositivos de seguridad activos. Debido a su microprocesador, pueden proveer necesidades específicas para el ambiente en el que se estén usando. Ofrecen señales seguras mediante las que un usuario puede ser identificado y autenticar un sistema de cómputo o una red de comunicación y viceversa. Permiten el manejo seguro y el almacenamiento de datos importantes como privilegios de usuario y claves encriptadas, así como el cifrado de datos.

Comparadas con los dispositivos convencionales de transmisión de datos, las TI's ofrecen mayor seguridad así como beneficios económicos y de conveniencia. Por ejemplo, mediante encriptación, el contenido y los datos pueden ser transferidos de forma segura a través de una red cableada o inalámbrica e inclusive pueden ser acoplados con métodos de autenticación biométrica, los cuales dependen de atributos físicos personales.

En adición, los sistemas basados en tarjetas inteligentes se configuran fácilmente de acuerdo con finalidades particulares. La multifuncionalidad como pago, aplicaciones y dispositivos en red, colocan a las TI's como la interfaz de usuario ideal.

2.3 DESARROLLO HISTÓRICO

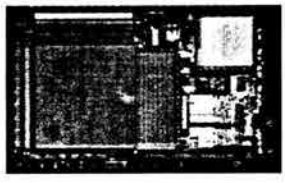
La industria de las TI's ha evolucionado en las últimas tres décadas. Se pueden mencionar desde 1968, cuando los inventores alemanes Jürgen Dethloff y Helmunt Grötrupp utilizaron un microprocesador montado en una tarjeta de plástico en uno de sus diseños. Dos años

más tarde, en 1970, Kunitaka Aritmura desarrolló una aplicación similar. La primera versión formal de la tarjeta inteligente se originó en 1974, cuando Rolando Moreno creó Innovatron y registró la primera de sus múltiples patentes en el campo de los sistemas de tarjetas de circuito integrado.

El principal desarrollo de las tarjetas inteligentes se vio favorecido en Europa a mediados de los años 70, cuando el gobierno y el banco francés Carte Bancaire, impulsados por el creciente número de fraudes a través de la falsificación de las tarjetas de crédito de banda magnética, se reúnen con la empresa Bull para encontrar la forma de reducir el desfalco en el sistema bancario. Surge entonces la idea de usar una tarjeta de crédito con un microprocesador que pudiera controlar el acceso a la información y reducir la falsificación de las mismas.

Las TI's pasaron por un periodo de desarrollo entre 1977 y 1988. La primera tarjeta estuvo disponible el 21 de marzo de 1979, surgida de los esfuerzos realizados en conjunto entre Bull, Honeywell y Motorola; ésta incluía dos circuitos integrados: un procesador de 8 bits 3870 y una memoria 2716, lo que permitió que fuera más flexible (ver Figura 2.3.a). Esta implementación constituyó una buena herramienta para realizar pruebas, pero sobre todo, fue importante para convencer a los encargados de tomar decisiones estratégicas de que era una tecnología redituable y con futuro prominente. Para 1981, Motorola introdujo la tarjeta con un sólo chip integrado programable (Figura 2.3.b), conocido como el SPOM (*Single Programmable One Chip Microcomputer*).

(a)



(b)

Figura 2.3 *Primeras tarjetas inteligentes*

Debido al vandalismo, la primera aplicación comercial fue desarrollada en 1983 para la compañía France's Public Telephone and Telegraph System, quien comenzó la sustitución de los teléfonos públicos de monedas para implementar un nuevo sistema de pago mediante tarjetas electrónicas llamadas Telecarte (ver Figura 2.4) en la ciudad de Velizy, cercana a París. Esta tarjeta podía ser insertada dentro del lector del teléfono para activar la llamada y descontar su costo.

Figura 2.4 *Primera tarjeta telefónica electrónica (Telecarte)*

Entre 1982 y 1984, los bancos franceses realizaron tres experimentos con el objeto de evaluar la viabilidad económica y la factibilidad técnica de tres tipos de tarjetas, en tres ciudades diferentes: Blois, Lyón y Caen. Este experimento fue llamado "IPSO" y en él se utilizaron 125,000 tarjetas y 750 terminales. La compañía Schlumberger proveyó las tarjetas empleadas en la ciudad de Lyón; Philips suministró las usadas en Caen y el grupo CII-Honeywell-Bull hizo lo propio en la ciudad de Blois, con tarjetas equipadas con el procesador CP8 de Bull.

Finalmente, sólo las pruebas efectuadas en Blois fueron exitosas y por lo tanto los bancos eligieron las tarjetas con procesador Bull CP8, que se generalizaron en toda Francia a partir de 1986, como se muestra en la Figura 2.5. Este componente fue por muchos años utilizado principalmente por el sistema bancario francés; éste contenía información de la cuenta, el número de identificación personal y un registro de transacciones financieras que podía ser usado para indagar actividades dudosas.

Figura 2.5 *Primera tarjeta bancaria con microprocesador (Carte Bancaire)*

Para 1989, las TI's comenzaron a ser una herramienta conocida y viable en Europa, especialmente en el mercado de Francia. En ese mismo año, Bull inicia el desarrollo de esta tecnología fuera del sistema bancario francés.

Durante los años 90's, las tarjetas inteligentes fueron incorporadas dentro de una gran variedad de aplicaciones. Por ejemplo, fueron empleadas para restablecer la seguridad en los sistemas de televisión de paga mediante la inserción de una tarjeta en el codificador.

La aplicación original en el sistema bancario de Francia fue implementada totalmente en 1993, cuando todas las tarjetas bancarias fueron convertidas a tarjetas inteligentes.

En 1992, Visa International Service Association se interesó en promover la tecnología de TI's y comenzó a desarrollar una infraestructura para soportar estas tarjetas en la industria de las compras. Anticipando sus potencialidades, formó un consorcio junto con Europay International S.A. y MasterCard International Incorporated (las dos más grandes organizaciones de pago) que se llamó EMV, tomando las tres letras iniciales de los participantes.

Este consorcio se estableció con la finalidad de crear las especificaciones para las transacciones financieras que permitirían estandarizar las tarjetas inteligentes y los lectores, garantizando así la universalidad de su uso, independientemente del fabricante o del emisor de la tarjeta. Para el año de 1996 se publicó la primera versión del documento con las especificaciones EMV.

El National Westmisnter Bank junto con el Midland Bank y British Telecommunications, en 1995, desarrollaron un sistema de pago llamado Mondex que reemplaza el efectivo por tarjetas (monedero electrónico), el cual soporta hasta cinco diferentes tipos de monedas y permite adicionalmente realizar llamadas telefónicas. Los usuarios pueden transferir dinero de su cuenta bancaria a la tarjeta desde un teléfono público que tenga el símbolo Mondex. También, mediante un equipo especial se puede transferir efectivo de una tarjeta a otra.

En los juegos Olímpicos de Atlanta 96, el First Union Bank y Nations Bank junto con Visa Cash diseñaron, mediante el uso de TI's, un programa para el control de acceso a los estadios y el pago de telefonía, transporte público, taxis, restaurantes, tiendas y máquinas expendedoras con un excelente resultado.

El PC/SC Workgroup fue establecido en Mayo de 1996, con la finalidad de definir las especificaciones para el uso de tarjetas inteligentes y lectores en la plataforma de computadoras personales (PC's). El resultado de las especificaciones finales, fue anunciado en Abril de 1998.

Hoy en día, toda la tecnología de telefonía móvil digital que cumple con el estándar GSM (*Global System for Mobile communications*), contiene una tarjeta inteligente SIM (*Subscriber Identification Module*) que identifica al usuario responsable del pago de las llamadas. GSM es ampliamente utilizado en distintas regiones a nivel mundial.

2.4 TIPOS DE TARJETAS INTELIGENTES

Las tarjetas inteligentes más utilizadas están disponibles en dos tipos; la diferencia se encuentra en que pueden tener o carecer de un microprocesador (CPU). Las tarjetas sin CPU son llamadas tarjetas de memoria y las que lo tienen se conocen como tarjetas con microprocesador. Cada tipo de tarjeta, con sus propias características, costos, operaciones y funcionalidad, tiene aplicaciones en particular dentro de algún segmento en el mercado.

2.4.1 Tarjetas de memoria

Cualquier tarjeta con un circuito integrado de almacenamiento de memoria, se puede considerar como inteligente. Generalmente, se puede leer todo el contenido de la memoria aunque existe un área reservada por el fabricante que no puede modificarse.

También, se elaboran algunas más sofisticadas que cuentan con una clave de acceso para permitir la lectura de información, sin embargo, contienen datos confidenciales en un área protegida.

Las tarjetas de memoria pueden tener miles de veces más información que una tarjeta de banda magnética. Los datos que se requieren para las aplicaciones son almacenados en una memoria EEPROM, la cual tiene una capacidad desde cientos de bytes hasta alrededor de 8 KB.

El acceso de los datos es manejado por un módulo de seguridad del circuito integrado que permite la lectura y, en algunos otros casos, la escritura (o actualización) de datos; en la Figura 2.6 se muestran sus elementos.

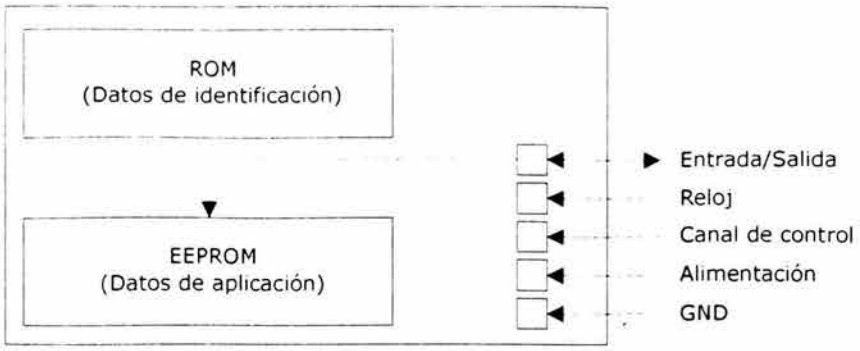


Figura 2.6 *Esquema de bloques para una tarjeta de memoria*

Las funciones que desempeñan las tarjetas de memoria están optimizadas para operaciones particulares en las que no se requieren complejos mecanismos de seguridad. Una aplicación típica son las tarjetas de pago telefónicas, en las cuales, la deducción del costo de las llamadas es realizada por medio del circuito integrado.

Este tipo de tarjetas no puede ser recargada ya que para hacerlo es necesario borrar su contenido con rayos ultravioleta. Además, las tarjetas telefónicas están recubiertas con una resina opaca que protege al circuito integrado de los rayos UV; por otra parte, sería necesario reprogramar el área del fabricante que está protegida contra escritura por un fusible que es fundido después de programar la tarjeta durante el proceso de manufactura. Por último, su simplicidad permite que estas tarjetas y los lectores de las mismas sean producidos a un bajo costo.

2.4.2 Tarjetas con microprocesador

Las tarjetas con microprocesador pueden operar como un dispositivo procesador con múltiples funciones como las de lectura/escritura, encriptación, mecanismos de seguridad avanzados, procesamiento local de información, cálculos complejos y otros procedimientos interactivos. Estas tarjetas, además del microprocesador, cuentan con algunos elementos adicionales como son, una ROM, una EEPROM, una RAM y un puerto de entrada/salida, como se indica en la Figura 2.7.

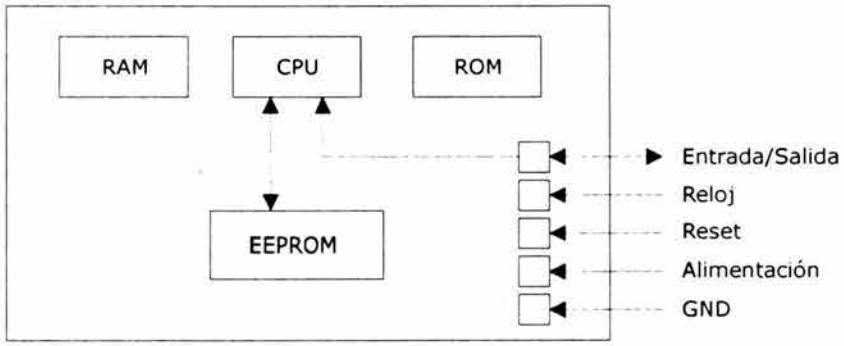


Figura 2.7 *Arquitectura de una tarjeta con microprocesador*

La ROM contiene el sistema operativo con las instrucciones básicas de la tarjeta y se graba durante el proceso de fabricación. La EEPROM es la memoria no-volátil del microprocesador y en ella se encuentran los datos del usuario o de la aplicación, así como el código del programa que está bajo el control del sistema operativo.

La RAM es la memoria de trabajo del microprocesador, que al ser volátil toda la información se pierde al desconectar la tarjeta de la terminal. El puerto de entrada/salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit.

2.4.3 Super Smart Cards

Estas tarjetas cuentan con un teclado integrado, una pantalla LCD (*Liquid Cristal Display*, pantalla de cristal líquido), y una batería o celda solar para proporcionar una propia alimentación, como se observa en la Figura 2.8. En contraparte, debido a su complejidad y alto costo, este tipo de tecnología aún se encuentra bajo desarrollo.

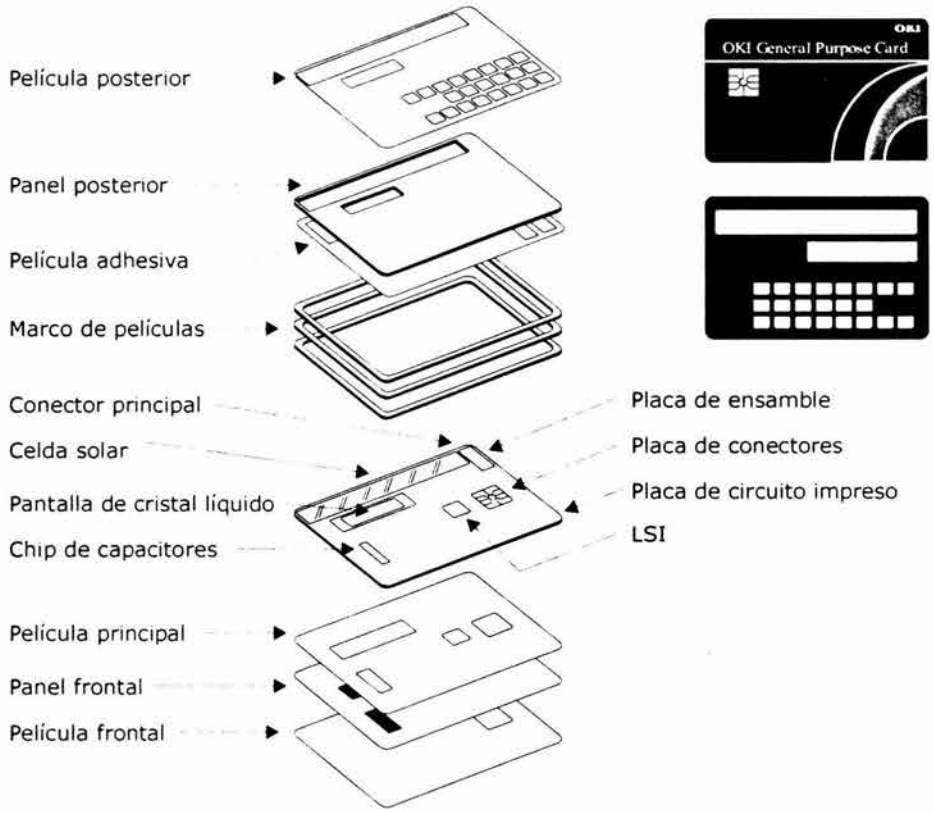


Figura 2.8 *Esquema de una Super Smart Card*

2.5 TIPOS DE INTERFAZ

Las tarjetas inteligentes están disponibles como tarjetas con contactos y sin contactos. Como su nombre lo indica, la principal diferencia está en la transferencia de la información o

aplicación residente con el dispositivo de lectura. Las tarjetas de contactos requieren su inserción dentro de un lector. Las tarjetas sin contactos necesitan una proximidad cercana a un dispositivo receptor, en el cual no hay inserción.

2.5.1 Tarjetas con contactos (*Contact Cards*)

Este tipo de tarjetas tienen en su superficie unos contactos que permiten la comunicación de la propia tarjeta con los dispositivos lectores (ver Figura 2.9), esto con la finalidad de proporcionar la alimentación y la señal de reloj para la operación del chip.

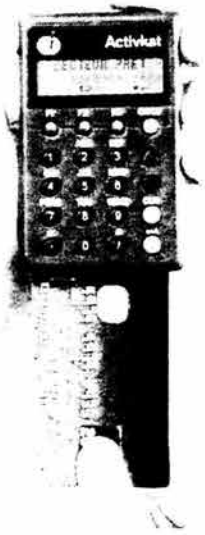


Figura 2.9 *Tarjeta y lector con contactos*

2.5.2 Tarjetas sin contactos (*Contactless Cards*)

Las tarjetas sin contactos fueron desarrolladas por primera vez en el Instituto Arimura en 1978. Por medio de un acoplamiento capacitivo e inductivo se transfiere energía y potencia a la tarjeta y su información es accedida por medio de radiofrecuencias con el dispositivo de lectura, un ejemplo de este tipo de tarjeta y su terminal se muestra en la Figura 2.10.

La alimentación se suministra mediante una batería que se encuentra al lado del chip o un hilo metálico incrustado que se somete a un campo electromagnético variable que a su vez induce una corriente eléctrica.

La ventaja de este tipo de tarjeta es su mayor durabilidad, que la hace ideal en las aplicaciones de uso intensivo.

Por ejemplo, en sistemas de control de acceso o identificación muy transitados, ahorra el tiempo que se necesita para insertar la tarjeta en el lector; además, evita fallas de funcionamiento, debido al deterioro en la superficie de los contactos o a la suciedad adherida en ambos dispositivos.

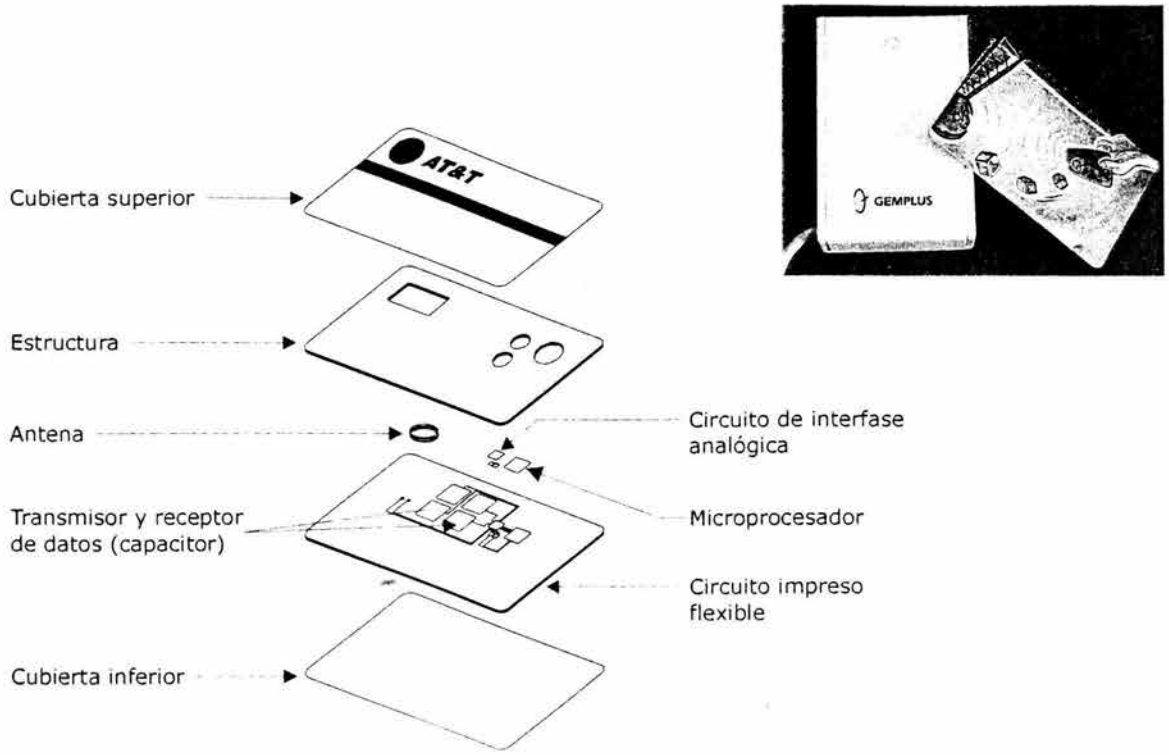


Figura 2.10 *Tarjeta y lector sin contactos*

En la Tabla 2.2 se realiza una comparación entre las diferentes tarjetas, asimismo se muestra un costo aproximado que existe para cada una de ellas.

Característica	Magnética	Con contactos	Sin contactos
Almacenamiento de datos	Bajo	Bajo a alto	Bajo a alto
Multifunciones	No	Si	Si
Seguridad	Baja	Media a alta	Media a Alta
Confiablidad	Media	Buena	En progreso
Estándares	Completo	En desarrollo	Emergente
Costo (USD)	0.1	0.5 a 15	2 a 15

Tabla 2.2 *Características de la tecnología de las tarjetas*

2.5.3 Tarjetas híbridas (*Hybrid Cards*)

En las tarjetas híbridas se combinan la tarjeta electrónica junto con la de banda magnética. De igual forma, el término híbrido se refiere a las tarjetas que tienen ambas interfaces. La interfaz con contactos es usada por un chip microprocesador y la sin contactos es utilizada por un chip de memoria.

2.6 CICLO DE VIDA

El ciclo de vida de una TI comprende muchos procesos, los cuales comienzan por la especificación de los requerimientos de la aplicación hasta el fin de vida de la tarjeta cuando ésta es deshabilitada, todo esto cumpliendo con las especificaciones establecidas por los estándares internacionales. Estos procesos, que se enumeran en la Figura 2.11, se pueden dividir en cinco fases principales: fabricación, pre-personalización, personalización, utilización y de invalidación; estas fases se describen a continuación.

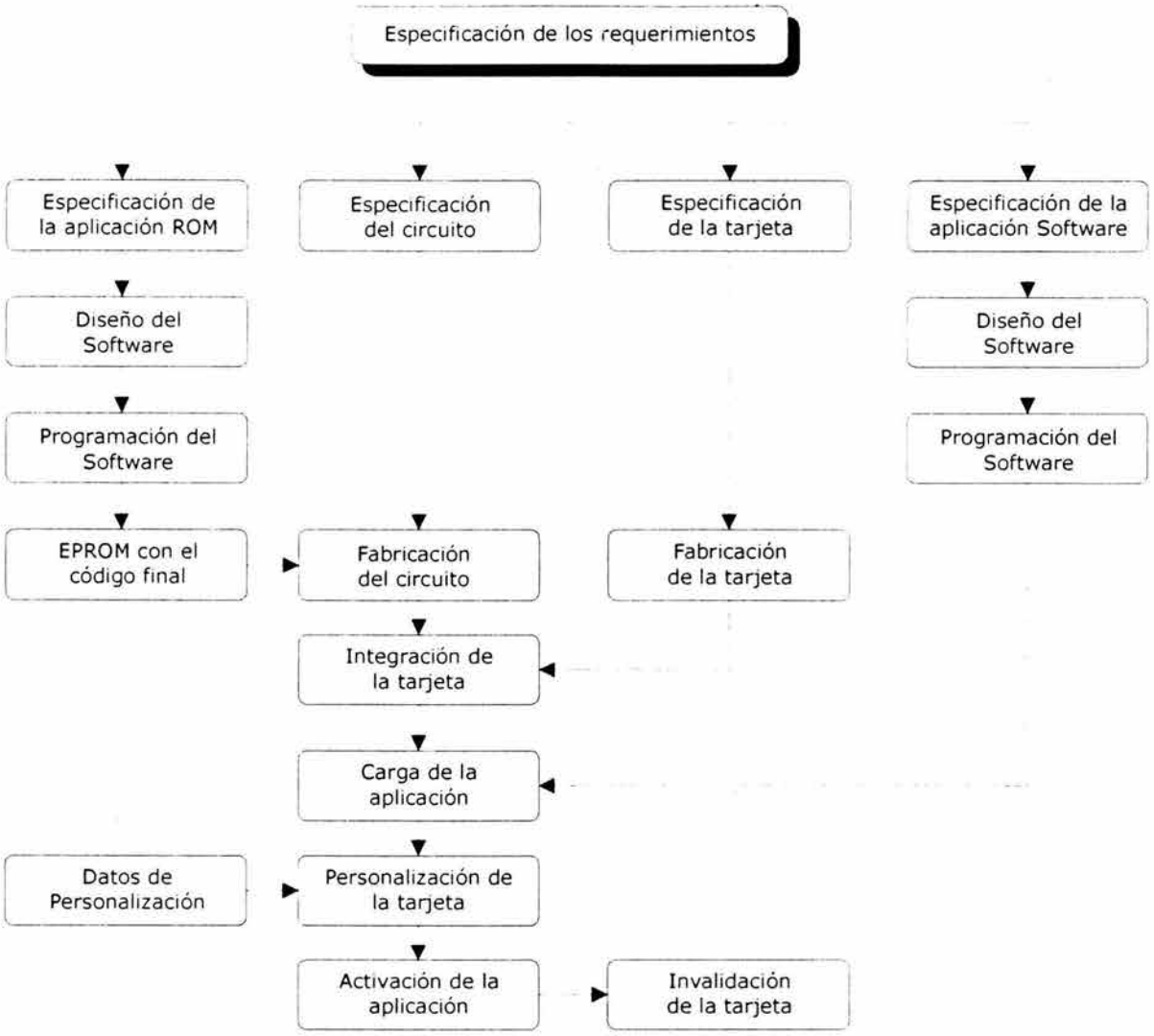


Figura 2.11 *Ciclo de vida de la tarjeta inteligente*

2.6.1 Especificación de los requerimientos

El proceso comienza con la especificación de los requerimientos necesarios para la tarjeta, tipo de integrado, memoria, ROM Mask, tarjeta, software, etc., y suele finalizar con la impresión de los datos del emisor y del usuario. Luego de esta etapa, la tarjeta estará lista

para recibir el software, que se alojará en la memoria y que dependerá de la aplicación a la que se destinará.

2.6.1.1 Circuito integrado

Considerando una TI con un procesador incorporado, aunque en muchos casos sólo se integra un chip de memoria, los principales parámetros que se deben definir son:

- Tipo de microcontrolador.
- Tipo de memoria no-volátil (EPROM, EEPROM).
- Tamaño de ROM o PROM.
- Tamaño de RAM.
- Tamaño de memoria no-volátil.
- Velocidad de reloj (externo o interno).
- Características eléctricas (voltaje de alimentación, consumo de corriente).
- Parámetros de comunicación (síncrona, asíncrona).
- Mecanismo de reinicio.
- Modo de reposo (operación en *stand-by*).
- Coprocesador (por ejemplo, para algoritmos de encriptación).

En general, los fabricantes cuentan con una gran variedad de productos para los cuales muchos de los parámetros mencionados están predefinidos, como se observa en la Tabla 2.3, por lo que el diseñador sólo debe elegir el modelo adecuado para la aplicación.

Fabricante	Producto	Memoria			Voltaje (V)	Frecuencia (MHz)
		EEPROM (Kbytes)	ROM (Kbytes)	RAM (Kbytes)		
Hitachi	AE43C	8	64	2	3 - 5	1 - 8
	AE45C	32	96	4	3 - 5	1 - 8
Philips	P8WE5033	32	96	2	2.7 - 5.5	1 - 8
	P8WE6008	8	32	1	2.7 - 5.5	1 - 8
	P8WE6033	32	96	2	2.7 - 5.5	1 - 8

Tabla 2.3 *Ejemplos de productos de circuitos integrados*

2.6.1.2 Tarjeta

En este punto deben definirse las siguientes características para la propia tarjeta:

- Dimensiones.
- Ubicación del integrado.
- Material.
- Requerimientos de impresión.
- Banda magnética (opcional).
- Lugar para la firma del poseedor (opcional).
- Holograma o foto (opcional).
- Impresión en sobre relieve (opcional).
- Parámetros ambientales.

El tamaño físico de una tarjeta inteligente se denomina ID1 y está descrito por la norma ISO 7816/1 (ver Tabla 2.4), las dimensiones son 85.6 mm X 54 mm con esquinas redondeadas de 3.18 mm de radio con un grosor de 0.76 mm (Figura 2.12).

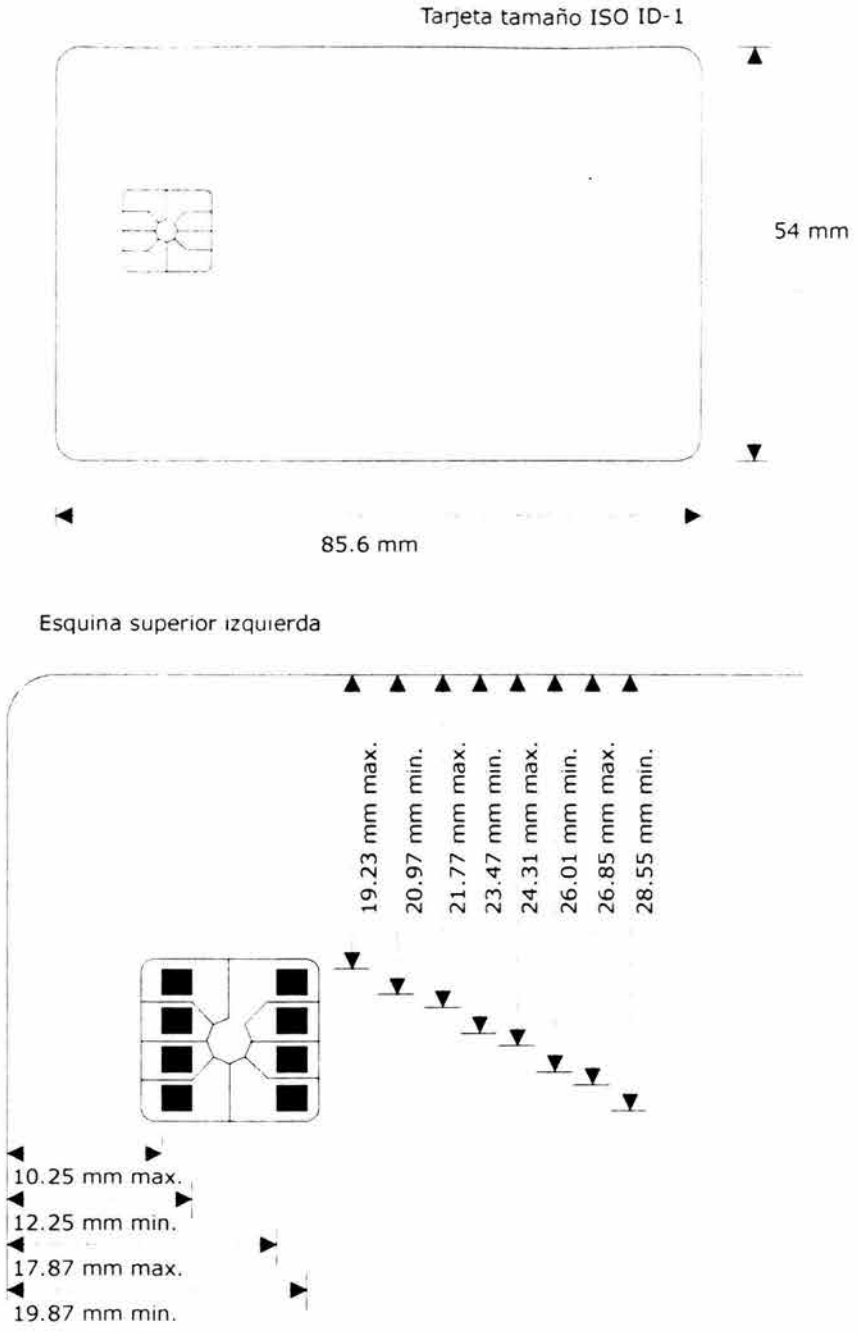


Figura 2.12 *Dimensiones de la tarjeta inteligente y posición de los contactos*

También en esta norma se definen la ubicación, la cantidad y el tamaño de los contactos del circuito integrado. Especifica, por ejemplo, que se localice en la parte superior de la tarjeta al lado opuesto de la banda magnética para lograr mayor resistencia a la torsión. Se indica

igualmente la robustez mecánica y la resistencia que debe tener a la radiación ultravioleta, rayos X, temperatura y descargas electromagnéticas.

Estándar	Aspectos
ISO 7816/1 Características físicas	- Luz ultravioleta, rayos X. - Perfil de los contactos de la superficie. - Fuerza mecánica de la tarjeta y el contacto. - Resistencia eléctrica. - Radiación electromagnética. - Electricidad estática. - Robustez mecánica.
ISO 7816/2 Dimensión y localización de los contactos	- Tamaño. - Localización. - Asignación. - Ubicación.
ISO 7816/3 Señales eléctricas y protocolos de transmisión	- Descripción de las señales eléctricas. - Valores de voltaje y corriente. - Protocolos de transmisión. - Respuesta a Reinicio.

Tabla 2.4 *ISO 7816. Estándar para tarjetas de circuitos integrados con contactos*

La mayoría de las tarjetas inteligentes tienen ocho contactos en la cara frontal, sin embargo dos de ellos están reservados para su uso en el futuro, por lo que algunos fabricantes producen tarjetas sólo con seis contactos, lo cual reduce ligeramente los costos de producción. Los contactos eléctricos se numeran, de acuerdo con la norma ISO 7816/2, de C1 a C8 del superior izquierdo al inferior derecho (Figura 2.13).

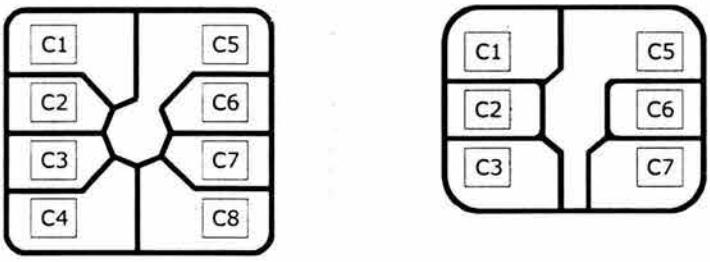


Figura 2.13 *Configuración de los contactos*

La función de los contactos se define en la Tabla 2.5. Es importante mencionar que el contacto VPP fue utilizado hace algunos años para la programación y borrado de la EEPROM, sin embargo, con el desarrollo de circuitos con alimentación propia este contacto es raramente utilizado.

La fuente de voltaje VCC está especificada a 5 V ± 10% pero la industria está tratando de establecer un estándar de soporte de 3 Volts ya que todos los componentes de la telefonía móvil están disponibles en configuraciones de 3 V y las tarjetas inteligentes son el único remanente que requiere que un teléfono móvil tenga un convertidor de carga. Es posible fabricar tarjetas que utilicen 3 V, pero no serían compatibles con los sistemas actuales de 5 Volts.

Posición	Abreviación	Función
C1	VCC	Voltaje de alimentación
C2	RST	Reset de la tarjeta
C3	CLK	Frecuencia de Reloj
C4	RFU	Reservado para uso futuro
C5	GND	Tierra
C6	VPP	Voltaje para programación de la memoria
C7	I/O	Comunicación Serial Entrada/Salida
C8	RFU	Reservado para uso futuro

Tabla 2.5 *Función de los contactos*

2.6.1.3 Memorias ROM/PROM/EPROM

La memoria contiene el sistema operativo de la tarjeta, por lo que se relaciona tanto a las tareas de la comunicación de datos como, eventualmente, al manejo de algoritmos de encriptación.

La memoria ROM sólo puede ser grabada durante el proceso de fabricación, y tiene como ventajas su bajo costo y el pequeño espacio de integración. Obviamente, una vez fabricada no es posible utilizar la tarjeta para otra aplicación diferente a la que se pensó en el diseño, ya que el contenido de la ROM no puede modificarse.

En lugar de las memorias ROM's, pueden emplearse memorias PROM's, que permiten definir la aplicación luego de la fabricación del integrado ya que pueden ser grabadas posteriormente, aunque sólo una vez. Una de las desventajas es que la grabación requiere quemar fusibles, con voltajes más elevados que el que usa frecuentemente la tarjeta.

Debido a esta limitación, las memorias PROM's son actualmente reemplazadas por memorias tipo EPROM's. Estas memorias pueden borrarse con luz ultravioleta, aunque, como la tarjeta carece de la ventana necesaria, en definitiva se utilizan como memorias de sólo escritura OTP (*One Time PROM*). La ventaja es que las EPROM's pueden ser escritas con los voltajes de trabajo de la tarjeta.

La memoria EEPROM puede ser escrita y borrada eléctricamente, es la memoria elegida para el almacenamiento de datos que no deben perderse al desconectar la tarjeta de la terminal. Al igual que las memorias EPROM's, frecuentemente utilizadas para almacenar la aplicación, las EEPROM's no necesitan de voltajes elevados para ser reprogramadas y normalmente pueden ser re-escritas hasta 1,000,000 de veces.

2.6.1.4 Software de aplicación

Dentro del proceso completo del desarrollo de una tarjeta, ésta es la parte relacionada específicamente con la aplicación particular para la que se utilizará. El software podría implementarse dentro de la ROM o PROM, aunque actualmente se tiende a implementar memorias EPROM's en las tarjetas.

El hecho de usar memorias EPROM's permite una mayor flexibilidad ya que la aplicación puede grabarse en las tarjetas luego de su fabricación, o incluso modificarse en caso de que se use memoria que se pueda borrar eléctricamente (EEPROM).

2.6.2 Fabricación del circuito integrado

La manufactura de las tarjetas inteligentes involucra numerosos pasos, desde las especificaciones iniciales de la tarjeta misma y el integrado, pasando obviamente por la implementación del chip sobre la tarjeta, este último proceso es clave para la obtención de un producto de calidad.

Varios cientos de circuitos integrados son manufacturados a la vez en forma de obleas de silicio, como se muestra en la Figura 2.14. Un circuito integrado para una tarjeta inteligente mide aproximadamente 25 mm^2 (5 mm por lado).

El formato para la circuitería en un integrado es repetido cientos de veces en una oblea de 10.16 cm (4 pulgadas) de diámetro aproximadamente y cuando está completada puede contener entre doscientos y trescientos circuitos integrados individuales.

La fabricación actual de integrados en la oblea es realizada a través de procesos altamente refinados de depósito al vacío de material semiconductor extremadamente puro sobre el sustrato de silicio.

Figura 2.14 *Oblea de silicio*

Una vez que la oblea es completada, cada circuito individual debe ser probado para asegurar que es funcional.

Cada circuito que pasa esta prueba es marcado físicamente en preparación para el corte de la oblea en cientos de piezas, este proceso de corte puede hacerse escribiendo una marca con un diamante y después ejerciendo presión con unos rodillos para que la oblea se fracture sobre las marcas de corte.

Una vez que los circuitos han sido segmentados, es adherido un conector eléctrico un poco más grande que el circuito. Los conectores eléctricos (cables muy delgados de 25 µm.) de oro o aluminio, conectan varias áreas de este conector con pines específicos del mismo circuito. La configuración resultante es llamada normalmente módulo (ver Figura 2.15).

Figura 2.15 *Inserción de conexiones al módulo*

2.6.3 Fabricación de la tarjeta

La tarjeta era fabricada tradicionalmente con cloruro de polivinilo o PVC (*PolyVinyl Chloride*), esto permitía imprimirla con una buena resolución; estas tarjetas eran laminadas con tres capas con cubiertas transparentes en el frente y el respaldo. Recientemente, el estireno acrílico o ABS (*Acrylonitrile Butadiene Styrene*) es el más utilizado ya que permite que la tarjeta sea producida mediante un proceso de inyección sobre un molde.

Las características físicas y químicas, además de las dimensiones de la tarjeta y sus tolerancias asociadas, están reguladas por los estándares internacionales. El material para la tarjeta es fabricado en hojas planas grandes del grosor preestablecido. Para un gran volumen de producción de tarjetas, las hojas son impresas y después se cortan en tarjetas individuales.

La fabricación de la tarjeta inteligente sin contactos es diferente ya que involucra el laminado de cinco capas, dos cubiertas transparentes, dos cubiertas impresas y la tarjeta central; en este último sustrato flexible se insertan los circuitos integrados, sus conexiones y los circuitos aéreos.

2.6.3.1 Inserción del módulo en la tarjeta

Una vez que el módulo y la tarjeta han sido preparados, éstos se unen por medio de una operación de inserción. Se hace una cavidad en la tarjeta y el módulo es pegado en ella, esta cavidad es producida típicamente por medio de una operación de fresado o fundiendo el material y presionando el módulo directamente en la tarjeta, como se muestra en la Figura 2.16.

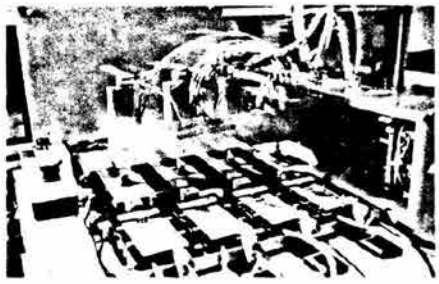


Figura 2.16 *Inserción del módulo en la tarjeta*

La primera parte de este proceso es la fabricación del sustrato que va a contener al integrado. Este sustrato generalmente contiene la placa de contactos a los que se soldará el módulo. El conector definido en las normas ISO está pensado para un integrado de aproximadamente 25 mm², aunque podrá utilizarse uno de mayor tamaño.

El problema de aumentar la superficie del módulo es la confiabilidad, y la resistencia mecánica. Una vez que el integrado está pegado al sustrato, se sueldan los contactos y se sella el conjunto con un material inerte (resina epóxica). Después, este micromódulo se pega a la tarjeta que prevé un espacio adecuado y se sella la tarjeta.

Una vez que la tarjeta está lista, terminado ya el proceso de fabricación, cada fabricante almacena en la memoria una clave de fabricación o KF (*Key Fabrication*) para proteger el circuito de modificaciones fraudulentas hasta el proceso de pre-personalización.

La KF de cada circuito es única y es derivada de una clave maestra del fabricante, otros datos de fabricación son adicionados al final de esta fase. En la Figura 2.17 se muestra el esquema de la fabricación de la tarjeta inteligente.

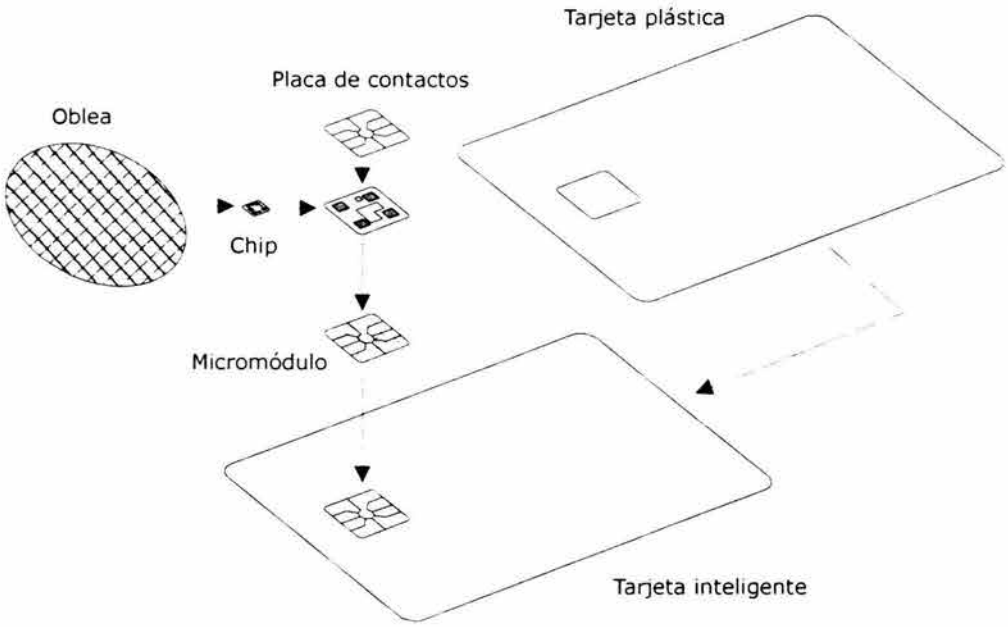


Figura 2.17 *Esquema de la fabricación de la tarjeta inteligente*

2.6.4 Fase de pre-personalización

Esta fase es conducida por el proveedor de tarjetas. En esta fase el circuito ya está montado en la tarjeta de plástico la cual podrá tener impresa en ella el logotipo del proveedor de la aplicación.

Para seguridad adicional y para facilitar una entrega segura de la tarjeta al emisor, la clave del fabricante (KF) es reemplazada por una clave de personalización o KP (*Key Personalization*). Después de esto, un candado de personalización VPER será escrito para prevenir futuras modificaciones de la KP.

En adición, serán deshabilitadas las instrucciones al acceso físico de la memoria y el acceso a la tarjeta puede ser realizado sólo mediante el uso del direccionamiento lógico de memoria; esto previene que el sistema y las áreas de fabricación sean accedidos o modificados.

2.6.5 Fase de personalización

De esta fase se encargan los emisores de las tarjetas, esto completa la creación de estructuras lógicas de datos. El contenido de los archivos de datos y de la aplicación es escrito en la tarjeta, asimismo son almacenados los datos de la identidad del poseedor, un PIN y un PIN de desbloqueo; al final un candado de utilización o VUTIL será escrito para indicar que la tarjeta está en la fase de utilización.

El procedimiento de personalización usualmente involucra también una manipulación física de la tarjeta al ser impresa información como imágenes, nombres o direcciones; del mismo modo, estos datos pueden ser grabados en sobre relieve como lo es el número de cuenta de una tarjeta de crédito.

La impresión de gráficas y texto en la TI es una característica importante ya que su apariencia es un reflejo estético y económico del emisor, información como símbolos corporativos y logotipos generan el reconocimiento de una marca. Usualmente son adicionados elementos de seguridad como los hologramas.

2.6.6 Fase de utilización

Esta es la fase para el uso normal de la tarjeta por el poseedor. El sistema de aplicación, los controles de acceso a archivos lógicos y otros son activados en esta etapa. El acceso a la información en la tarjeta será limitado por las políticas de seguridad establecidas por la aplicación.

2.6.7 Fase de invalidación

Existen dos formas para llevar la tarjeta a esta fase. Una es iniciada por la aplicación, la cual escribe el candado de invalidación a un sólo archivo o al archivo maestro. Todas las operaciones incluyendo la escritura y actualización serán deshabilitadas por el sistema operativo, sólo las instrucciones de lectura permanecerán activas para propósitos de análisis.

La otra forma de poner la tarjeta en esta fase es cuando el sistema de control bloquea irreversiblemente el acceso a la tarjeta porque ambos el PIN y el PIN de desbloqueo están bloqueados, entonces todas las operaciones serán deshabilitadas incluyendo las de lectura.

Un resumen de las claves y mecanismos de seguridad que se utilizan durante la vida de una tarjeta inteligente se encuentra en la Tabla 2.6.

Áreas/Fases	Fabricación	Pre-Personalización	Personalización	Utilización	Fin de Vida
Modo de acceso	Direccionamiento físico		Direccionamiento lógico		
Sistema	No accesible				
Claves de Fabricación	Se escribe KF	Se escribe KP	No accesible		
Datos de Fabricación	Leer, escribir, borrar	Leer	Leer		
Directorio	Leer, escribir, borrar		Conforme condiciones de acceso de archivo lógico		
Datos	Leer, escribir, borrar		Conforme condiciones de acceso de archivo lógico		
Código Opcional	Leer, escribir, borrar		Conforme condiciones de acceso de archivo lógico		

Tabla 2.6 *Claves y mecanismos de seguridad del ciclo de vida*

2.7 FABRICANTES

Existen diferentes fabricantes de tarjetas inteligentes a nivel mundial, en la Tabla 2.7, se muestra una lista de algunos junto con la dirección de la página de acceso a Internet.

Fabricante	Página Web
Allegheny Printed Plastics	www.allegheny.com
Allsafe Co.	www.allsafe.com
American Microdrive Manufacturing, Inc.	www.ammismarteards.com
Bull Personal Transaction Systems	www.cp8bull.net
Datakey, Inc.	www.datakey.com
Deister Electronics	www.deister.com
Fábrica Nacional de Monedas y Timbres	www.fnmt.es
Gemplus-DataCard	www.gemplus.com
Giesecke & Devrient America Inc.	www.gdm.de
GPT Card Technology	www.gpt.co.uk
Laminex	www.laminex.com
NBS Technologies Inc.	www.nbstech.com
Oberthur Smart Cards	www.kirkplastic.com
Orga Kartensystems GmbH	www.orga.com
Schlumberger Cards & Systems	www.slb.com/et
Spartanics	www.spartanics.com
SSI Custom Data Cards	www.ssiphoto.com
SuperTech Systems Inc.	www.supertecsystems.com
Versatile Card Technology, Inc.	www.versacard.com
Worldtronix	www.worldtronix.ca

Tabla 2.7 *Fabricantes de tarjetas inteligentes a nivel mundial*

2.8 ESTÁNDARES

Conforme a la Organización Internacional de Estándares (ISO), Estándares son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para medición de materiales, productos, procesos y servicios que son convenientes para su propósito. Los estándares y normas internacionales referentes a las TI's, se resumen en la Tabla 2.8.

Estándar	Título/Descripción
Estándares ISO para Tarjetas de Identificación	
ISO 7810	Características físicas.
ISO 7811	Técnicas de grabado.
ISO 7812	Tarjetas de identificación.
ISO 7813	Tarjetas para transacciones financieras.
ISO 7816	Tarjetas de circuitos integrados con contactos.
ISO/IEC 10373	Métodos de chequeo.
ISO/IEC 10536	Tarjetas sin contactos.
ISO/IEC 14443	Tarjetas para comunicaciones por acoplamiento remoto.
Estándares ISO generales de seguridad	
ISO 9564	Administración del PIN y seguridad.
ISO 9796	Tecnología de información. Técnicas de Seguridad. Firma digital que da la recuperación del mensaje.
Estándares específicos para la industria (Financiera, Telecomunicaciones, Aerolíneas)	
ISO 9992	Tarjetas para transacciones financieras. Mensajes entre tarjetas de circuito integrado y el dispositivo lector.
ISO DIS 10202	Tarjetas para transacciones financieras. Esquema de seguridad para transacciones realizadas con tarjetas de circuito integrado.
EMV	Especificaciones para tarjetas de circuito integrado aplicadas en sistemas de pago.
EN-726	Sistemas de identificación por medio de tarjetas de circuito integrado. Terminales y aplicación en las telecomunicaciones.
ETSI GSM 11.11	Sistema europeo digital de telecomunicación celular (Fase 2). Especificación del módulo de identidad del suscriptor. Interfaz del equipo móvil.
ETSI GSM 11.14	Sistema europeo digital de telecomunicación celular (Fase 2+). Especificación del módulo de identidad del suscriptor usando un voltaje de 3 Volts.
ANSI T1P1	Estándar norteamericano de telecomunicaciones
IATA JPSC 791	Asociación Internacional de Líneas Áreas de Transportación (IATA). Especificaciones de Tarjetas Inteligentes.

Tabla 2.8 *Estándares y especificaciones relacionados con las tarjetas inteligentes*

2.9 APLICACIONES

El beneficio que aporta una tarjeta inteligente está en función del proceso que pueda realizar: pagos, identificación, computación en red, administración de servicios, etc.

Hay una gran variedad de instituciones como Visa, MasterCard, Lucent Technologies, Nec y otros fabricantes y/o proveedores de servicios que juegan un papel muy importante en el desarrollo y la oferta de soluciones, permitiendo aprovechar las ventajas que ofrece la tecnología de las TI's. De las diversas aplicaciones existentes en el mundo se pueden mencionar:

En el sector de las telecomunicaciones.

- Tarjetas de prepago telefónico.
- Tarjetas para telefonía celular GSM.
- Acceso seguro a redes privadas.
- Servicios bidireccionales de televisión por cable o satelitales.
- Servicios de acceso a Internet.

En el sector salud.

- Registro de historial médico de pacientes.
- Registro de emergencias.
- Prescripción y adquisición de medicamentos.

En el sector transporte.

- Control de acceso a estacionamientos.
- Pago de boletos de transporte público urbano y foráneo.
- Pago de cuotas en autopistas.

En el sector de la educación.

- Identificación de alumnos.
- Acceso a bibliotecas.
- Máquinas expendedoras.
- Pago de servicios.

En el sector financiero.

- Medios electrónicos de pago.
  - Monedero electrónico.
  - Tarjeta de débito/crédito.
- Sistemas electrónicos de firma y verificación.

En el sector comercio.

- Medios electrónicos de pago.
- Programas de lealtad.
- Boletos electrónicos.

Adicionalmente, la tarjeta inteligente tiene como aplicación de propósito general la identificación y control de acceso a instalaciones.

En la gráfica de la Figura 2.18 se puede apreciar la distribución del mercado de las tarjetas inteligentes de acuerdo a su aplicación, siendo preponderante su uso como tarjeta telefónica.

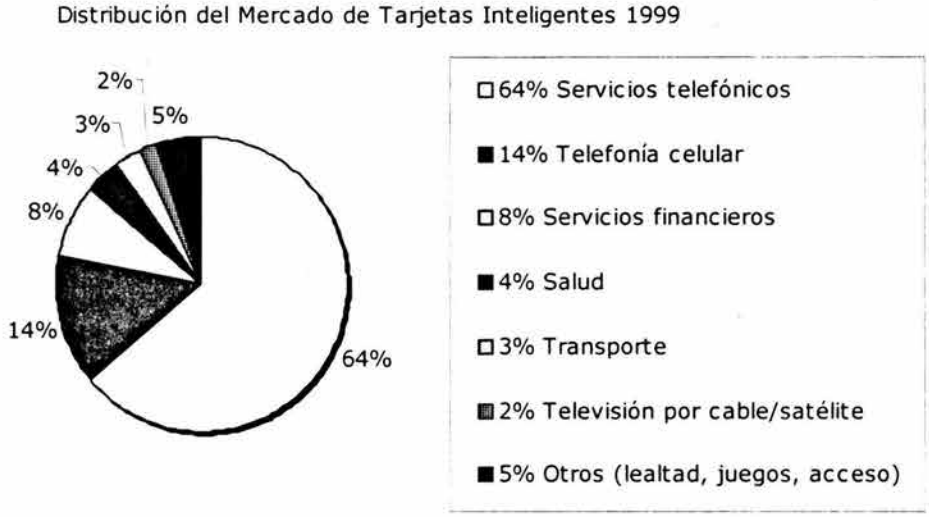


Figura 2.18 *Gráfica de la distribución del mercado de las tarjetas inteligentes en 1999 (Fuente: Schlumberger)*

2.10. EVOLUCIÓN DEL MERCADO

Las TI's han tenido una fuerte aceptación en el mundo entero sobre todo en Europa, su lugar de origen como se observa en la Tabla 2.9.

Tarjetas inteligentes con microprocesador (millones)							
Región	**2001**	**2002**	Crecimiento	**2003**	Crecimiento	**2004**	Crecimiento
Europa, Medio Este, África	320	340	47%	360	45%	385	41%
Asia-Pacífico	272	310	43%	350	44%	425	46%
Latinoamérica	20	25	3%	34	4%	45	5%
Norteamérica	30	50	7%	60	7%	75	8%
Total	642	725	13%	804	11%	930	16%

Tabla 2.9 *Mercado de las tarjetas con microprocesador, por región (Fuente: Schlumberger)*

De acuerdo al reporte anual del 2002 realizado por Schlumberger, empresa fabricante, las tarjetas con microprocesador tuvieron un crecimiento del 13% para ese año (ver Tabla 2.10), a diferencia de las tarjetas de memoria (ver Tabla 2.11), que muestran un decremento en el mismo periodo. Asimismo, se estima un incremento del 7% para el 2003 y un 10% en el siguiente año.

Tarjetas con microprocesador (millones)							
Aplicación	**2001**	**2002**	Crecimiento	**2003**	Crecimiento	**2004**	Crecimiento
Telefonía	400	450	13%	480	7%	530	10%
Banca	145	170	17%	190	12%	230	21%
Otros	97	105	8%	134	28%	170	27%
Total	642	725	13%	804	11%	930	16%

Tabla 2.10 *Mercado de las tarjetas inteligentes con microprocesador, por aplicación (Fuente: Schlumberger)*

Tarjetas de memoria (millones)							
Aplicación	**2001**	**2002**	Crecimiento	**2003**	Crecimiento	**2004**	Crecimiento
Telefonía	1060	980	-8%	950	-3%	920	-3%
Otros	99	110	11%	120	9%	130	8%
Total	1159	1090	-6%	1070	2%	1050	-2%

Tabla 2.11 *Mercado de las tarjetas de memoria, por aplicación (Fuente: Schlumberger)*

Estos datos ofrecen una clara idea de las oportunidades que existen para el diseño de aplicaciones que utilicen tarjetas con microprocesador, pero sobre todo, que permiten la posibilidad de integrar aplicaciones o servicios diversos en una sola para satisfacer las necesidades de un mercado bastante atractivo y en constante crecimiento.

2.11 COSTO DE UNA TARJETA INTELIGENTE

Los costos de las TI's varían en función del fabricante y características de la tarjeta como puede ser su capacidad de almacenamiento. La Tabla 2.12 muestra un cuadro de precios de la tarjeta inteligente utilizada por VISA.

Tipo de Tarjeta	Seguridad	Memoria	Costo (USD)
Static/Native	DES	N/A	$0.99
GP-DES/16	Triple DES	45K ROM 16K EEPROM	$2.37
GP-DES/17	Triple DES	64K ROM 16K EEPROM	$2.50
GP-DES/32	Triple DES	96K ROM 32K EEPROM	$2.64
GP-Entry	Llave Pública	64K ROM 8K EEPROM	$1.98
GP-PK/8	Llave Pública	64K ROM 8K EEPROM	$2.46
GP-PK/16	Llave Pública	64K ROM 16K EEPROM	$2.86
GP-PK/32	Llave Pública	96K ROM 16K EEPROM	$3.36
GP-DI/16 Inalámbrica	Llave Pública	64K ROM 16K EEPROM	$3.47

Tabla 2.12 *Costo de las tarjetas inteligentes utilizadas por VISA*

La Tabla 2.13 muestra el cuadro de costos para los productos fabricados por Schlumberger.

Tipo de tarjeta	Características	Costo (USD)
Cryptoflex 8K	RSA, DES, 3DES 8K EEPROM Almacena Llave privada y certificados digitales.	$12.80
Cryptoflex para Windows 2000 y XP	Manejo de seguridad	$12.80
MicroPayfles	Diseñada para el manejo de monedero electrónico privado y programas de lealtad.	$4.10
Cryptoflex e-gate 32K sin conector	Inalámbrica.	$20.00
Cryptoflex e-gate 32K con conector	Incorpora una interfaz USB en la tarjeta permitiendo la conexión directa de la tarjeta al puerto USB de una computadora.	$20.00

Tabla 2.13 *Costo de las tarjetas inteligentes fabricadas por Schlumberger*

Sistemas Operativos para Tarjetas Inteligentes

- Principios fundamentales
- Principios de diseño e implementación
- Estructura de la memoria
- Estructura de los datos
- Seguridad
- Integración en la plataforma Windows
- Integración en la plataforma Java
- Sistemas operativos en el mercado

Capítulo 3

CAPÍTULO 3. SISTEMAS OPERATIVOS PARA TARJETAS INTELIGENTES

Los sistemas operativos se utilizan en diferentes plataformas de hardware, las cuales cubren desde calculadoras de bolsillo, organizadores, PC's, hasta las propias tarjetas inteligentes. En un sentido amplio el término sistema operativo, para el cual no existe una definición general, se refiere a un grupo de programas requerido para la operación de la computadora.

El sistema operativo provee funciones predefinidas para el usuario, quién no requiere tener conocimiento alguno del hardware. El usuario puede ejecutar y programar aplicaciones independientemente del equipo. El sistema operativo se ocupa de controlar y organizar los dispositivos de almacenamiento como son la memoria RAM, discos duros, CD'S, etc., y de programar los procesos efectuados por el procesador central. También, permite a los fabricantes de hardware incorporar una amplia variedad de desarrollos tecnológicos sin la necesidad de realizar cambios en las funciones del sistema operativo.

El cerebro de una tarjeta inteligente es su sistema operativo; es el código encargado de manejar los archivos del sistema, la seguridad de los datos, E/S, la manipulación de la información para las diferentes aplicaciones, etc. Esto es similar a los sistemas operativos de las PC's, sólo que se limita a unos cuantos miles de bytes.

Las tareas básicas del sistema operativo de la TI pueden ser caracterizadas de la forma siguiente:

- Transmisión bidireccional de datos en una interfaz serial.
- Carga, operación y manejo de aplicaciones.
- Control de ejecución y procesamiento de instrucciones.
- Manejo de memoria y archivos.
- Administración de la seguridad del hardware.
- Ejecución de métodos criptográficos para autenticación.
- Almacenamiento seguro de datos.
- Manejo de algoritmos de encriptación.

3.1 PRINCIPIOS FUNDAMENTALES

En contraste con los sistemas operativos conocidos, los sistemas basados en tarjetas inteligentes no permiten al usuario el almacenamiento externo de información, siendo las prioridades más importantes la ejecución segura de los programas y el control de acceso a los datos.

Debido a la restricción de memoria, la cantidad de información que se puede almacenar es muy pequeña, estando entre 2 y 60 KBytes. Los módulos de programa se graban en la ROM, esto posee la desventaja de no permitir al usuario programar el funcionamiento de la tarjeta según sus propios criterios, ya que una vez grabado el sistema operativo es imposible realizar algún cambio. Por esto, el programa grabado en la ROM debe ser bastante fiable y robusto.

Otra característica importante del sistema operativo es que no permite el uso de puertas traseras, que son bastante frecuentes en los sistemas grandes. Esto quiere decir, que es

imposible hacer una lectura desautorizada de los datos contenidos usando el código propio de la tarjeta.

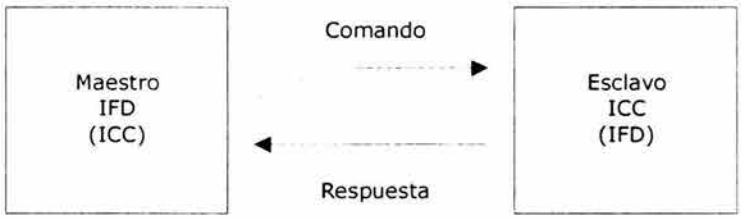
Un sistema operativo seguro es aquel que protege la información que se intercambia entre un usuario y el sistema, y está asociado a las siguientes áreas:

- Confidencialidad: La información es mantenida en secreto, donde tendrán acceso a ésta solamente personas autorizadas.
- Integridad: La información no puede ser alterada ni destruida por un usuario sin autorización.
- Autenticación: Es la verificación de la identidad de un usuario o dispositivo para que éste tenga acceso al sistema.
- No-Repudiación: Asegura que el autor de un mensaje no puede negar que él envío dicho mensaje, así como el receptor de éste no puede negar que lo recibió.
- Autorización: Es permitir el acceso a una parte de la información dentro de un sistema.

Por definición, el sistema operativo de una TI debe ser bastante seguro puesto que debe administrar y proteger datos confidenciales. Por otro lado, no deben permitirse modificaciones en dicho sistema que puedan conducir a posibles fallos en el funcionamiento de la tarjeta.

3.2 PRINCIPIOS DE DISEÑO E IMPLEMENTACIÓN

El flujo de información entre el dispositivo de interfaz y la tarjeta inteligente ocurre mediante los protocolos de transporte en forma de pares de comando-respuesta. En la mayoría de los casos el dispositivo de interfaz o la aplicación tiene el rol de maestro, es decir, los comandos serán generados y procesados por el dispositivo de interfaz. Lo anterior se muestra en la Figura 3.1.



IFD Dispositivo de interfaz (*Interface Device*)
ICC Circuito Integrado de la Tarjeta (*Integrated Circuit Card*)

Figura 3.1 *Transacción de información.*

La información de la transacción puede ser dividida en tres secciones de protocolos:

- Capa física.
- Protocolos de transmisión de datos.
- Protocolos de información para datos de instrucciones y respuesta de datos.

Los sistemas operativos para TI's están divididos en unidades modulares de funciones llamadas administradores (ver Figura 3.2). Una transacción de información es procesada por los siguientes administradores:

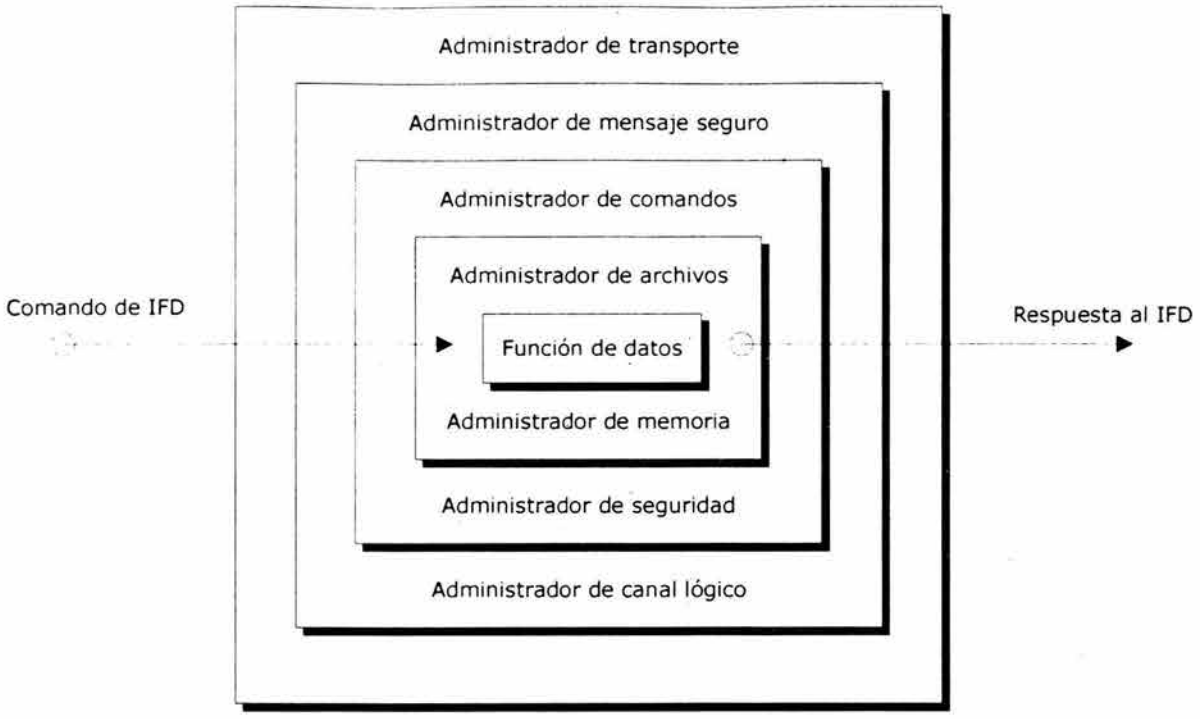


Figura 3.2 *Estructura del sistema operativo de una tarjeta inteligente.*

- Administrador de transporte. Controla y asegura la transmisión de datos mediante protocolos de transporte asíncronos half-duplex. Estos son conocidos como T=0 y T=1.
- Administrador de mensaje seguro. Cubre la protección criptográfica de la transmisión mediante la encriptación y desencriptación de la información y/o mediante la verificación de la autenticidad de la información.
- Administrador de canal lógico. Se requiere para acceder una aplicación en caso de existir más de una aplicación abierta simultáneamente. En este caso se necesita manejar procesos multitarea; un ejemplo de ello es cuando un banco transfiere fondos a un monedero electrónico.
- Administrador de comandos. Verifica la sintaxis de los comandos. En algunos sistemas operativos también controla el protocolo de procesamiento de comandos.
- Administrador de seguridad. Está a cargo del control de acceso a los objetos, en particular a las llaves.
- Administrador de archivos. Administra los diferentes tipos y categorías de archivos.
- Administrador de memoria. Gestiona la organización de la memoria tanto para aplicaciones como para archivos. Calcula el checksum, restaura estructuras de archivos defectuosas o con error y administra la memoria disponible.
- Función de datos. Realiza operaciones matemáticas requeridas para funciones criptográficas específicas, en algunos chips son soportadas por el hardware. Estas

funciones pueden ser parte del sistema operativo o bien estar incluidas como parte de la aplicación.

3.2.1 Comandos

La funcionalidad de un sistema operativo no sólo se refleja en el número de comandos disponibles, sino también en su complejidad. Ésta crece con la necesidad de incrementar la seguridad de las aplicaciones. El estándar ISO 7816-4, ver Tabla 3.1, define a un conjunto de comandos básicos para proporcionar acceso, seguridad y transmisión de datos de la tarjeta y pueden ser agrupados en las siguientes clases de acuerdo a su función:

- Selección de archivos.
- Lectura de datos.
- Modificación y borrado de datos.
- Generador de datos.
- Comparación de datos.
- Autenticación usando funciones criptográficas.

Perfil	Descripción	Características
M	Estructura de datos	Transparente Lineal fijo
	Comandos	READ BINARY, UPDATE BINARY READ RECORD, UPDATE RECORD SELECT FILE (usando FID) VERIFY INTERNAL AUTHENTICATE
N		Permite el comando SELECT FILE usando AID
O	Estructura de datos	Transparente Lineal fijo y variable Cíclico
	Comandos	READ BINARY, UPDATE BINARY READ RECORD, UPDATE RECORD APPEND RECORD SELECT FILE VERIFY INTERNAL AUTHENTICATE EXTERNAL AUTHENTICATE GET CHALLENGE
P	Estructura de datos	Transparente
	Comandos	READ BINARY, UPDATE BINARY SELECT FILE (usando AID, *Application ID*) VERIFY INTERNAL AUTHENTICATE
Q	Transferencia de datos	Intercambio seguro de datos
	Comandos	GET DATA PUT DATA SELECT FILE (usando AID) VERIFY INTERNAL AUTHENTICATE EXTERNAL AUTHENTICATE GET CHALLENGE

Tabla 3.1 *Perfiles especificados en el ISO 7816-4*

En contraste con el funcionamiento de cualquier computadora, la memoria de una tarjeta está muy restringida en capacidad, por esto, en algunos casos es imposible incluir en una sola tarjeta todas las instrucciones y estructuras de archivos. Por esta razón se han creado varios "perfiles" de tarjetas inteligentes que están especificados en el ISO 7816-4.

Cada uno de estos perfiles define un subconjunto de instrucciones y estructuras de archivos que se resumen en la Tabla 3.1. Por lo tanto, las tarjetas realizarán distintas funciones de acuerdo al perfil al que pertenecen.

Debido a la complejidad de las aplicaciones actuales, aproximadamente el 60% de los comandos de un sistema operativo son de uso privado y no están definidos en el estándar ISO 7816-4. Como ejemplo se puede mencionar los comandos para autenticación mutua de funciones de seguridad criptográfica, los cuales están desarrollados mediante el encadenamiento de funciones básicas, también conocidos como macros.

3.3 ESTRUCTURA DE LA MEMORIA

Existen tres tipos de memoria dentro de la TI de circuito integrado y cada una tiene propiedades totalmente diferentes.

La ROM sólo se puede programar durante el proceso de fabricación y no se puede alterar una vez terminada dicha fase. Por otro lado, la RAM mantiene su contenido solamente cuando se aplica voltaje sobre la tarjeta. Cualquier fallo en la alimentación provoca la pérdida total de los datos almacenados en dicha memoria. En la Figura 3.3 se muestra un ejemplo de como está dividida la memoria RAM.

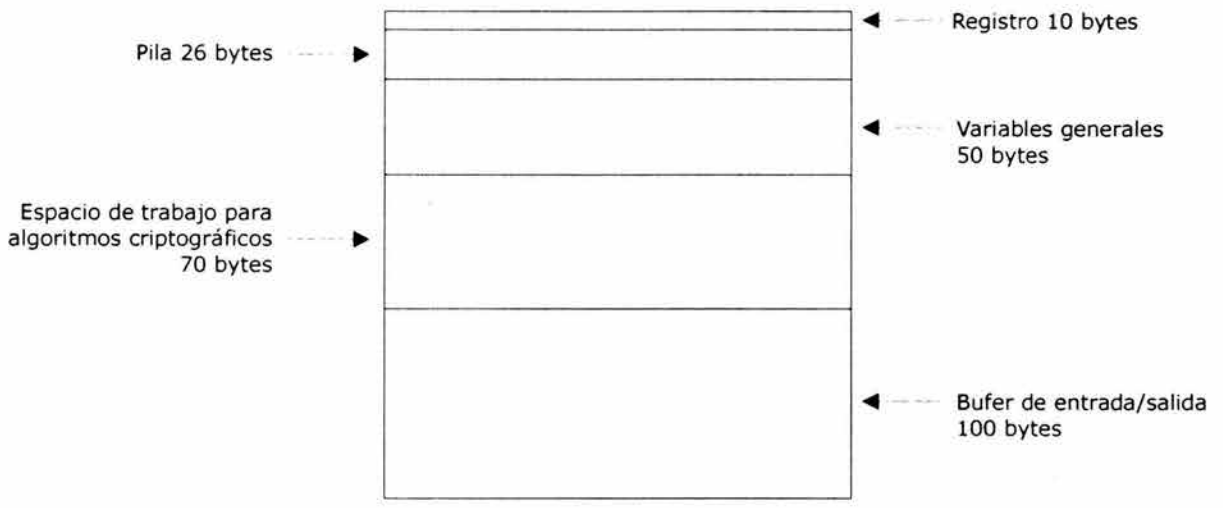


Figura 3.3 *Estructura de una memoria RAM de 256 bytes*

La memoria EEPROM puede retener los datos almacenados en ella incluso una vez desconectada la alimentación, pero su tiempo de escritura/lectura es demasiado grande (1 ms/byte). Si, por ejemplo, es necesario un buffer de entrada/salida de 256 bytes, que es

la capacidad total de la memoria, el sistema operativo puede usar la memoria EEPROM como si fuera RAM, pero con la desventaja de que la escritura sobre la EEPROM es más lenta.

La estructura de la EEPROM es más complicada que la de otras memorias. En los sistemas operativos modernos la división es la siguiente: primero están almacenados algunos datos de producción que pueden ser números fijos, y por lo tanto no varían, que son usados para funciones específicas. Esta zona suele estar protegida contra accesos no autorizados por algún mecanismo de hardware.

Después de esta zona, que habitualmente es de 32 bytes, están las tablas y los punteros del sistema. Estos se graban durante la fase de fabricación y en conjunto con el programa de la ROM forman el sistema operativo. Para asegurar que el sistema funcione perfectamente esta sección de la EEPROM está protegida con un checksum que es calculado antes de cada acceso a esta zona. Si se encuentra algún error en este cálculo, el sistema operativo dejará de usar esta zona de memoria.

A la sección de memoria anterior le sigue otra que contiene códigos adicionales de los programas de aplicación. En algunos casos, esta zona está protegida contra posibles alteraciones mediante el uso de un checksum. Los datos contenidos también pueden ser algoritmos que no están almacenados en la ROM por falta de espacio.

La zona adyacente contiene todas las estructuras de archivos. Esta zona no está protegida por ningún mecanismo, pero generalmente existen módulos de hardware o software orientados a proteger los archivos.

Al final de la memoria EEPROM existe una zona libre que está administrada por el portador de la tarjeta, esto quiere decir que en ella se pueden almacenar los datos de usuario. En la Figura 3.4 se muestran estas divisiones.

Figura 3.4 *Ejemplo de la división de la EEPROM*

3.4 ESTRUCTURA DE LOS DATOS

Una de las principales características de las TI's es que pueden almacenar datos e incluso proteger el acceso a ellos por lectores no autorizados. Las TI's incluyen sistemas de administración de archivos que siguen una estructura jerárquica. Los programas que controlan estos sistemas están minimizados para reducir el uso de memoria.

Los sistemas operativos están orientados a trabajar con objetos, esto quiere decir que los datos referentes a un archivo están contenidos en él mismo, como se muestra en la Figura 3.5. Para efectuar un cambio en el contenido de un archivo, éste debe ser seleccionado con la correspondiente instrucción.

Los archivos están divididos en dos secciones: la primera se denomina cabecera que contiene los datos referentes a la estructura de archivo y a las condiciones de acceso. La otra sección es el cuerpo del archivo que comprende los datos del usuario.

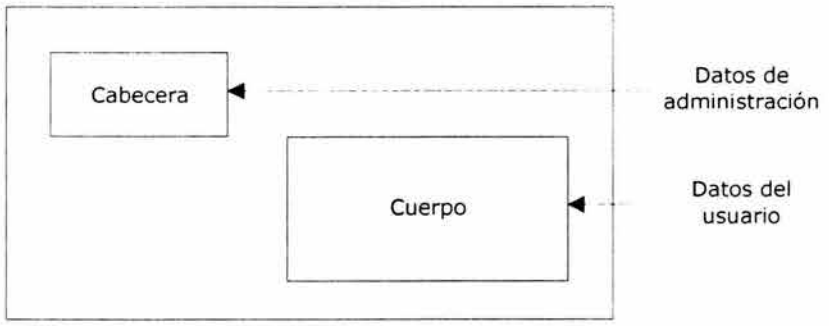


Figura 3.5 *Estructura interna del sistema de archivos de una TI*

3.4.1 Tipos de Archivos

La estructura de los archivos contenidos en una TI está especificada en el estándar ISO 7816-4 y es similar a los sistemas DOS o UNIX. Existen varios directorios que hacen las funciones de carpetas que contienen los archivos. Los tipos de archivos son:

- **Archivo maestro o MF**

El MF es la raíz del sistema de archivos y sólo existe uno en cada tarjeta. Normalmente se selecciona de forma automática después de reinicializar la TI. Los datos utilizados para todas las aplicaciones en la tarjeta (por ejemplo, información administrativa y de seguridad como el número de serie, llaves, PIN) y datos relacionados con el manejo del ciclo de vida de la tarjeta son almacenados en este archivo. Esta información es utilizada por los sistemas operativos para la creación de nuevas aplicaciones. El archivo maestro también representa a toda la memoria disponible de la tarjeta para almacenar información.

- **Archivo dedicado o DF**

La información para el control específico de una aplicación y sus archivos se almacena en un archivo dedicado. Están separados lógicamente y/o físicamente de otras aplicaciones contenidas en diferentes DF's. En caso necesario, pueden existir archivos dedicados en el siguiente nivel, es decir, un directorio puede contener archivos o incluir a otros DF's. El nivel de anidamiento es infinito y está restringido por la capacidad de memoria de la tarjeta.

- **Archivo elemental o EF**

Un archivo elemental solamente puede contener datos. El tamaño máximo de un EF debe ser especificado al momento de su creación. De igual forma, los datos del usuario necesarios para la aplicación están almacenados en estos archivos. Los EF's pueden existir a continuación del archivo maestro, ver Figura 3.6.

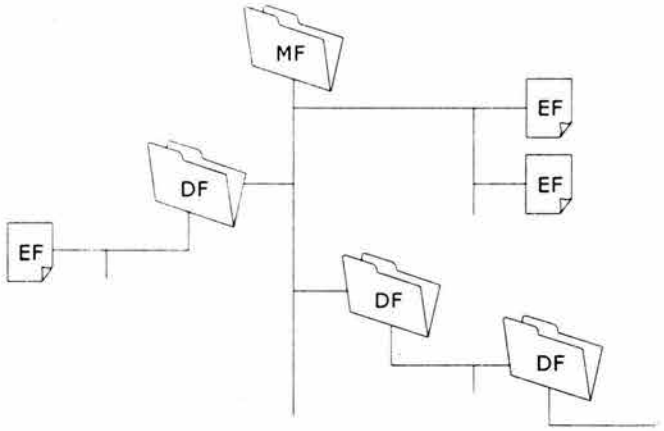


Figura 3.6 *Tipos de archivos de una TI*

3.4.2 Archivo interno del sistema

Además de los archivos elementales, pueden existir en la tarjeta archivos propios del sistema operativo los cuales se utilizan para ejecutar aplicaciones o almacenar códigos secretos. El acceso a estos archivos es controlado por el sistema operativo.

Existen dos maneras distintas de integrar estos archivos dentro de la memoria, el método ISO consiste en ocultarlos dentro del archivo dedicado correspondiente a la aplicación y por lo tanto no pueden ser seleccionados. Otro método, propuesto por el Instituto Europeo para la Estandarización de las Telecomunicaciones (*ETSI*) consiste en asignar a estos archivos un nombre o FID *(File ID)* con el cual puedan ser seleccionados.

Es habitual relacionar todos los datos referentes a una determinada aplicación con un mismo archivo dedicado, con esto se consigue una estructura clara y organizada. Además, si el usuario desea aumentar el número de aplicaciones de su tarjeta bastará con crear un nuevo DF que contenga los datos. Cuando la tarjeta tiene una sola aplicación los datos pueden estar contenidos en un archivo maestro como se muestra en la Figura 3.7.

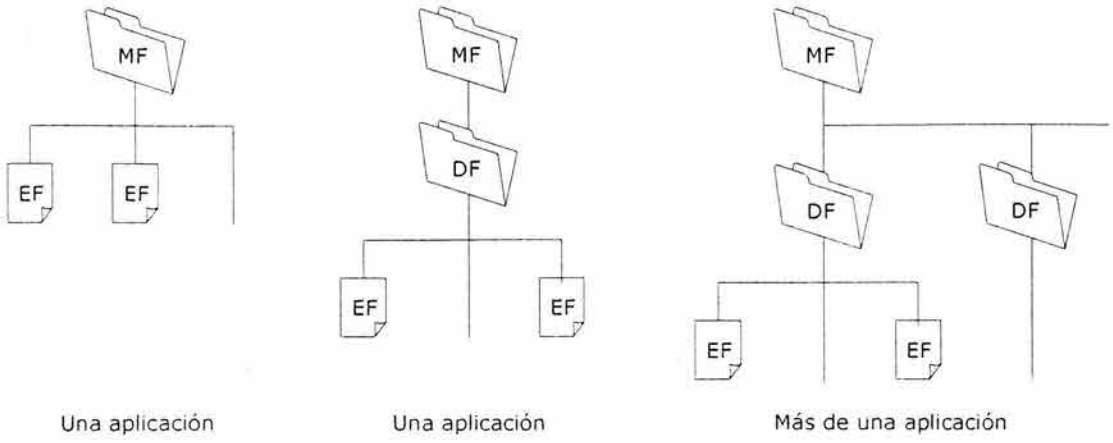


Figura 3.7 *Estructura de archivos en función de las aplicaciones contenidas en la TI*

3.4.3 Identificación de los archivos

Todos los archivos y directorios tienen un identificador o FID de 2 bytes de longitud que se usa para seleccionarlos. El archivo maestro tiene el FID 3F00 hexadecimal. El valor FFFF está reservado para aplicaciones futuras.

Los valores del FID de cada archivo deben escogerse de tal manera que no se repitan, de forma que dos EF que estén dentro del mismo DF no tengan el mismo FID; tampoco está permitido que un DF posea un FID igual al de un EF que esté directamente relacionado con él.

La telefonía GSM representa un ejemplo del identificador FID. En el estándar GSM 11.11 el byte más significativo del FID representa la posición dentro de la estructura de archivos. Si el archivo es un DF este byte tiene siempre el valor 7F.

Los EF que pertenecen directamente al archivo maestro tienen el valor 2F como primer byte del FID, y todos los EF que pertenezcan a un mismo DF tienen el valor 6F en esa posición. El byte menos representativo se enumera de manera consecutiva según se vayan creando los archivos.

Los archivos dedicados o DF se usan para organizar los archivos que pertenecen a una misma aplicación y por lo tanto actúan como si fueran carpetas. Poseen, aparte del FID, un identificador de aplicación llamado AID (*Application ID*) que tiene una longitud de 5 a 16 bytes.

Este identificador está dividido en dos secciones: el primer elemento es el identificador de registro o RID (*Register ID*), en él se almacena información como el código de país, la categoría de la aplicación y un número que sirve para identificar al proveedor de la aplicación o PIX (*Proprietary Extension*).

Este último elemento es opcional y es grabado por el proveedor de la aplicación. Su longitud puede ser hasta 11 bytes como se observa en la Figura 3.8.

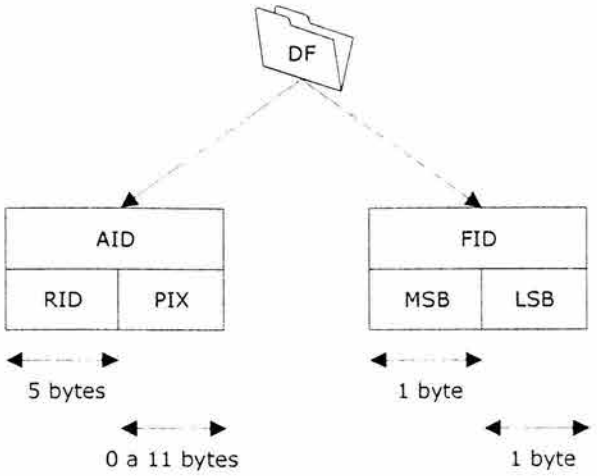


Figura 3.8 *Identificadores de un archivo DF*

3.4.4 Direccionamiento de los archivos

Debido a la estructuración en objetos del sistema operativo de las TI's, es necesario seleccionar los archivos antes de su acceso. Esto sirve para indicarle al sistema operativo con que archivo se desea trabajar. Así, se impide la posibilidad de seleccionar dos archivos a la vez.

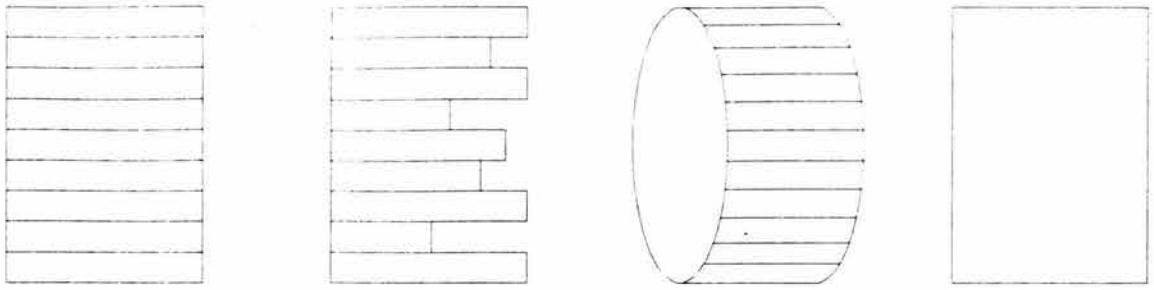
El archivo maestro se puede seleccionar desde cualquier parte de la estructura de la memoria usando el identificador 3F00. Los archivos dedicados se pueden direccionar a través del correspondiente FID o también usando el identificador de aplicación AID.

Existen dos métodos para seleccionar los archivos EF. La selección explícita consiste en enviar a la tarjeta una instrucción especial que contenga los dos bytes del FID como parámetro para identificar al archivo.

En algunos casos, sólo es necesario especificar en la instrucción de selección de archivos, los cinco primeros bits menos significativos del FID, en este caso a la selección se le denomina implícita. Este método permite elegir un archivo y al mismo tiempo posibilita que el acceso a dicho archivo se realice con la misma instrucción de selección.

3.4.5 Tipos de estructura de archivos

Los archivos de las tarjetas inteligentes poseen una estructura interna con diferentes tipos, mostrados en la Figura 3.9, que se pueden aplicar libremente a cualquier EF dependiendo del propósito del mismo. Estos tipos son:



(a) Lineal fijo (b) Lineal variable (c) Cíclico (d) Transparente

Figura 3.9 *Estructuras de archivos de una TI (a,b,c,d)*

- **Archivo lineal fijo**

El archivo lineal fijo, ver Figura 3.9a, está basado en una serie de celdas de igual longitud que están unidas en forma de matriz. La unidad más pequeña a la que se tiene acceso es una celda y no se puede acceder a fracciones de la misma. Las instrucciones que se usan para acceder a las celdas son: READ RECORD, WRITE RECORD y UPDATE RECORD.

A la primera celda se le identifica con el número 01 hexadecimal mientras que el número más alto permitido es FE, estando FF reservado para usos futuros. El tamaño de cada celda puede variar entre 1 y 254 bytes, siendo las celdas de una matriz del mismo tamaño.

- **Archivo lineal variable**

El archivo lineal variable, Figura 3.9b, fue creado para resolver las limitaciones en el espacio de memoria y aprovecha el hecho de almacenar datos de longitud variable. Cada celda puede tener un tamaño variable en función de los datos que se almacenan en ella. El tipo de numeración y el tamaño de cada celda son exactamente iguales que en el caso anterior. Las instrucciones usadas también son las mismas.

- **Archivo cíclico**

El archivo cíclico, mostrado en la Figura 3.9c, se basa en la estructura de datos de un archivo lineal fijo. En este caso existe un puntero que indica cuál fue el último conjunto de datos accedido. Una vez que el puntero llega a la última celda, este es colocado por el sistema operativo de la tarjeta en la primera posición de la matriz.

- **Archivo transparente**

Al archivo transparente, Figura 3.9d, se le conoce normalmente como archivo binario. Este archivo no posee ningún tipo de estructura y los datos se pueden leer o escribir byte a byte por medio de un puntero que se desplaza a través del mismo. Las instrucciones usadas para

trabajar con esta estructura son: READ BINARY, WRITE BINARY y UPDATE BINARY. El tamaño mínimo que puede tener es de un 1 byte mientras que el máximo no está especificado.

- **Archivo ejecutable**

El archivo ejecutable se describe en el estándar europeo EN 726-3, ofrece posibilidades de ampliación del sistema operativo de las tarjetas inteligentes. Este archivo no se creó para almacenar datos sino para contener archivos que puedan ser ejecutados directamente por la propia tarjeta.

3.4.6 Tipos de acceso a los archivos

Todas las estructuras contienen datos que sirven para regular el acceso a las mismas. Estos datos están contenidos en la cabecera. La responsabilidad de la seguridad de los datos almacenados en una tarjeta recae en el sistema de administración de archivos.

La autorización de acceso es determinada cuando se crea el archivo y como norma general no puede ser modificada posteriormente. Los distintos tipos de accesos varían en función del sistema operativo de la tarjeta y de las instrucciones que soporte. Cada vez que se crea un EF es necesario, por seguridad de los datos, definir los derechos de accesos sobre dicho archivo.

Las instrucciones para manipular los archivos varían de un sistema operativo a otro, las más comunes se muestran en la Tabla 3.2.

Instrucción	Descripción
APPEND	Ampliar el tamaño de un archivo
DELETE FILE	Borrar archivo
INVALIDATE	Bloquear el acceso al archivo
LOCK	Bloquear indefinidamente el archivo
READ/SEEK	Leer o buscar en el contenido de un archivo
REHABILITATE	Desbloquear archivo
WRITE/UPDATE	Escribir en un archivo
CREATE	Generar un archivo nuevo
REGISTER	Registrar un archivo nuevo

Tabla 3.2 *Instrucciones para la administración de archivos*

3.4.7 Atributos de los archivos

Adicionalmente a los derechos de acceso, los archivos cuentan con otros atributos que se explican a continuación, estos se definen en el momento de la creación del archivo.

- **Atributo WORM**

El atributo WORM (*Write Once, Read Many*) o "escribe una vez, lee muchas veces" permite que los datos contenidos en un archivo se puedan escribir una vez, pero se pueden leer

muchas veces. Esta característica debe ser soportada por el hardware de la EEPROM o también se puede incorporar usando una función de software. El propósito de este atributo es proteger los datos importantes contenidos en la tarjeta contra posibles sobre escrituras.

- **Atributo de escritura múltiple**

Este atributo es muy usado en telefonía GSM para archivos de gran actividad de uso. Permite que el contenido del archivo pueda ser alterado muchas veces, el número máximo depende de los ciclos de lectura y escritura de la EEPROM.

- **Atributo de corrección de errores**

Este atributo se usa para datos que son particularmente importantes y que requieren algún tipo de código de detección de errores o EDC (*Error Detection Code*). La protección EDC combinada con la posibilidad de múltiples escrituras, permite incluso la corrección de errores producidos en la memoria EEPROM.

3.4.8 Código programado en circuito

A diferencia de otros sistemas operativos, no es frecuente en la industria de las TI's almacenar programas como si fueran archivos y ejecutarlos cuando sea necesario. Sin embargo, ésta es una de las principales funciones de cualquier sistema. Existen varias razones por las que esta función ha estado ausente en las tarjetas durante mucho tiempo.

La razón principal es que cualquiera que conozca los métodos para crear un archivo ejecutable puede con ese programa simular el comportamiento de algunas aplicaciones para las cuales la tarjeta no fue creada. Teniendo en cuenta que los microprocesadores de las tarjetas inteligentes no tienen protección de memoria de ningún tipo, tan pronto como el contador de programa sea cargado con la dirección del archivo ejecutable, el control de las secciones de memoria pasará enteramente a dicho archivo. Esto quiere decir que podrá saltarse los mecanismos de seguridad y acceder cualquier dato almacenado.

La programación de una tarjeta puede realizarse de dos maneras: la primera consiste en almacenar el código de programa en un archivo ejecutable. Para activar el programa basta con seleccionar dicho archivo y enviar la orden EXECUTE, en algunos casos también deben satisfacerse las condiciones de acceso. La respuesta generada por el programa se devuelve como parte de la respuesta a la orden de ejecución.

El otro método de creación de archivos ejecutables está descrito en el estándar EN 726-3 que define a los Sistemas de Identificación por medio de tarjetas de circuito integrado - Terminales y aplicación en las telecomunicaciones. De acuerdo con esta norma, los archivos dedicados o DF contienen todos los datos referentes a una determinada aplicación y también pueden incluir instrucciones específicas para esa aplicación ASC (*Application Specific Code*).

El DF posee un área donde almacena el archivo ejecutable que es administrado por el sistema operativo. Cada vez que se selecciona un DF se envía una orden, el sistema comprueba si dicha instrucción pertenece al conjunto ASC, en caso afirmativo se ejecuta el programa almacenado. En el caso de que la instrucción no pertenezca a la aplicación actual, el sistema operativo ignora la orden.

3.5 SEGURIDAD

La seguridad es básicamente la protección de un bien valioso para asegurar que no sea robado, perdido o alterado. La seguridad de la información es la aplicación de procedimientos para reforzar la privacidad de los datos en el manejo de su almacenamiento y distribución; además, maneja un amplio rango de aplicaciones y es muy importante debido al rápido avance de la tecnología. La combinación de varios elementos de seguridad es obligatoria para proporcionar un alto nivel de protección contra fraudes y otros riesgos.

3.5.1 Criptografía

La palabra criptografía deriva de "cripto" (oculto) y "grafos" (escritura), su objetivo es garantizar la privacidad y autenticidad del mensaje y del emisor. La criptografía es la implementación de funciones de seguridad por medio de algoritmos matemáticos y busca resolver tres problemas básicos: la confidencialidad, la integridad y la autenticación.

3.5.2 Algoritmos de cifrado

La técnica de cifrado se basa en un algoritmo de cifrado y una llave, de tal forma que se requieren ambos para generar el cifrado a partir de un texto. Para descifrar, se necesitan un algoritmo de descifrado y una llave de descifrado. La seguridad de las técnicas criptográficas actuales no se basa en la ocultación del algoritmo de cifrado/descifrado, que es público, sino en la ocultación de la llave de cifrado/descifrado.

Un algoritmo criptográfico es un mecanismo que permite convertir un texto legible en otro cifrado o ilegible. Se pueden clasificar en dos divisiones: cifrados matemáticamente seguros y cifrados impracticables. Un algoritmo es matemáticamente seguro, cuando se ha demostrado formalmente que es imposible obtener el texto legible a partir del cifrado sino se conoce la llave.

Un algoritmo es impracticable, si los requisitos de potencia de cálculo y de tiempo no permiten obtener el mensaje legible a tiempo para que la información sea útil al atacante. Dentro de la primera división sólo existe el algoritmo OTP (*One Time Pad*) y además existe la demostración que cualquier algoritmo que sea matemáticamente seguro es equivalente al OTP. Para la segunda clasificación se encuentran todos los algoritmos modernos, como el RSA (Rivest, Shamir, Adleman) y el DES (*Data Encryption Standard*).

Los algoritmos de cifrado, por el número de llaves que maneja, pueden dividirse en cifrado simétrico y cifrado asimétrico.

3.5.3 Cifrado simétrico

El cifrado simétrico se caracteriza por poseer un único algoritmo de cifrado/descifrado y por una sola "llave secreta" para cifrar y descifrar (ver Figura 3.10). Esto implica que la llave tiene que permanecer oculta y ser compartida por el emisor y el receptor, lo que significa que se debe distribuir en secreto y se necesita una llave para cada par de interlocutores. El algoritmo simétrico más conocido es el DES (*Data Encryption Standard*).

El DES fue inventado en 1974 por IBM, llegando a ser un algoritmo estándar. Este fue modificado de acuerdo a las recomendaciones de la NSA (*National Security Agency*). El algoritmo ha sido estudiado por criptógrafos cerca de 20 años; durante este tiempo ningún método ha sido publicado que describa la forma de romper el algoritmo, excepto técnicas de fuerza bruta, es decir, probar todas las posibles llaves hasta encontrar la correcta. Este estándar tiene una llave de 56 bits, lo cual ofrece 2^{56} o $7.205X10^{16}$ posibles combinaciones.

Figura 3.10 *Cifrado simétrico (llave secreta)*

La causa de la desconfianza en el uso de este algoritmo se encuentra en las bases iniciales en las que se estableció el diseño del mismo. Estudios realizados pronosticaron que se podría diseñar una máquina especial con más de un millón de chips, la cual podría destruir el sistema en un sólo día.

3.5.4 Cifrado asimétrico

El cifrado asimétrico se caracteriza por la existencia de dos llaves independientes para cifrar y descifrar, mostradas en la Figura 3.11. Esta independencia permite al receptor hacer pública la llave de cifrado, de tal forma que cualquier entidad que desee enviarle un mensaje pueda cifrarlo y enviarlo. La llave de descifrado permanece secreta, por lo que sólo el receptor legítimo puede descifrar el mensaje.

Ni siquiera el emisor es capaz de descifrar el mensaje una vez cifrado. La llave de cifrado se puede distribuir con menos problemas que las llaves simétricas, y sólo se necesita un par de llaves, una pública para cifrar y una privada para descifrar, por cada interlocutor. Estas llaves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una llave a partir de la otra.

Figura 3.11 *Cifrado asimétrico (llave pública)*

El algoritmo asimétrico más conocido es el RSA, su nombre se debe a las iniciales de sus tres inventores, Ron Rivest, Adi Shamir y Leonard Adleman, los cuales crearon el algoritmo en 1978. La seguridad del RSA se basa en la resolución del problema matemático complejo de la factorización de grandes números, ya que el par de llaves pública-privada se obtiene a partir de un par de números primos grandes. Para que el RSA sea efectivo, se requieren longitudes de llaves del orden de 100 a 200 dígitos e incluso mayores.

3.5.5 Seguridad en las tarjetas inteligentes

La capacidad para proteger un sistema completo es una de las ventajas de las tarjetas inteligentes sobre otras alternativas. Algunas características de seguridad utilizadas cuando la TI está en operación incluyen los procesos de autenticación externa, autenticación interna y el envío de mensaje seguro.

La autenticación externa es la autenticación de una entidad externa a una tarjeta inteligente. La tarjeta inteligente y la entidad externa establecen un protocolo de prueba-respuesta como se muestra en la Figura 3.12 y se explica a continuación.

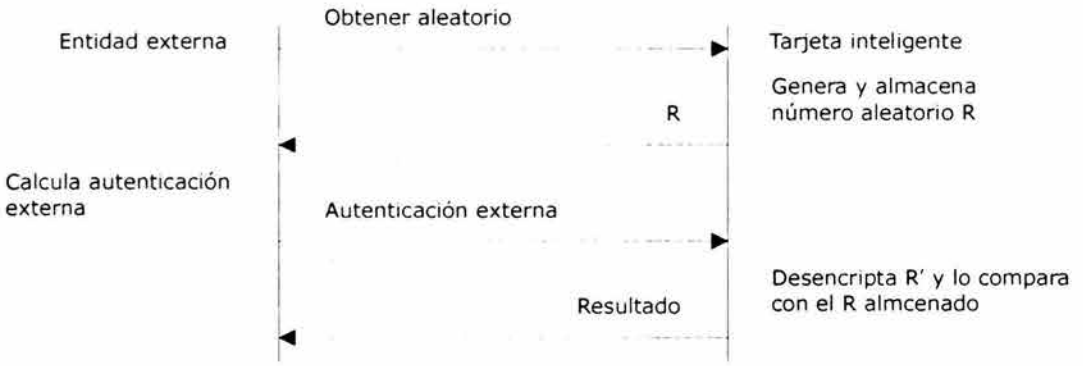


Figura 3.12 *Autenticación externa*

La entidad externa obtiene una prueba, típicamente un número aleatorio, de la tarjeta inteligente y lo encripta con una llave compartida entre la tarjeta y la entidad externa.

1. La entidad externa solicita un número aleatorio R a la TI mediante el envío del comando correspondiente.
2. La tarjeta inteligente crea un número aleatorio R, lo almacena y lo regresa como respuesta a la entidad externa.
3. La entidad externa usa la llave criptográfica correspondiente a la llave criptográfica inteligente para encriptar R. Envía un comando de autenticación conteniendo el número aleatorio encriptado a la tarjeta.
4. La tarjeta recibe el comando de autenticación y desencripta el número aleatorio encriptado contenido en el comando. Si el resultado es igual al número aleatorio R almacenado, la tarjeta inteligente asume que la entidad externa es auténtica.

Los algoritmos criptográficos pueden ser simétricos como DES o algoritmos de llave pública como RSA o DSA. En caso de algoritmos simétricos, la entidad externa y la tarjeta

inteligente deben compartir una llave secreta. Si se utilizan algoritmos de llave pública, la entidad externa usa la llave privada correspondiente a la llave pública que será utilizada para la validación en la TI.

La autenticación interna es la autenticación de una tarjeta inteligente a una entidad externa, la TI y la entidad externa llevan a cabo el siguiente protocolo (ver Figura 3.13).

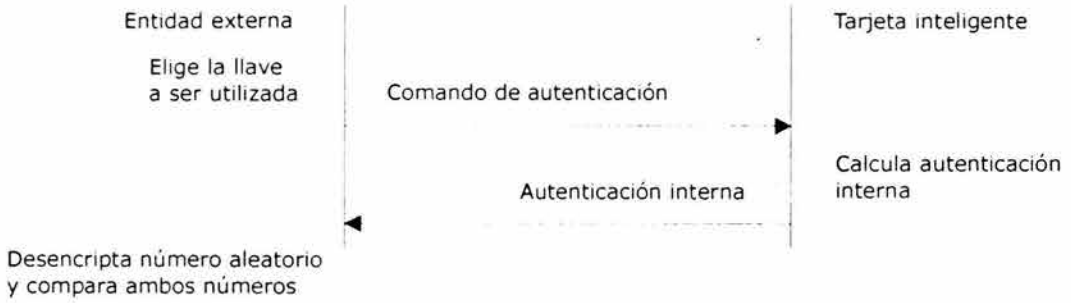


Figura 3.13 *Autenticación interna*

1. La entidad externa envía un comando de autenticación conteniendo un número aleatorio R y un número de llave N, especificando la llave que será utilizada por la tarjeta inteligente.
2. La TI encripta el número aleatorio R recibido de la entidad externa usando la llave de autenticación con el número N y envía de regreso el número aleatorio encriptado.
3. La entidad externa desencripta el número aleatorio encriptado usando la llave criptográfica correspondiente a la llave que fue usada en la tarjeta inteligente, si el resultado es igual a R, la entidad externa asume que la TI es auténtica.

Si se utilizan algoritmos simétricos la entidad externa y la TI deben compartir una llave secreta. Si se utilizan algoritmos de llave pública la entidad externa usa la llave pública correspondiente a la llave privada usada en la TI.

El envío del mensaje seguro incluye varios conceptos diferentes en las tarjetas inteligentes. Los mensajes pueden ser protegidos con un Código de Autenticación de Mensaje o MAC (*Message Authentication Code*), también pueden ser protegidos con un MAC y además ser encriptados.

Para el cálculo del MAC o el encriptamiento de los datos transferidos pueden ser usadas directamente claves secretas compartidas por la entidad externa y la TI o se pueden establecer claves por sesión. De toda la gama de posibles esquemas los más representativos son las operaciones en modo protegido, y las operaciones en modo protegido y encriptado.

3.5.5.1 Operaciones en modo protegido

Este es un esquema simple en el que la tarjeta inteligente y la entidad externa que está accediendo a ella comparten una llave común la cual es utilizada para calcular el MAC sobre los datos transmitidos. El propósito del MAC es asegurar la integridad y autenticidad de los mensajes enviados. La Figura 3.14 muestra como trabaja este esquema cuando se leen datos de una tarjeta inteligente con un archivo de sistema.

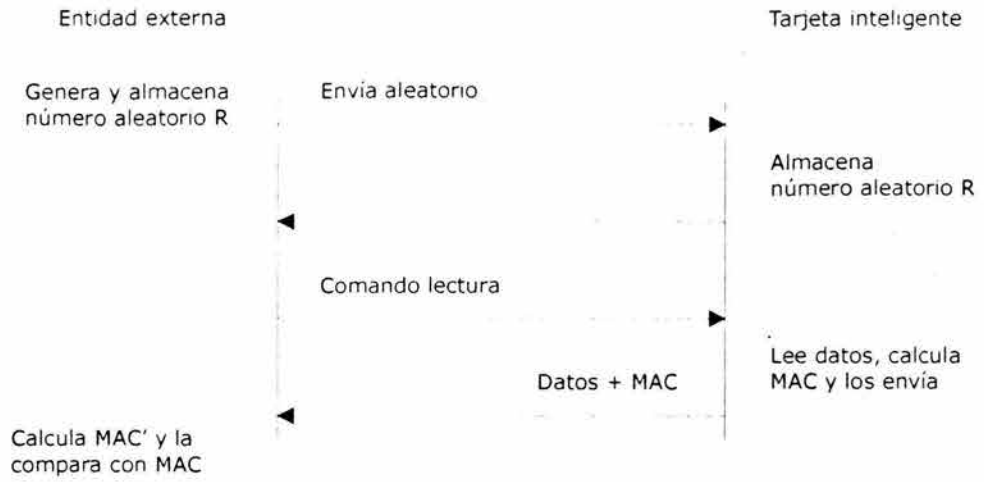


Figura 3.14 *Operación de lectura en modo protegido*

1. La entidad externa genera un número aleatorio R y lo envía a la tarjeta inteligente como prueba mediante el envío del comando apropiado.
2. La tarjeta inteligente almacena el número aleatorio R y envía una respuesta indicando que ahora tiene un número aleatorio para ser utilizado por los comandos siguientes.
3. La entidad externa envía un comando para leer datos de una longitud específica, de un archivo determinado, empezando en un índice establecido en modo protegido.
4. La tarjeta inteligente recibe el comando de lectura y obtiene los datos deseados del archivo guardados en el depósito permanente de la tarjeta. La TI utiliza la llave K y el número aleatorio R para calcular el MAC sobre los datos. La TI envía los datos y el MAC de regreso a la entidad externa en respuesta.
5. La entidad externa recibe los datos leídos y el MAC de la tarjeta inteligente. La entidad calcula el MAC sobre los datos recibidos utilizando la llave K, que debe ser la misma que tiene la tarjeta, junto con el número aleatorio R generado en el paso 1. Sólo si ambos MAC son iguales los datos son aceptados.

Un método similar puede proteger los datos enviados a la tarjeta como se muestra en la Figura 3.15.

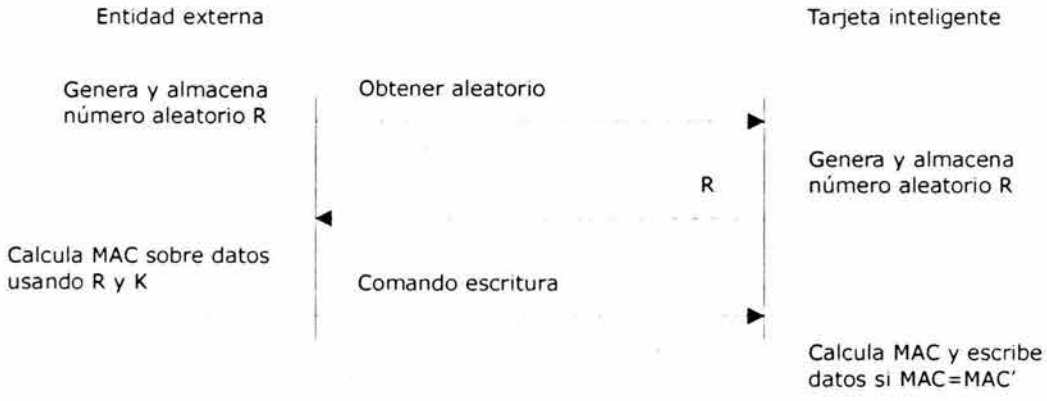


Figura 3.15 *Operación de escritura en modo protegido*

1. La entidad externa solicita una prueba aleatoria de la tarjeta inteligente enviando el comando apropiado a la TI.
2. La tarjeta inteligente genera un número aleatorio R, lo almacena y envía una respuesta conteniendo el número R.
3. La entidad externa calcula un MAC sobre la cabecera del comando de escritura APDU y los datos que serán escritos en la tarjeta inteligente. Para el cálculo utiliza la prueba aleatoria R recibida de la tarjeta inteligente y la llave que concuerda con la llave que protege el archivo en la tarjeta. La entidad externa construye el comando completo con la cabecera del comando APDU, los datos y el MAC, y lo envía a la tarjeta inteligente.
4. La TI recibe el comando de escritura, calcula el MAC sobre la parte relevante de la cabecera del comando APDU y los datos contenidos utilizando el número aleatorio R y la llave. Si el MAC que calcula coincide con el MAC contenido en el comando, los datos son escritos en la memoria permanente de la tarjeta.

3.5.5.2 Operaciones en modo protegido y encriptado

En las operaciones en modo protegido y encriptado normalmente la tarjeta inteligente o la entidad externa primero calculan un MAC, después se lo adicionan a los datos y los encriptan. La Figura 3.16 muestra la operación de lectura.

Figura 3.16 *Operación de lectura en modo protegido y encriptado*

1. La entidad externa genera una prueba aleatoria R y se la envía a la TI mediante el comando apropiado.
2. La tarjeta inteligente almacena el número aleatorio R y envía una respuesta indicando que ahora tiene un número aleatorio para ser utilizado en los comandos subsecuentes.
3. La entidad externa envía un comando para leer datos de una longitud específica, de un archivo determinado, empezando en un índice establecido en el modo encriptado.

4. La TI recibe el comando de lectura y obtiene los datos solicitados del archivo guardado en el almacén permanente de la tarjeta. La tarjeta inteligente utiliza la llave K y el número aleatorio R para calcular un MAC sobre los datos. La TI adicionalmente encripta los datos y el MAC utilizando la misma llave y usa el número aleatorio R como valor inicial de la cadena (para DES-CBC) y envía de regreso la cifra a la entidad externa en respuesta.
5. La entidad externa recibe los datos y el MAC de la tarjeta inteligente como una cifra-texto. Primero desencripta la cifra-texto recibida utilizando la llave que concuerda con la llave y el número aleatorio R; entonces, calcula un MAC sobre los datos recibidos, utilizando la llave K y el número R para verificar la autenticidad de los datos.

La Figura 3.17 muestra la operación de escritura en el modo encriptado.

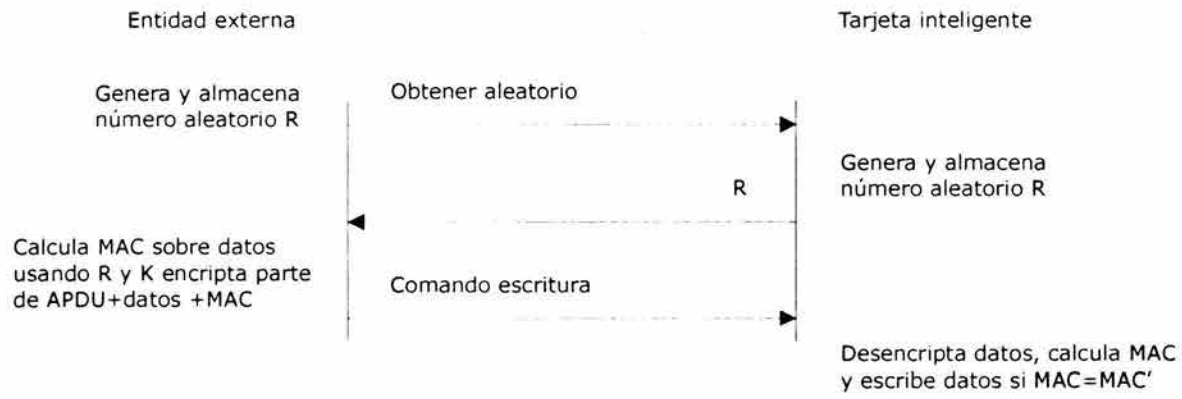


Figura 3.17 *Operación de escritura en modo protegido y encriptado*

1. La entidad externa solicita una prueba aleatoria R de la tarjeta inteligente por medio del envío del comando apropiado a la TI.
2. La tarjeta inteligente genera un número aleatorio R, lo almacena y lo envía de regreso en respuesta.
3. La entidad externa calcula un MAC sobre una parte de la cabecera del comando de escritura APDU y los datos que serán escritos en la tarjeta inteligente utilizando el número aleatorio R y la llave K. Esta llave debe concordar con la llave que protege el archivo en la TI. Entonces, la entidad externa encripta la parte relevante del APDU, los datos y el MAC, y construye un comando completo con estos elementos.
4. La tarjeta inteligente recibe el comando de escritura. Lo desencripta utilizando el número aleatorio R y la llave K apropiada. Calcula el MAC sobre la parte relevante de la cabecera del comando APDU y los datos contenidos utilizando la misma llave K y el número aleatorio R, si esta MAC es igual a la MAC contenida en el comando, los datos son escritos en la memoria permanente de la tarjeta.

Una variante de estos dos esquemas es el que se origina cuando una TI ofrece la posibilidad de establecer una llave de sesión ya sea por una derivación de la llave o generando y transfiriendo una llave de sesión utilizando una llave pública para la encriptación de la llave de sesión. La Figura 3.18 muestra como trabaja la derivación de la llave.

1. La entidad externa envía un comando para establecer una llave de sesión a la tarjeta inteligente.
2. La TI genera un número aleatorio R que utiliza para derivar una llave de sesión de una llave maestra establecida y lo envía de regreso a la entidad externa.
3. La entidad externa recibe el número aleatorio R y lo utiliza para derivar una llave de sesión de una llave maestra que comparte con la tarjeta inteligente como un secreto común.

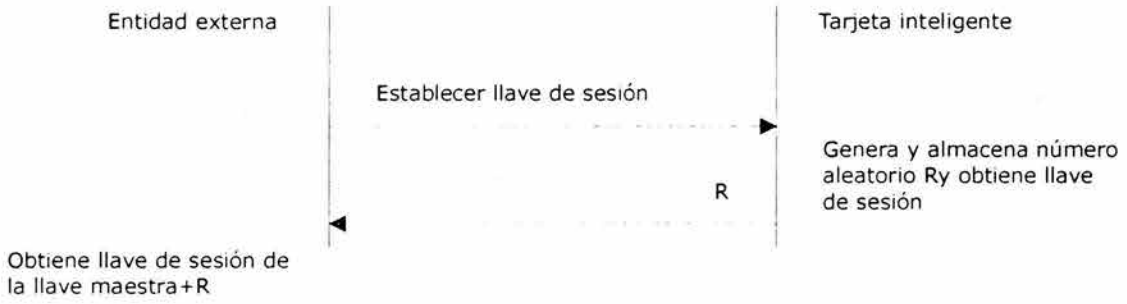


Figura 3.18 *Proceso de obtención de una llave de sesión*

Otra posibilidad para establecer una llave de sesión es utilizar la criptografía de la llave pública para transmitir la llave de sesión como se muestra en la Figura 3.19.

Figura 3.19 *Proceso de obtención de una llave de sesión utilizando la llave pública*

1. La entidad externa genera una llave de sesión, la encripta utilizando una llave pública que concuerda con la llave privada K en la tarjeta inteligente y la envía a la tarjeta.
2. La tarjeta inteligente desencripta la llave de sesión utilizando la llave privada apropiada e indica el suceso.

3.6 INTEGRACIÓN EN LA PLATAFORMA WINDOWS

La necesidad de una mejor seguridad y privacidad en la información ha incrementado las maneras de identificación electrónica sustituyendo a las formas tradicionales.

El surgimiento global del Internet y la expansión de redes corporativas que permiten el acceso de usuarios, clientes y proveedores ha acelerado la demanda para soluciones basadas en infraestructura de llave pública.

Algunos ejemplos que hacen uso de este tipo de tecnología son las firmas digitales, que permiten garantizar la integridad y confidencialidad, así como la autenticación de un usuario a un servidor y viceversa. Las tarjetas inteligentes se han convertido en una aplicación importante en la autenticación de la información, los mensajes y la tecnología de llave pública.

3.6.1 PC/SC (*Personal Computer/Smart Card Workgroup*)

La incompatibilidad entre las tarjetas inteligentes, los lectores y sus aplicaciones había llegado a ser la razón principal para su escasa aplicación fuera de Europa.

Es por ello, que las compañías más grandes de cómputo y de tarjetas, Groupe Bull Transac, Gemplus, Hewlett-Packard, IBM Corporation, Microsoft, Schlumberger, Siemens Nixdorf Information Systems, Sun Mycrosystems, Toshiba y Verifone desarrollaron el modelo estándar PC/SC (*Personal Computer/Smart Card Workgroup*) que facilita la integración de tecnología para TI's en plataformas basadas en computadoras personales.

Microsoft anunció en 1998 la decisión de integrar la tecnología de las TI's dentro de todos sus sistemas operativos. Hoy en día, se encuentran los controladores (*Plug and Play*) para las versiones de Windows 95, 98, Millennium Edition, y NT disponibles de forma gratuita en el Web; mientras que para Windows 2000 y XP ya están incluidos en el propio sistema.

De esta manera, se pueden crear aplicaciones de manera sencilla y sin tener que conocer en profundidad el funcionamiento de las tarjetas gracias a las API's (*Application Programming Interfaces*) que son herramientas suministradas por Microsoft en sus sistemas.

Desde el punto de vista del desarrollo de aplicaciones, existen tres mecanismos para tener acceso a los servicios admitidos por una tarjeta inteligente: CryptoAPI, API Win32 y Scard COM, los cuales son descritos en la Tabla 3.3. El mecanismo elegido depende del tipo de aplicación y de las capacidades específicas de la tarjeta.

Mecanismos	Descripción
CryptoAPI	Es la API de encriptado que se utiliza para crear un proveedor de servicios de cifrado o CSP (*Cryptographic Service Provider*) y requiere un kit de desarrollo independiente, disponible en Microsoft. Las ventajas de utilizar CryptoAPI son significativas porque el desarrollador puede aprovechar las características de encriptación integradas en la plataforma de Windows sin necesidad de tener conocimientos de cifrado o saber cómo funciona un algoritmo de encriptado en particular.
Scard COM	Es una implementación de interfaz sin cifrado para acceder a servicios basados en tarjetas inteligentes desde aplicaciones escritas en lenguajes diferentes, tales como C, Microsoft Visual C++, Java y Microsoft Visual Basic. El desarrollador de software puede utilizar las herramientas de desarrollo estándar, como Visual C++ y Visual Basic, para implementar aplicaciones y proveedores de servicios habilitados para las TI's y compatibles con éstas. En general, el desarrollador de la aplicación no necesita conocer los detalles del funcionamiento de una TI determinada para acceder a sus servicios a través de COM. Esto acelera el desarrollo de aplicaciones Windows ya que reduce el tiempo y el costo de desarrollo y protege a las aplicaciones de la obsolescencia causada por cambios posteriores en el diseño de una tarjeta.
API Win32	Son las API básicas para tener acceso a las tarjetas inteligentes, para utilizarlas de forma eficaz requieren un conocimiento más profundo de las tarjetas inteligentes y del sistema operativo Windows. También, proporcionan mayor flexibilidad a las aplicaciones para controlar los lectores, tarjetas y otros componentes relacionados. Cuando se requiere un máximo control sobre el uso de una aplicación de las TI's, esta extensión a la API básica de Win32 proporciona las interfaces necesarias para administrar interacciones con dispositivos de las tarjetas inteligentes.

Tabla 3.3 *Descripción de los mecanismos API's.*

La arquitectura definida por el grupo de trabajo PC/SC puede verse en la Figura 3.20, sus secciones serán descritas a continuación.

- **Lector de tarjetas**

Este dispositivo es el encargado de enlazar físicamente los contactos de la tarjeta con la PC. También es capaz de alimentar eléctricamente los circuitos internos que están incrustados en la TI, así como suministrar una señal de reloj estable a la misma.

Para su instalación, algunos lectores han sido incluidos en el sistema operativo Windows 2000 (ver Tabla 3.4), en caso contrario, se debe utilizar el disco de instalación proporcionado por el fabricante.

Fabricante	Lector de tarjetas	Interfaz
Bull CP8	Smart TLP3	RS-232
GemPlus	GCR410P	RS-232
GemPlus	GPR400	PCMIA
Litronic	220P	RS-232
Rainbow Technologies	3531	RS-232
SCM Microsystems	SwapSmart	RS-232
SCM Microsystems	SwapSmart	PCMIA

Tabla 3.4 *Lectores de Tarjetas Inteligentes reconocidos por Windows 2000.*

- **Administrador del lector**

Consiste en el software a bajo nivel que debe adaptarse a todas las características del puerto usado para conectar la computadora al lector; además, proporciona la capacidad para acceder a las funciones del mismo.

Las interfaces comunes permiten que un dispositivo lector sea desarrollado de manera uniforme y ser accesible en todas las aplicaciones de Windows. En otras palabras, el administrador de la terminal o el lector consiste en la implementación del software de los protocolos de la transmisión definidos en el estándar ISO 7816.

- **Administrador de recursos**

Es el responsable de administrar los recursos referentes a las TI's y el sistema, y también de controlar los accesos sobre dichas tarjetas. Este componente de la arquitectura es proporcionado normalmente por el fabricante del sistema operativo; asimismo, debe existir un sólo administrador de recursos por cada sistema.

El Administrador de Recursos realiza las siguientes tareas:

- Identificar y direccionar los lectores instalados.
- Enlazar los distintos tipos de tarjetas inteligentes y sus proveedores de servicios asociados.
- Habilitar operaciones primordiales de acceso disponibles en una tarjeta, permitiendo ejecutar múltiples comandos sin interrupción, garantizando que la información no sea dañada.
- Controlar eventos tales como la introducción o extracción de una tarjeta.
- Localizar la tarjeta insertada y relacionarla con la aplicación correspondiente.

- **Proveedor de Servicios y Aplicaciones**

Es el responsable de encapsular las funciones suministradas por una tarjeta específica y hacerlas accesibles a través de interfaces de programación de alto nivel.

El proveedor de servicios está dividido en dos componentes:

- Proveedor de servicios de la tarjeta.
- Proveedor de servicios de encriptamiento.

Sólo las tarjetas que incorporen funciones encriptadas deberán disponer de un proveedor de servicios de encriptamiento. Cada aplicación deberá conocer qué proveedor de servicios debe usar; sin embargo, dicha aplicación puede también determinar, mediante el administrador de recursos, que proveedor desea usar.

Desde el punto de vista del usuario que va a realizar aplicaciones en Windows usando TI's, la parte más importante de la estructura general es la del proveedor de servicios. Las partes que están por debajo de ésta son diseñadas por el fabricante del lector y de las tarjetas. La importancia radica en que la aplicación desarrollada usará las posibilidades que le brinda el proveedor de servicios para utilizar la tarjeta inteligente de manera eficiente.

La característica principal que debe tener el proveedor de servicios es la de poder ser usado por cualquier plataforma de programación bajo el entorno Windows, esto implica el uso de API's. Éstas no las proporciona el fabricante del lector o de la tarjeta, sino que Microsoft las ha integrado en su sistema operativo y son las mismas para todos los lectores y tarjetas que siguen las especificaciones del grupo PC/SC, facilitando así la creación de software basado en tarjetas inteligentes.

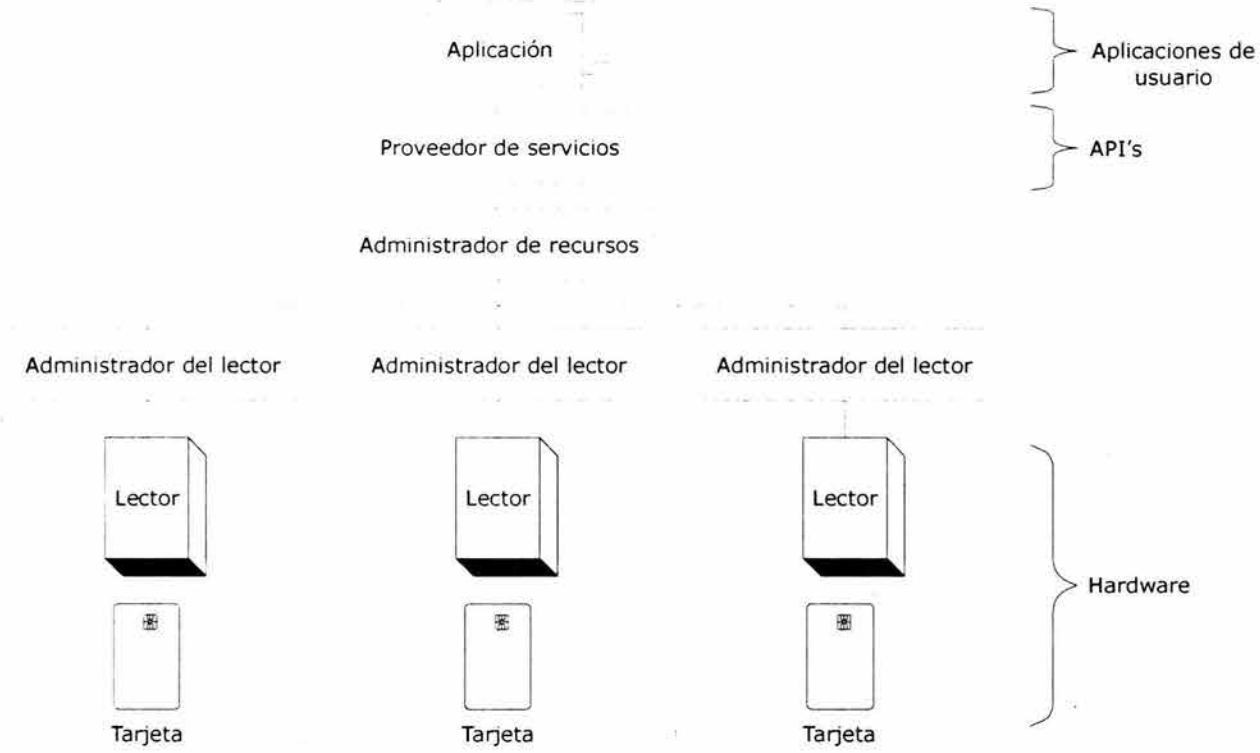


Figura 3.20 *Arquitectura general del estándar PC/SC.*

3.6.2 Ventajas de la plataforma Windows

Actualmente, la mayoría de las redes de computadoras son configuradas requiriendo una contraseña a través de la pantalla de inicio de sesión. La contraseña es el mecanismo de seguridad más ampliamente utilizado, pero es insegura debido al manejo propio del usuario. Por ejemplo, algunas personas eligen contraseñas que puedan recordar con facilidad, lo que convierte su uso en un método de seguridad relativamente vulnerable.

También, si el usuario no protege correctamente la contraseña y si alguna persona ajena la obtiene, puede utilizarla para ingresar indebidamente a la red, pudiendo ocasionar daños a la información. Además, la contraseña se envía a través de una línea de comunicación a un servidor principal para su verificación, la cual puede ser relativamente fácil de interceptar.

El inicio de sesión en una red con una tarjeta inteligente proporciona un medio seguro para la autenticación y autorización de un usuario, ya que utiliza un sistema de identificación criptográfica y constituye una prueba de posesión cuando se acredita a un usuario de un dominio. Solamente el usuario debe insertar la tarjeta en el dispositivo lector e ingresar el número de identificación personal PIN, en lugar de escribir el nombre de usuario, la contraseña y el dominio.

Es importante mencionar que el PIN está almacenado en el microprocesador de la tarjeta inteligente, por lo cual, éste no es enviado al servidor principal. Para que una persona ajena pudiera acceder a la red, tendría que obtener la tarjeta inteligente y el PIN del usuario, lo cual reduce las posibilidades de que se produzca un daño, ya que se requieren más elementos. Otra de las ventajas es que si se escribe varias veces un PIN incorrecto, la tarjeta se bloquea, lo que dificulta enormemente un acceso indebido. El número permitido de intentos no válidos de inicio de sesión antes del bloqueo varía según el fabricante de la tarjeta inteligente.

Si la tarjeta es extraviada o robada, nadie puede utilizarla para acceder a la red porque solamente el propio usuario conoce el mecanismo de autenticación (por ejemplo, el PIN correspondiente). Igualmente, la información contenida en la tarjeta no se pierde porque puede ser replicada, es decir, cuando una tarjeta reemplazada es activada e insertada dentro del lector, la información anterior es transferida a la nueva tarjeta.

Por lo anterior, las tarjetas inteligentes son un componente importante de la infraestructura de llave pública que Microsoft ha estado integrando dentro de la plataforma Windows, porque garantizan mecanismos de seguridad, tal como la autenticación de un cliente, inicio de sesión y seguridad en el correo electrónico.

Las tarjetas inteligentes son esencialmente un punto de convergencia para los certificados de llave pública y las llaves asociadas. En conclusión:

- Proporcionan una excelente protección para claves privadas y otras formas de información personal.
- Aíslan del resto del sistema puntos de seguridad críticos, como la autenticación, firmas digitales y claves de intercambio.
- Permiten portabilidad de credenciales e información privada entre computadoras.

3.7 INTEGRACIÓN EN LA PLATAFORMA JAVA

Las tarjetas inteligentes, en general, tienen algunas limitantes como la escasa portabilidad de aplicaciones y flexibilidad para descargarlas. La tarjeta Java Card es una TI que puede ejecutar programas de Java, lo cual, permite agregar o remover aplicaciones de cualquier tipo. Por lo tanto, en una sola tarjeta se puede tener más de una sola aplicación. La API para Java Card fue desarrollada en Noviembre de 1996, por Schlumberger. En los siguientes años, JavaSoft una subsidiaria de Sun Microsystems registró la API Java Card 2.0, llegando a ser la especificación más aceptada en la industria.

El programa ejecutable de la tarjeta consiste de códigos de bytes que son interpretados por el Environment Runtime Java Card, el cual controla la ejecución de diferentes aplicaciones además de impedir que interfieran entre sí. Estrictamente hablando, Java Card es una plataforma pero no es un sistema operativo para tarjetas inteligentes. Esta plataforma es soportada por un sistema operativo, el cual no es directamente accesible por las

aplicaciones. Las aplicaciones son escritas para las interfaces y la plataforma Java, la cual usa los servicios del sistema operativo de otra manera.

3.8 SISTEMAS OPERATIVOS EN EL MERCADO

La mayoría de los fabricantes de TI's tienen sus propias versiones de sistemas operativos; sin embargo, algunos de ellos autorizan sistemas de otras compañías, de esta forma se tiene un margen para extender y modificar comandos y aplicaciones para diferentes propósitos; en la Tabla 3.5 se aprecia la lista de algunas compañías que diseñan este tipo de sistemas operativos.

Fabricante	Sistema operativo
Bull	SmarTB, CC, Odyssey I (JavaCard)
DeLaRue	DS, DX, DXPLUS, CC, Mondex Card, JavaCard
Gemplus	PCOS, MPCOS, GemVersion, GemXpresso(JavaCard)
Giesecke & Devrient	Starcos S, Starcos PK, Starcos X
ORGA	ICC
Schlumberger	ME2000, PayFlex, Multiflex, Cryptoflex, Cyberflex (JavaCard)
Siemens	Card OS
Advanced Card Systems	ACOS
AMMI	AMOS
Digicash	Blue
Datakey	DKCCOS
Obethur	Host
Incard	Ios
Gis	Isos
Protekila	Procos
Spyrus	Spycos

Tabla 3.5 *Fabricantes de sistemas operativos*

Dispositivos de Interfaz

- Lectores
- Terminales
- Protocolo de comunicación de datos
- Fabricantes

Capítulo 4

CAPÍTULO 4. DISPOSITIVOS DE INTERFAZ

Para escribir y leer datos en una tarjeta inteligente es necesario disponer de una conexión física. Existe una gran variedad de dispositivos disponibles en el mercado, los cuales se pueden dividir en dos grupos:

- Lector. Básicamente, es un conector que permite el enlace físico entre una tarjeta inteligente y el dispositivo que se comunica con la misma, por ejemplo, una computadora central. La industria de las tarjetas inteligentes ha tomado la convención de denominar lector a una unidad que se conecta con una PC para la mayoría de las necesidades de procesamiento.
- Terminal. Es un dispositivo con capacidades para procesar información y puede operar sin que sea conectado a otro elemento.

4.1 LECTORES

El lector energiza la tarjeta, la inicializa y actúa como mediador entre ésta y la computadora central. La tarjeta se energiza mediante las terminales del micromódulo de contactos insertado en la misma, o bien, por medio de la inducción de corriente a través de una antena, como es el caso de las tarjetas sin contactos. La inicialización es un protocolo preestablecido que cualquier tarjeta debe efectuar. Todos los lectores de TI's permiten la inicialización de cualquier tipo de tarjeta, pero no todos soportan la tarjeta una vez que ésta se ha conectado con alguna aplicación.

Los lectores permiten a los usuarios la realización de lectura, escritura y ejecución de todas las funciones correspondientes a la seguridad, así como modificar, analizar y monitorear el estado de las tarjetas. Las TI's dependen de estos dispositivos para el envío y recepción de información del usuario; asimismo, facilitan el desplegado de los datos de salida.

Las funciones que se realizan entre el lector y una tarjeta inteligente son:

1. Conexión. En un sistema de tarjetas con contactos, la tarjeta se inserta en el dispositivo de lectura. Las tarjetas inalámbricas sólo requieren aproximarse al lector.
2. Autenticación de la tarjeta. La tarjeta genera un mensaje al lector que confirma que es una tarjeta válida. El mensaje puede estar encriptado por razones de seguridad. El lector puede verificar la tarjeta contra una lista de tarjetas robadas y si es necesario retenerla para que no sea usada nuevamente.
3. Autenticación del lector. El lector envía un mensaje a la tarjeta el cual es verificado contra códigos programados previamente para establecer si el lector es válido. Si la tarjeta no reconoce al lector como válido, puede evitar la lectura de la información contenida en ella.
4. Selección de la aplicación. Una TI puede soportar diferentes aplicaciones interrelacionadas o independientes. La aplicación puede ser seleccionada por el usuario de la tarjeta o en forma automática por el lector, dependiendo del método de autenticación inicial.
5. Requerimientos de identificación de seguridad. La tarjeta es capaz de definir los requerimientos de seguridad para la aplicación seleccionada y puede imponer diferentes niveles de seguridad para distintos propósitos, personas u organizaciones.

6. Autenticación del usuario. Esto puede ser realizado solicitando al usuario el ingreso de un PIN o con algún tipo de información biométrica. La tarjeta guarda en un área secreta la información relevante para realizar la comparación, sin divulgar al usuario los datos contenidos para el procedimiento de autenticación.
7. Transacción. Es generada por una entrada manual o un proceso automático. La tarjeta verifica y autoriza la transacción.
8. Registro de la transacción. La tarjeta genera un registro de la transacción y lo transmite electrónicamente al lector. El registro puede ser utilizado en otra parte del sistema, por ejemplo, para permitir al proveedor de servicios realizar el cargo al banco por el pago de un servicio, a un tercero para propósitos estadísticos, o como respaldo de la información almacenada en caso de que la tarjeta sea dañada o extraviada.
9. Comprobante. Un registro en papel, como un recibo, puede ser generado por el lector para el usuario de la tarjeta o el proveedor del servicio.

Un lector puede escribir y leer datos en la tarjeta, por lo cual se refiere a ellos como dispositivos de lectura-escritura. Otros nombres que se pueden encontrar para estos elementos son: unidad de lectura-escritura, unidad de contacto, dispositivo para tarjetas con chip (CAD, *Chip Card Accepting Device*), lector de tarjetas con chip (CCR, *Chip Card Reader*) o dispositivo de interfaz (IFD, *Interface Device*).

Existe una gran diversidad de lectores, y sus capacidades varían de acuerdo a las necesidades de los usuarios. Los lectores pueden ser de contactos, inalámbricos, con teclado, sin teclado, con pantalla o sin ella.

4.1.1 Tipos de lectores

Existen diferentes tipos de lectores de tarjetas inteligentes que por sus características físicas se dividen en:

- Lector portátil de saldo.
- Lector conectado a una PC.
- Lector modular.
- Lector híbrido.

Otra clasificación puede hacerse de acuerdo con la interfaz eléctrica utilizada entre la tarjeta y el lector, estos pueden ser:

- Lector de tarjetas con contactos.
- Lector de tarjetas sin contactos o inalámbricos.

Este último tipo de lectores se detallan más adelante en el inciso 4.1.2.2.

4.1.1.1 Lector portátil de saldo

Están preprogramados para leer el monto de un monedero electrónico o de una tarjeta telefónica, por lo cual, son llamados también lectores de balance y su costo es muy bajo. Pueden incluir funciones adicionales como el desplegado de las últimas transacciones de débito/crédito o recarga realizadas. En la Figura 4.1, se muestra un ejemplo de este tipo de lector.

Figura 4.1 *Lectores portátiles de saldo*

4.1.1.2 Lector conectado a una PC

Estos lectores compactos son diseñados para ser conectados a una computadora portátil o de escritorio. Existen en el mercado diferentes tipos dependiendo del puerto de comunicación al que se conecten. Pueden ser energizados mediante una batería interna, el puerto serial o un adaptador externo. En la Tabla 4.1, se muestran las ventajas y desventajas de los diferentes lectores.

Conexión Física	Ventajas	Desventajas
Puerto Serial	Muy común, robusto, barato. Soporta varios sistemas operativos (Windows, Mac, Unix)	Muchas computadoras no tienen puertos seriales libres. Requieren un adaptador de corriente externo o baterías.
PCMCIA	Excelente para usuarios de computadoras portátiles.	Pueden ser un poco más costosos. Muchas computadoras de escritorio no tienen puertos PCMCIA.
PS/2 Teclado	Fácil de instalar con un adaptador. Soporta la protección del PIN.	Baja velocidad de comunicación.
Disco flexible	Muy fácil de instalar.	Requiere baterías. La velocidad de comunicación no es muy alta.
USB	Velocidad muy alta de transferencia de datos.	El compartir un bus podría ser un problema de seguridad.
Interconstruido	No necesita hardware o software de instalación	No se adquiere con facilidad.

Tabla 4.1 *Tipos de lectores para PC's*

Se utilizan comúnmente para el control de acceso, personalización de tarjetas y pruebas de diseño. En la Figura 4.2 se muestran algunos ejemplos de este tipo de lectores.

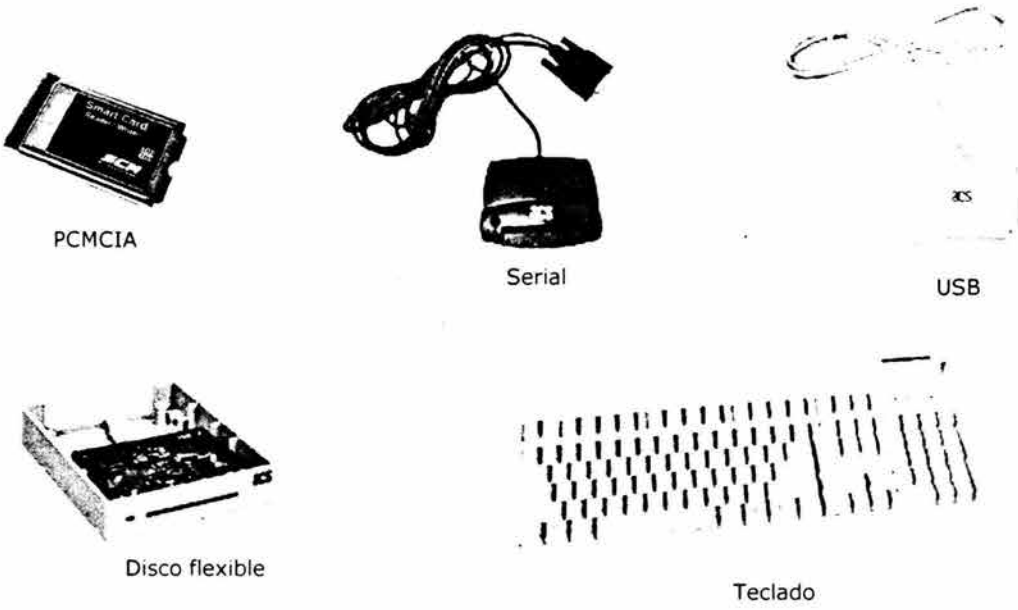


Figura 4.2 *Lectores que se conectan a una PC*

4.1.1.3 Lector modular

Estos lectores cuentan con mecanismos y componentes electrónicos para su integración en diferentes productos, se pueden instalar previa fabricación y diseño en un aparato determinado para cumplir con una función. Estos lectores se pueden encontrar en cajeros automáticos (ver Figura 4.3), máquinas expendedoras, parquímetros, puertas de control de acceso, teléfonos de prepago, etc.

Figura 4.3 *Lector modular de un cajero automático*

4.1.1.4 Lector híbrido

Estos lectores, además de la lectura de TI's, tienen la capacidad de leer tarjetas de banda magnética o tarjetas ópticas. Se utilizan principalmente en cajeros automáticos y kioscos.

4.1.2 Características del lector

Las tarjetas inteligentes, así como sus lectores, se ajustan a un estándar que les permite que, con el software adecuado se pueda acceder a la información de la tarjeta. Esto quiere decir que en un principio no importa el modelo o la marca del lector, pero en la práctica se debe tener en cuenta algunos parámetros como el software empleado, el puerto de conexión en la PC, la velocidad de comunicación y su portabilidad.

La mayoría soportan las siguientes modalidades para detectar la presencia de una tarjeta:

- Detección física. El lector identifica la estructura física de la tarjeta y actúa como un traductor entre la misma y la computadora central. Las tarjetas de memoria requieren esta modalidad porque el lector debe conocer la dirección exacta de la información.
- Detección genérica. El lector conoce la estructura lógica de la tarjeta y transfiere comandos de la computadora central a la tarjeta. Las tarjetas con microprocesador utilizan la detección genérica ya que tienen su propio sistema operativo, así como la lógica para interpretar los comandos.

Los lectores permiten la lectura de los campos de los archivos almacenados en la tarjeta y, de igual forma, autorizan la modificación de aquellos campos protegidos contra escritura. La protección de los archivos contra escritura puede ser a través de una clave maestra, mediante el PIN del usuario o por medio del SAM (*Security Application Module*).

4.1.2.1 Características de la interfaz física

Los lectores se conectan a interfaces periféricas estándar, como el puerto serial RS-232, PS/2, PCMCIA, puerto USB, ranuras para disco flexible, puerto infrarrojo IRDA (*InfraRed Data Association*) o pueden estar incrustados en teclados. Los lectores se consideran dispositivos estándar, incluyen un descriptor de seguridad e identificador "Plug and Play" y se manejan a través de controladores de dispositivo.

Cuando se inserta una tarjeta en un lector, se debe aplicar energía a los contactos del integrado y una señal de reloj para su operación. Aún cuando las tarjetas de hoy en día poseen un área de contactos estándar de acuerdo con la norma ISO, las primeras tarjetas de pruebas francesas utilizaban el estándar francés, el cual indica una ubicación diferente. Como resultado, algunos lectores de tarjetas tienen dos módulos de contactos.

Un lector de contactos puede tener alguna de las siguientes características:

- Contacto corredizo. Los lectores con contactos corredizos simples tienden a dejar marcas o raspaduras en el área de contacto. Esto afecta seriamente la tarjeta después de algún tiempo de uso y ésta puede requerir varias inserciones para hacer una buena conexión.

- Contacto por presión. Al insertar la tarjeta, se hace un contacto más suave en su superficie por medio de alfileres. Cuando se retira la tarjeta, los alfileres sueltan la presión de manera que hay menos desgaste en sus contactos.
- Despliegue. Algunos lectores tienen una pantalla LCD capaz de desplegar caracteres en líneas y, algunas veces, tienen pantallas más grandes que permiten visualizar gráficos.
- Teclado. El lector puede tener un teclado pequeño muy simple (numérico) o uno más seguro para introducir un PIN y verificarlo directamente con la tarjeta. Éste se sella normalmente junto con un módulo de seguridad encriptado para evitar una brecha en seguridad y no exponer el PIN al exterior. El módulo de seguridad también puede detectar cualquier tipo de ataque. Dependiendo del lector, se pueden programar funciones adicionales.
- Unidades motorizadas. Son lectores sofisticados y más avanzados, utilizados ampliamente en cajeros automáticos, cuentan con unidades electromecánicas para jalar y expulsar la tarjeta en forma automática. Su costo es más elevado de los aparatos simples que usan el método empujar-jalar de forma manual.

4.1.2.2 Interfaz eléctrica

Existen dos métodos para realizar el intercambio de información con los dispositivos periféricos, mediante tarjetas con contactos o con tarjetas inalámbricas.

Una tarjeta con contactos debe conectarse físicamente al lector con el fin de transferir información, mientras que una tarjeta sin contactos utiliza formas avanzadas de transmisión de radiofrecuencia cuando es aproximada físicamente al lector.

Para las TI's con contactos, el consumidor puede elegir entre lectores portátiles o fijos, o dispositivos que se conectan a una PC.

Estos lectores generalmente soportan la transmisión asíncrona, donde el lector es capaz de restaurar la tarjeta y recibir el comando de respuesta. De la misma forma, admiten la transmisión síncrona, donde el lector es capaz de restaurar la tarjeta y entonces leer o escribir datos de la tarjeta una vez realizada su verificación.

Para el caso de las tarjetas sin contactos existen tres tipos de lectores, que se clasifican de acuerdo con la distancia que permite la comunicación entre el lector y la tarjeta, como se muestra en la Tabla 4.2.

Tipo de lector	Distancia entre lector y terminal (mm)
De proximidad inmediata	1
De proximidad cercana	1 - 2
De acoplamiento remoto	3 - 5

Tabla 4.2 *Tipos de lectores para tarjetas sin contactos*

Las tarjetas sin contactos utilizan una sola bobina incrustada para realizar las siguientes funciones:

- Energizar la electrónica de la tarjeta.
- Enviar los datos del lector a la tarjeta
- Enviar los datos de la tarjeta al lector.

El lector de tarjetas inalámbricas se comunica con la TI mediante bajas frecuencias de radio, de 10 MHz a 15MHz. El lector produce un campo magnético de baja frecuencia mediante una antena transmisora, generalmente, en forma de bobina. El campo magnético sirve como portador de energía del lector a la tarjeta, la cual accede este campo mediante una antena incrustada. El lector recupera la señal electromagnética de la TI y la convierte en una señal eléctrica. Una vez que el lector verifica los posibles errores y valida los datos recibidos, la información es decodificada y reestructurada para transmitirla en el formato requerido por la computadora central.

En la Figura 4.4 se muestran las diferentes interfaces eléctricas para las tarjetas inteligentes.

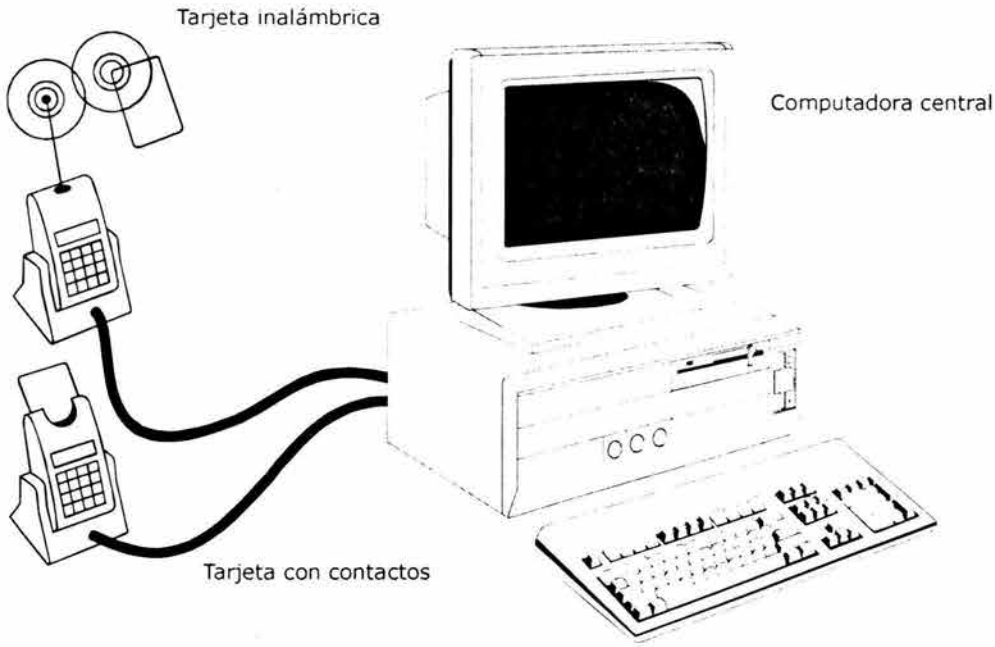


Figura 4.4 *Interfaces eléctricas de las tarjetas inteligentes*

4.2 TERMINALES

Las terminales, también llamadas lectores independientes, tienen su propio procesador y unidad de memoria, además incluyen la lógica requerida para inicializar una tarjeta y actúan como mediador entre la TI y una computadora central. Por ejemplo, la computadora central puede enviar un paquete de información de gran tamaño al lector para que éste a su vez lo envíe a la tarjeta inteligente. La terminal debe verificar el paquete de información y, algunas veces dividirlo en dos o más paquetes antes de enviarlo a la tarjeta. Esto significa que la computadora solamente se encarga de la comunicación con la terminal y no con la tarjeta.

Todas las terminales tienen grabado un microcódigo o sistema operativo pequeño, para manejar diferentes tareas, tales como registrar accesos, procesar comandos e interrupciones, controlar el teclado, la comunicación y el despliegue de datos. El servicio de despliegue en la terminal, el control de mecanismos electromecánicos, la comunicación serial y por módem, son realizados por módulos especializados de E/S bajo el control del sistema operativo.

Las terminales deben manejar diferentes características y códigos encriptados de diversas tarjetas, así como encriptar las comunicaciones con el exterior. Esto se logra con el módulo de seguridad SAM localizado dentro de la terminal. El código de seguridad que se requiere para transacciones se almacena en el módulo SAM o en una tarjeta inteligente más pequeña similar al módulo SIM que se conecta con el módulo SAM. Una terminal puede tener más de un SAM, hasta seis en algunos casos, para ofrecer el servicio a diferentes emisores de tarjetas.

La terminal puede tener aplicaciones programadas, por ejemplo, tomar el pago de una tarjeta inteligente y, más tarde enviar el cargo al banco emisor. El código de aplicación es normalmente cargado en la terminal, utilizando una conexión con alta seguridad del servidor. Los lectores requieren un mayor número de controladores que las terminales, pero su manufactura es más barata y fácil de cambiar. Las terminales, aunque son más caras que los lectores, cuentan con juegos de controladores genéricos para manipular la comunicación entre la terminal y la computadora central.

Algunos ejemplos de terminales, se enlistan a continuación:

- Terminal de propósito general.
- Terminal de monedero electrónico.
- Terminal EFTPOS.

4.2.1 Terminal de propósito general

Estas terminales operan fuera de línea, tienen los módulos de aplicaciones y de seguridad cargados en su memoria programable. Pueden tener acceso telefónico a un sistema central para actualizar una lista de tarjetas robadas o para descargar actualizaciones de software. En la Figura 4.5 se muestra un ejemplo de este tipo de terminal.

Figura 4.5 *Terminal de propósito general*

4.2.2 Terminal de monedero electrónico

Esta terminal es pequeña y portátil, puede funcionar como una terminal fuera de línea, transfiriendo automáticamente el valor del monedero electrónico del usuario a la TI del vendedor, almacenada dentro del módulo SAM de la terminal. Otras funciones normalmente incluyen el desplegado del estado de cuenta y el despliegue de las últimas cinco o diez transacciones. Se utilizan comúnmente en restaurantes, aeropuertos, taxis y transporte público

4.2.3 Terminal EFTPOS (*Electronic Fund Transfer and Point of Sale*)

Las terminales especializadas de transferencia electrónica de fondo y punto de venta, permiten transferencias seguras de fondos para el pago de bienes o servicios desde una tarjeta inteligente. Estas terminales pueden estar equipadas para autorizar el pago vía marcado telefónico o comunicación inalámbrica utilizando una red GSM.

4.3 PROTOCOLO DE COMUNICACIÓN DE DATOS

El protocolo de transmisión entre la tarjeta inteligente y el dispositivo periférico está definido en el estándar ISO 7816/3 y puede ser T=0, protocolo de transmisión de caracter half duplex asíncrono, o T=1, protocolo de transmisión de bloque half duplex asíncrono.

El periférico o dispositivo de interfaz siempre inicia el comando para el protocolo T=0. El mensaje de comandos consiste de un encabezado de cinco caracteres que el dispositivo de interfaz envía al circuito integrado de la tarjeta inteligente.

La tarjeta responde con un byte de procedimiento y, a partir de ese momento, puede ser enviada la información desde o al circuito integrado de la TI en respuesta al comando.

El protocolo T=1 tiene la ventaja, sobre el protocolo T=0, de ser capaz de encadenar los bloques de datos; de manera que, un bloque muy grande puede ser transferido con un sólo comando mediante la transmisión de un número determinado de tramas encadenadas en secuencia. El protocolo T=1 tiene un sistema de manejo de errores más sofisticado que el protocolo T=0.

Como desventaja, el protocolo T=1 requiere de un software complejo cargado en el circuito integrado de la TI y en el dispositivo de interfaz. Adicionalmente, el protocolo T=1 requiere mayor memoria RAM del circuito integrado de la tarjeta para almacenar el último bloque de datos transmitido y utilizarlo en caso de requerir la retransmisión del mismo.

4.4 FABRICANTES

Existen diversos fabricantes de lectores y terminales de tarjetas en el mercado que ofrecen a través del Internet información acerca de sus productos (véase Figura 4.6), tal como características, detalles y, en algunas ocasiones, catálogos electrónicos especializados.

Figura 4.6 *Lector de tarjeta y catálogo electrónico*

En la Tabla 4.3 se presentan las direcciones de algunos productores y proveedores de lectores de TI's.

Fabricante	Página Web
ALPS	www.simpletechnology.com
ASCOM MONTEL	www.ascom.com
Cardom Technology	www.viage.com
Cherry	www.cherrycorp.com
De La Rue Card Technology, Ltd.	www.delarue.com
Gemplus	www.gemplus.com
Giesecke & Devrient America, Inc.	www.gdm.de
Fischer International	www.fisc.com
Hewlett-Packard	www.hp.com
Ingenico	www.ingenico.com
Intellect Holdings Limited	www.intellect.com.au
Innovatron	www.innovatron.com
Litronic Inc.	www.litronic.com
Orga Kartensysteme GMBH	www.orga.com
Schlumberger Cards & Systems	www.slb.com
SCM Microsystems	www.scmmicro.com
Toshiba Information Systems, Inc.	www.toshiba.co.jp
Ultimaco Safeware	www.ultimaco.com
VeriFone	www.verifone.com

Tabla 4.3 *Fabricantes y lectores en el mercado*

4.4.1 Productos existentes en el mercado

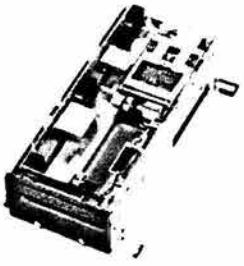
- Fabricante: CARDOM TECHNOLOGY.

La serie KDR-9000/KDM-9000, mostrada en la Figura 4.7, soporta la inserción manual de tarjetas magnéticas o inteligentes, está equipado con un mecanismo opcional diseñado para garantizar la comunicación confiable entre la tarjeta y el lector.

Lector de inserción manual
Características
• Serie 9000: Interfaz RS-232 para tarjetas inteligentes de 8 contactos • Serie 9800: Mecanismo de bloqueo de la tarjeta mediante un solenoide con un led indicador verde/rojo. Botón de expulsión. • Serie 9600: Mecanismo de bloqueo de la tarjeta mediante un motor con un bisel plano.

Figura 4.7 *Lectores Cardom Technology. Serie 9000*

La serie KSR-4600/KDM-4600, ver Figura 4.8, soporta la inserción automática de tarjetas magnéticas o inteligentes, está equipada con un mecanismo opcional diseñado para garantizar la comunicación confiable entre la tarjeta y el lector.



Lector de inserción automática	
Características	
• Alta confiabilidad • Contacto de 8 o 16 pins • Interfaz RS-232.	
Especificaciones	
Voltaje	24 Volts ±10%
Vida del lector	700,000 ciclos de lectura
Velocidad del motor	250 mm/s
Peso	1 Kg
Temperatura de operación	0 – 50 °C

Figura 4.8 *Lector Cardom Technology. Serie 4600*

La serie ST1000, como se muestra en la Figura 4.9, soporta la inserción manual de tarjetas magnéticas o inteligentes, está equipada con un mecanismo opcional diseñado para garantizar la comunicación confiable entre la tarjeta y el lector.

Terminal de inserción manual	
Características	
• Interfaz RS-232 para tarjetas inteligentes de 8 contactos • Mecanismo de bloqueo de la tarjeta mediante un solenoide con un led indicador verde/rojo. Botón de expulsión. • Mecanismo de bloqueo de la tarjeta mediante un motor con un bisel plano.	
Especificaciones	
Voltaje	5 Volts ±5%
Corriente	Menos de 250 mA
Vida del lector	300,000 ciclos de lectura
Peso	150 g
Temperatura de operación	0 – 50 °C

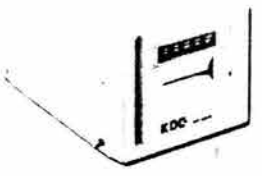
Figura 4.9 *Terminal Cardom Technology. Serie 1000*

La serie ST3000 ver Figura 4.10, soporta la inserción manual de tarjetas magnéticas o inteligentes. Puede ir montado sobre la superficie del teclado.

Terminal de inserción manual	
Especificaciones	
Interfaz	Teclado PS/2
Vida del lector	100,000 ciclos de lectura
Dimensiones (mm)	66.5 x 96.5 x 19.5
Peso	150 g
Temperatura de operación	0 - 50 °C

Figura 4.10 *Terminal Cardom Technology. Serie 3000*

La serie KDT4000, ver Figura 4.11, soporta la inserción automática de tarjetas magnéticas o inteligentes.



Terminal de inserción motorizada	
Características	
• Alta confiabilidad • Contacto de 8 pins • Interfaz RS-232.	
Especificaciones	
Voltaje	110-250 Volts ±10%
Vida del lector	700,000 ciclos de lectura
Velocidad del motor	250 mm/s
Peso	3.5 Kg
Temperatura de operación	0 - 50 °C

Figura 4.11 *Terminal Cardom Technology. Serie 4000*

- Fabricante: SIMPLE TECHNOLOGY

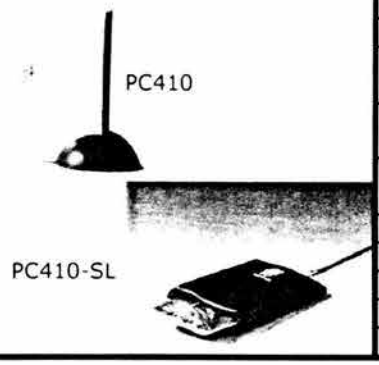
Teclado con lector de tarjeta y de huella digital, mostrado en la Figura 4.12, Key Tronic F-SCAN-KSC01US.

Teclado con lector de tarjeta	
Especificaciones	
Lectura de Tarjetas	ISO 7816
Protocolos estándar	T=0, T=1
Contactos	Corredizo, por presión
Interfaz	Serial o PS/2

Figura 4.12 *Teclado con lector de tarjetas y huella digital Key Tronic F-SCAN-KSC01US*

- Fabricante: GEMPLUS

Lector universal GEMPC410 y GEMPC410-SL, ver Figura 4.13.



Lector universal	
Especificaciones	
Dimensiones	GEMPC410: 90 x 86 x 26 mm
	GEMPC410-SL: 70 x 98 x 15 mm
Plataforma de Sistema Operativo	DOS, W3x,W95, W98, WNT4, W2000, WME, WXP, OS2
Tarjetas soportadas (ISO 7816)	De memoria
	Con microprocesador
Protocolos estándar	T=0, T =1
Voltaje	5 Volts
Corriente	20 mA
Interfaz	RS-232
Temperatura de operación	0 - 55 °C

Figura 4.13 *Lector de tarjetas Gemplus PC410 y PC410-SL*

El lector GemPC410-FD tiene características similares al GEMPC410. Se conecta en la bahía destinada al lector del disco flexible de una PC.

Lector compacto para puerto PC Card Tipo II PCMCIA, ver Figura 4.14.

Lector para PC Card PCMCIA	
Especificaciones	
Dimensiones	85 x 54 x 5 mm
Plataforma de Sistema Operativo	W95, W98, WNT4, W2000, WXP
Tarjetas soportadas (ISO 7811-7816)	De memoria
	Con microprocesador
Protocolos estándar	T=0, T =1
Voltaje	5 Volts
Corriente	12 mA
Peso	Menos de 20 gr
Interfaz	RS-232
Temperatura de operación	0 - 55 °C

Figura 4.14 *Lector de tarjetas Gemplus PC Card Tipo II PCMCIA*

Lector para puerto USB GemPC430, ver Figura 4.15.

Lector para USB	
Especificaciones	
Dimensiones	70 x 98 x 15 mm
Plataforma de Sistema Operativo	W98, W2000, WXP
Tarjetas soportadas (ISO 7816)	De memoria
	Con microprocesador
Protocolos estándar	T=0, T =1
Voltaje	5 Volts
Corriente	40 mA
Vida del lector	100,000 ciclos
Interfaz	USB
Temperatura de operación	0 - 55 °C

Figura 4.15 *Lector de tarjetas Gemplus GemPC430 USB*

- Fabricante: SCHLUMBERGER CARDS & SYSTEMS

Lector de tarjetas Reflex 20 y Reflex 72, ver Tabla 4.4.

	Lector	
Especificaciones	**Reflex 20**	**Reflex 72**
Plataforma de Sistema Operativo	W98,W2000, WME, WXP, WNT	W98,W2000, WME, WXP, WNT
Interfaz	PCMCIA Tipo II	Puerto serie

Tabla 4.4 *Lector de tarjetas Gemplus GemPC430 USB*

- Fabricante: VERIFONE

Lector SC 450, ver Figura 4.16.

Lector para RS-232	
Especificaciones	
Dimensiones	24 x 74 x 179 mm
Tarjetas soportadas	ISO 7816 1/2/3
Peso	500 gr
Voltaje	9 Volts
Corriente	22 mA
Interfaz	RS-232
Temperatura de operación	0 - 40 °C

Figura 4.16 *Lector de tarjetas Verifone SC 450*

Lector SC 550/552, ver Figura 4.17

Lector para RS-232	
Especificaciones	
Dimensiones	50 x 110 x 200 mm
Tarjetas soportadas	ISO 7816 1/2/3
Peso	700 gr
Voltaje	15 Volts
Corriente	230 mA
Interfaz	RS-232
Temperatura de operación	0 - 40 °C

Figura 4.17 *Lector de tarjetas Verifone SC 550/552*

- Fabricante: DATA KEY

Lector DKR730, ver Figura 4.18.

Lector para USB	
Especificaciones	
Dimensiones	60 x 79 x 25 mm
Plataforma de Sistema Operativo	WNT4
Tarjetas soportadas (ISO 7816)	De memoria / Con procesador
Protocolos estándar	T=0, T =1
Voltaje	5 Volts
Corriente	60 mA
Peso	60gr
Interfaz	USB
Temperatura de operación	0 - 55 °C

Figura 4.18 *Lector de tarjetas Data Key DKR730*

En la Tabla 4.5 se muestran algunos lectores soportados por el sistema operativo Windows.

Fabricante	Lector	Interfaz	Manejador
American Express	GCR435	USB	Grclass.sys
Bull	SmarTLP3	Serial	Bulltlp3.sys
Compaq	Serial reader	Serial	grserial.sys
Gemplus	GCR410P	Serial	Grserial.sys
Gemplus	GPR400	PCMCIA	Gpr400.sys
Gemplus	GemPC430	USB	Grclass.sys
Hewlett Packard	Protect Tools	Serial	Scr111.sys
Litronic	220P	Serial	Lit220p.sys
Schlumberger	Reflex 20	PCMCIA	Pscr.sys
Schlumberger	Reflex 72	Serial	Scmstcs.sys
Schlumberger	Reflex Lite	Serial	Scr111.sys
SCM Microsystems	SCR111	Serial	Scr111.sys
SCM Microsystems	SCR200	Serial	Scmstcs.sys
SCM Microsystems	SCR120	PCMCIA	Pscr.sys
SCM Microsystems	SCR300	USB	Stcusb.sys
Systemneeds	External	Serial	Scr111.sys
Omnikey AG	2010	Serial	Sccmn50m.sys
Omnikey AG	2020	USB	Sccmusbm.sys
Omnikey AG	4000	PCMCIA	Cmbp0wdm.sys

Tabla 4.5 *Lectores soportados por el sistema operativo Windows*

Aplicaciones

- Monedero electrónico
- Control de acceso físico y seguridad
- Telefonía móvil
- Tarjeta telefónica
- Aplicaciones de la tarjeta inteligente en México
- Proveedores de soluciones en México

Capítulo 5

CAPÍTULO 5. APLICACIONES

Actualmente, la mayoría de las personas trae en su cartera una gran variedad de tarjetas: de crédito, licencia para conducir, credencial para votar, credencial de una biblioteca, credencial para renta de películas, credenciales de aseguradoras, de usuario frecuente de alguna aerolínea, y muy probablemente una tarjeta de teléfono. Todas estas tarjetas están siendo o serán pronto reemplazadas por dos o tres tarjetas inteligentes, gracias a su cualidad para almacenar una gran cantidad de información.

La mayoría de las TI's manejan una sola aplicación, pero su verdadero valor se tiene cuando una misma tarjeta puede manejar varias aplicaciones. Por ejemplo, una tarjeta de crédito puede tener la función de almacenar valores para compras menores, en adición a información de usuario frecuente de una aerolínea o de renta de autos. Las aplicaciones de las tarjetas inteligentes pueden considerarse dentro de dos grandes grupos, el prepago y la autenticación.

Para lograr sus objetivos los sistemas interactúan con su medio ambiente, el cual está formado por todos los objetos que se encuentran fuera de sus fronteras. Los sistemas que interactúan con su medio ambiente (reciben entradas y producen salidas) se denominan sistemas abiertos. En contraste, aquellos que no interactúan con su medio ambiente se conocen como sistemas cerrados. Las aplicaciones de prepago pueden pertenecer a alguno de estos dos tipos de sistemas, cerrados o abiertos.

Hoy en día, la aplicación más grande de las TI's es la de tarjetas de prepago telefónico. Este es un sistema cerrado, ya que las tarjetas son emitidas por un proveedor de servicios para la utilización de su infraestructura; el mismo caso ocurre con aplicaciones de transporte público. Los elementos utilizados en estas tarjetas son circuitos simples de memoria y con limitada funcionalidad en aspectos de seguridad.

Un área de aplicación de un sistema abierto es el monedero electrónico, donde el emisor y el poseedor de la tarjeta no tienen relación comercial. Debido a que en este caso se está manejando una alternativa al valor en efectivo, los requerimientos de seguridad son mucho mayores.

El monedero electrónico tiene entre sus principales aplicaciones el pago electrónico de boletos en transporte, cine, teatro, compras menores y pago de servicios como el estacionamiento.

En el caso de las aplicaciones de autenticación, el uso clásico de las TI's es el de la identificación, donde el principal problema es asociar la tarjeta con el usuario indicado. Para este propósito el uso de un PIN es muy común, aunque actualmente también se utilizan elementos biométricos. Otras dos áreas importantes son la identificación para el acceso a computadoras y redes, además del acceso a Internet.

Los programas de aplicación manejan la lectura de datos realizada por lectores o terminales de tarjetas y los envían a computadoras centrales que pueden ser los servidores de bancos, centros de control de tráfico, centros de telefonía móvil, centros de entretenimiento, autoridades de tránsito, gobiernos y otros proveedores de servicios. A continuación, se presenta un análisis de los principales usos que tienen las tarjetas inteligentes.

5.1 MONEDERO ELECTRÓNICO

En la actualidad, es muy común el uso de las tarjetas como forma de pago en detrimento del dinero en efectivo, pero estas tarjetas son en su gran mayoría de banda magnética. Aunque es un método muy extendido tiene sus limitaciones, porque las transacciones siempre son en línea, es decir, se tiene que pedir una confirmación a un centro servidor antes de que el proveedor entregue el producto o el servicio solicitado.

Lo anterior permite con cierta facilidad su falsificación y debido al costo de la comunicación es poco viable la realización de pagos mínimos o existen situaciones donde es impráctico acceder a una red.

Las TI's permiten almacenar monedas electrónicas para realizar pequeños gastos y controlar el acceso a ese efectivo. Por lo que es otra forma de pago para compras mínimas, lo cual evita la necesidad de llevar monedas en el bolsillo. A la tarjeta inteligente más el efectivo almacenado en su memoria, se le llama monedero electrónico.

Las tarjetas inteligentes son un medio más adecuado de pago. La seguridad intrínseca y los modernos mecanismos de autenticación, llave pública y privada, la hacen prácticamente infalsificable. Además, permite que las transacciones se validen fuera de línea, es decir, sin tener que recurrir al sistema del banco, lo cual reduce los costos de comunicación, agiliza la transacción y mejora el nivel de servicio y aceptación de la tarjeta.

El sistema básico de prepago, consiste en que el usuario debe comprar dinero electrónico a un emisor y cargarlo a su tarjeta antes de poder hacer pagos con ella. El microprocesador contiene almacenado este valor, cuando se realiza alguna compra se disminuye automáticamente del saldo guardado. La propia tarjeta es la encargada de indicar la limitación del crédito disponible, en forma contraria a las tarjetas de banda magnética, donde hay un centro validador de transacciones.

La recarga de dinero se puede realizar con efectivo o mediante cualquier tarjeta de débito/crédito en terminales situadas en sucursales bancarias o en cajeros automáticos. En ocasiones, el dinero que se carga es retirado de la cuenta asociada a dicha tarjeta. A partir de ese momento el monedero electrónico puede ser usado para pagos en cualquier punto de venta donde sea aceptado hasta consumir la cantidad almacenada.

Con el pago fuera de línea, el importe de la transacción es transferido de la tarjeta del comprador a la del vendedor, ingresando este último el monto de las transacciones en el banco cuando lo considere oportuno.

El monedero electrónico está preparado para conectarse directamente con el banco y realizar la transacción de fondos desde la cuenta del usuario hasta la tarjeta en forma de dinero digital y viceversa. También está preparado para recibir efectivo de otros monederos. Es en sí un sistema que sustituye perfectamente al efectivo.

Otras características importantes de este sistema son:

- Reducción en los costos de administración.
- Facilidad en su uso.
- Bajo costo en la infraestructura de servicios bancarios y redes telefónicas.
- Versatilidad para combinar débito/crédito y valor almacenado en una misma tarjeta.
- Menor costo por transacción.

- Capacidad para operar fuera de línea o en línea.
- Posibilidad de almacenar diferentes divisas en la tarjeta y cambiarlas durante la fase de pago.
- Interoperabilidad entre usuarios de dinero electrónico, es decir, la oportunidad de realizar pagos entre clientes con diferentes emisores de monedero electrónico. Para estandarizar las aplicaciones, más del 90% de los monederos a nivel mundial han acordado seguir la especificación CEPS (*Common Electronic Purse Specification*).

Pero se pretende que el beneficio primordial que aportará el monedero electrónico sea que una misma tarjeta permita acceder a más información en ubicaciones tradicionales y nuevas, esto se muestra en la Figura 5.1, lo que aumentará su utilidad y el grado de conveniencia para el usuario, por ejemplo:

- Ampliar su uso para pagar en lugares como el transporte público, restaurantes de comida rápida, tiendas de artículos de primera necesidad, gasolineras, máquinas copiadoras, cines, parquímetros, puestos de revistas y periódicos, y máquinas expendedoras de refrescos.
- Realizar pagos de una persona a otra en cualquier parte del mundo a través de otros canales de comunicación como son el teléfono celular, la televisión interactiva o la computadora personal.
- Tener acceso a diversas cuentas de débito/crédito personales con un sólo plástico, evitando traer consigo varias tarjetas.
- Identificarse electrónicamente de manera segura, con lo cual se puede tener acceso a lugares como la oficina o a un sistema de cómputo.
- Almacenar datos no financieros, es decir, información médica, de seguros, historial académico, etc.

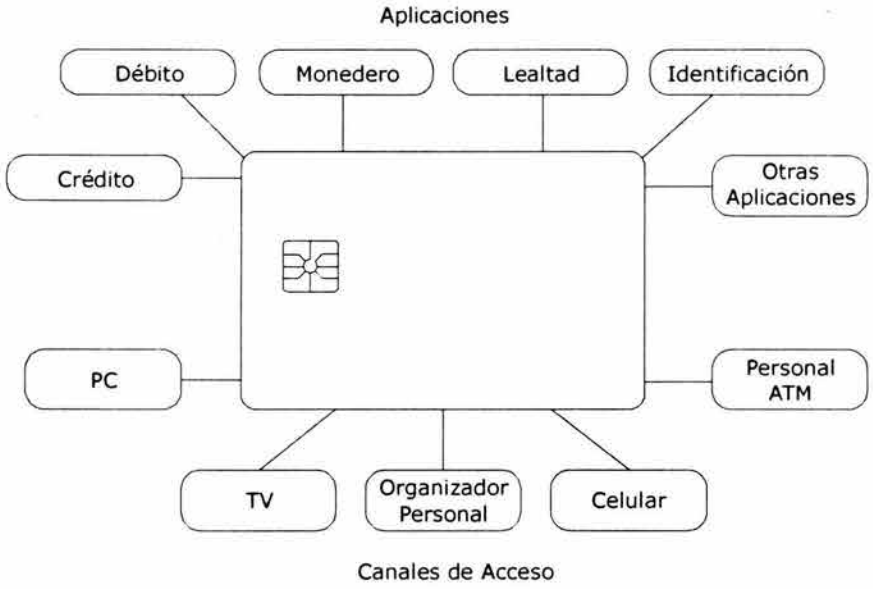


Figura 5.1 *Funcionalidad del monedero electrónico*

En la actualidad se está empezando a implantar este sistema principalmente en países de Europa, como se puede apreciar en la Tabla 5.1. Se ha desarrollado sólo en algunas áreas

debido a diversos inconvenientes; por ejemplo, algunos de los bancos han puesto en funcionamiento sus monederos electrónicos, pero son pocos los establecimientos que permiten trabajar con este tipo de efectivo, porque en primera instancia se tienen que actualizar todos los cajeros automáticos y terminales de puntos de venta.

Región	Monedero Electrónico
Estados Unidos	VisaCash, MasterCard Cash, Citibank
Europa	Eurocheque, Cafe Project, Avant (Finlandia), Quick (Austria), Zeelandkart (Holanda), Proton (Suiza), GeldKarte (Alemania), SEMP (España), SIBS (Portugal), Danmont (Dinamarca), Mondex (Inglaterra), Zolotaya Korona, (Rusia)
Canadá	Normadin
Australia	Freedom, Wizard Card
Asia	Bank of China, Thai Farmers Bank, Malaysian Card (Malasia) NETS (Singapur), Cash Card (Singapur)
Medio Oriente	Unicard (Israel)
Sudamérica	Moeda Electonica Bradesco (Brasil)
África	Mericien Biao (Sudáfrica)
Worldwide Web	Mondex, VisaCash, ProtonWorld
México	Inbursa, VisaCash

Tabla 5.1 *Ejemplos de monederos electrónicos*

Otro inconveniente es que el monto del dinero almacenado no está asegurado o protegido contra pérdida o robo. Siendo un equivalente al efectivo, el valor en una tarjeta inteligente no es recuperable.

Algunos sistemas de pago electrónico están protegidos contra esas pérdidas por un elaborado mecanismo de criptografía o requieren de autenticación en cada transacción. Esto adiciona costos significativos en cada operación minimizando sus ventajas sobre los cheques o el dinero en efectivo.

Por lo cual, se debe establecer una garantía sobre el costo efectivo o bien asegurar el valor almacenado para proteger a los consumidores. Las opiniones legales acerca de los derechos y responsabilidades de proveedores y usuarios del efectivo electrónico varían ampliamente en cada región.

5.2 CONTROL DE ACCESO FÍSICO Y SEGURIDAD

El control de acceso se refiere al proceso de permitir el ingreso de una persona o el uso de algún servicio, mientras se impide el acceso a otros. Un guardia de seguridad actúa como un agente de control de acceso cuando deja que ciertas personas pasen a través de la estación de seguridad evitando que personas no autorizadas lo hagan.

En general, se utiliza el control de acceso para proteger cosas que se consideran valiosas, de ser observadas o alteradas por cualquier entidad que se ha decidido que no está autorizada para hacerlo.

Las claves secretas, los números de identificación personal y la encriptación se han convertido en mecanismos comunes para limitar el acceso a valores como la información, el dinero o las computadoras.

Actualmente existen nuevos delitos como el ver programas de televisión por suscripción sin pagar por ello. Para controlar el acceso a estos bienes, han surgido tecnologías como la tarjeta inteligente. La intención de estas tecnologías es prevenir que personas no autorizadas tengan acceso a estos bienes.

Con la llegada de las tarjetas inteligentes, para las cuales la seguridad es un aspecto sumamente importante, pronto se desarrollaron aplicaciones para controlar el acceso mediante estos dispositivos. El éxito de las aplicaciones de control de acceso basadas en TI's depende de dos consideraciones:

- Determinar si el costo de la tecnología de seguridad es adecuada para la aplicación, esto quiere decir que el costo de romper la seguridad de la aplicación de la TI es mucho mayor al beneficio que se podría obtener de romper dicha seguridad.
- Asegurarse de que el diseño del sistema de la TI y del programa de aplicación estén bien implementados. Para seleccionar una tecnología de tarjeta inteligente adecuada se debe entender la naturaleza de la aplicación y la tecnología actual que podría utilizarse para burlar la seguridad.

Dentro de la aplicación de la tarjeta inteligente, el sistema de control de acceso para un usuario consta de tres elementos:

- Una tarjeta o identificación que es presentada al lector instalado en la puerta.
- Un lector de tarjeta, el cual indica si la tarjeta es válida y autoriza la entrada.
- Una puerta, la cual se desbloquea cuando el acceso es autorizado.

Detrás de lo anterior, está una compleja red de datos, computadoras y software que incorporan una seguridad robusta, ver Figura 5.2. Un sistema típico de control de acceso está compuesto por los siguientes componentes:

- Credencial de identificación (tarjeta inteligente). Es el dispositivo físico de reconocimiento general.
- Lector de tarjetas inteligentes. Elemento que se encuentra en cada puerta para la lectura de una tarjeta de identificación o credencial. Envía los datos correspondientes al panel de control para tomar la decisión de los derechos de acceso.
- Cerradura de la puerta. Interfaz electrónica que está conectada al panel de control.
- Panel de control. Es el componente del sistema de control de acceso donde están conectados todos los lectores, las cerraduras y el servidor de control de acceso. El panel de control valida al lector y acepta los datos. Dependiendo del diseño integral del sistema, el panel de control envía los datos al servidor de control de acceso o puede tener la capacidad de decisión para determinar los permisos de usuarios y autorizar finalmente su acceso. El panel de control también puede ser llamado controlador o panel.
- Servidor de control de acceso. Recibe los datos de la tarjeta desde el panel de control. Compara los datos de la tarjeta con la base de datos, determina los privilegios de acceso de los usuarios e indica si la persona puede ser admitida.
- Software. Programa para administrar el sistema de acceso.
- Base de datos. Contiene la información actualizada de los derechos de acceso de los usuarios.

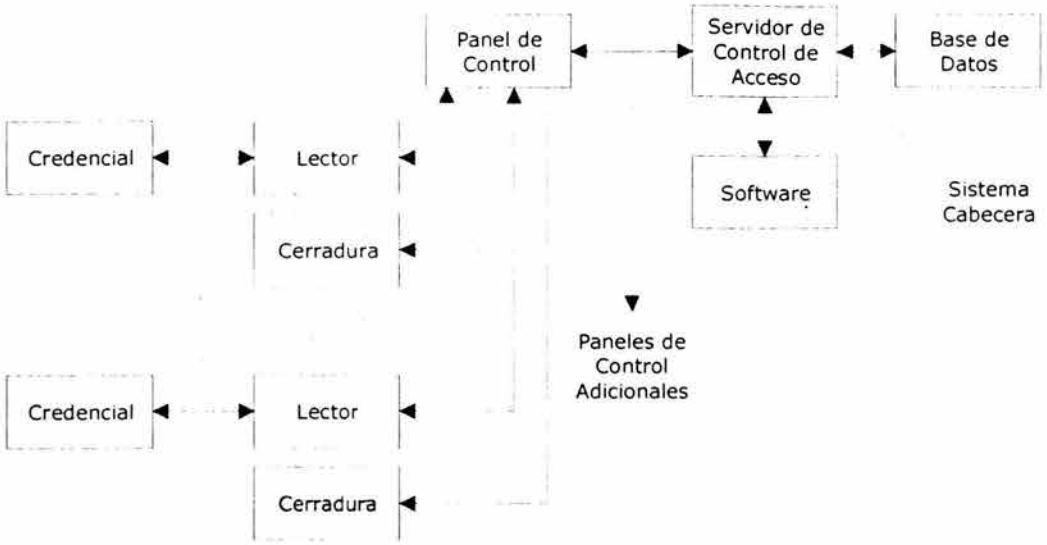


Figura 5.2 *Esquema del sistema de control de acceso*

5.2.1 Elementos biométricos

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian; la forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos distinguen del resto de las personas.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de una persona. La biometría es una propiedad física única, medible y como tal, diferenciable.

Algunos de los elementos biométricos más conocidos son:

- El reconocimiento de las huellas digitales.
- El reconocimiento facial.
- El reconocimiento de la geometría de la mano.
- Verificación de la voz.
- Barrido de la retina
- Barrido del iris

En la Figura 5.3 se muestra el proceso básico de un sistema biométrico, el cual convierte los datos derivados de las características fisiológicas en plantillas, para compararlas posteriormente; las diferentes etapas de este proceso son:

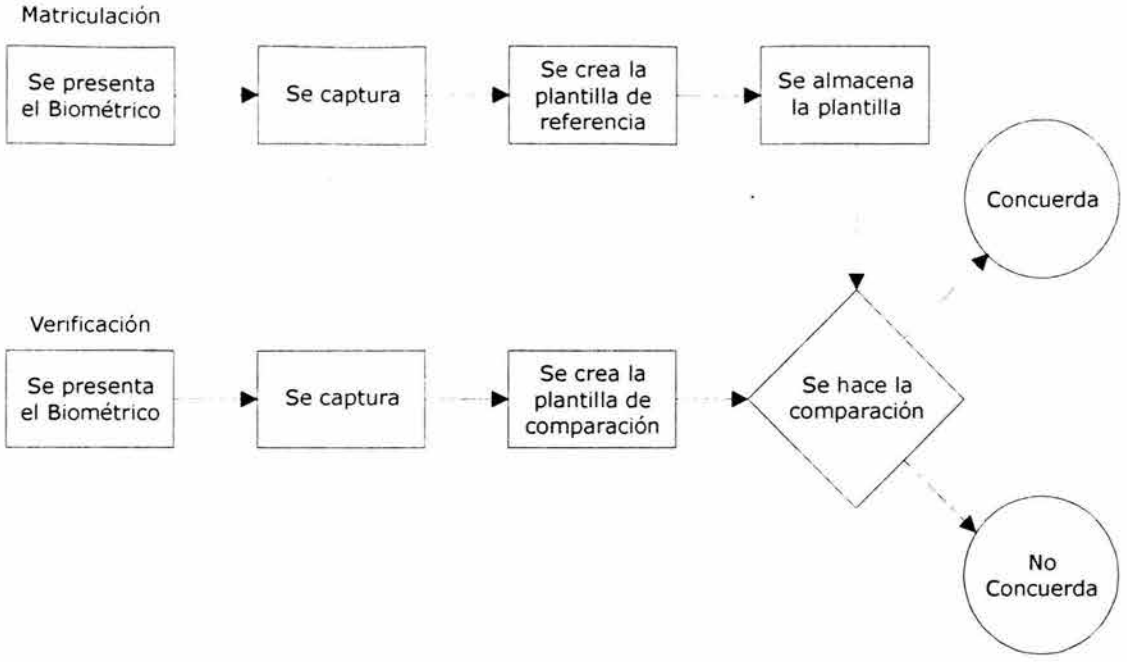


Figura 5.3 *Proceso de comparación biométrica*

Matriculación. Es el proceso mediante el cual los ejemplos biométricos iniciales son recolectados, valorados, procesados y almacenados para su uso posterior. Este proceso comprende los siguientes pasos:

- Presentación del biométrico. En esta etapa el usuario provee los datos fisiológicos en forma de ejemplos biométricos, es decir, se puede requerir que mire en dirección a una cámara o que coloque su dedo en un lector. Dependiendo del sistema biométrico el usuario debe quitarse los lentes, permanecer en una posición durante algunos segundos o pronunciar una frase para proveer el ejemplo biométrico.
- Captura. En esta etapa el hardware del sistema obtiene los ejemplos biométricos.
- Creación de la plantilla de referencia. Las características fisiológicas obtenidas son utilizadas para generar una plantilla biométrica, la extracción de características puede requerir varios grados de procesamiento de imágenes o ejemplos para obtener la suficiente cantidad de datos precisos. Por ejemplo, en la tecnología de reconocimiento de voz se pueden filtrar ciertas frecuencias y patrones. La plantilla generada es un archivo pequeño pero altamente distintivo generado por un algoritmo biométrico que identifica características únicas del ejemplo capturado. Dependiendo en donde son generadas, se les pueden llamar plantillas de matriculación o plantillas de verificación.
- Almacenamiento de la plantilla. Las plantillas obtenidas son almacenadas en una base de datos para realizar comparaciones.

Verificación. En este proceso se establece la validez de una identidad comparando la plantilla de verificación contra la plantilla de matriculación almacenada. Este proceso tiene etapas

similares al proceso de matriculación, como son la de presentación del biométrico, captura y creación de la plantilla.

Comparación. En la gran mayoría de las tecnologías y sistemas biométricos no existe una concordancia del 100%, sin embargo, estos sistemas proveen un alto grado de seguridad. Estas comparaciones se realizan con algoritmos propietarios de los fabricantes aplicados a las plantillas biométricas, de esta comparación se obtiene un número que indica el grado de similitud entre ambas.

5.2.2 Proceso de control de acceso

El proceso de control de acceso comienza cuando el usuario presenta su credencial de identificación al lector, el cual normalmente está colocado junto a la entrada o puerta de acceso. El lector extrae los datos de la TI, los procesa y los envía al panel de control. El panel de control primero valida el lector y entonces acepta los datos transmitidos por el lector, lo que sucede posteriormente depende de si el sistema es centralizado o distribuido.

En un sistema centralizado, el panel de control transmite los datos al servidor de control de acceso. El servidor compara los datos recibidos de la tarjeta con información del usuario que está almacenada en una base de datos. El software de control de acceso determina los privilegios de acceso del usuario, la autorización, hora, fecha, y la puerta de entrada, y cualquier otra información que la compañía pueda requerir para garantizar su seguridad. Cuando el acceso es autorizado, el servidor de control de acceso envía entonces dos señales, una para la cerradura apropiada de la puerta que libera la misma, y otra al lector de la puerta, el cual emite una señal audible o alguna otra para que el usuario ingrese.

En un sistema distribuido, el panel de control permite o deniega la entrada. El servidor de control de acceso periódicamente provee de información a los paneles de control, para que el software del panel determine si un usuario tiene permitido el acceso. Realiza las funciones del servidor de control de acceso descritas anteriormente y toma la decisión de autorizar o denegar la entrada. El permitir que los paneles de control realicen la función de la toma de decisiones tiene la ventaja de requerir menos comunicación entre los paneles y un servidor central de control de acceso, lo que permite mejorar el desempeño general del sistema y su seguridad.

Si el uso de un PIN o un elemento biométrico se incorporan al sistema, el lector comúnmente autentica estos datos. La validez puede ser determinada por el lector o dentro de la tarjeta inteligente, comparando los datos con un formato biométrico o un PIN almacenado en la misma. En algunos casos, los datos biométricos pueden ser enviados al panel de control para procesarlos. Si la información adicional es válida, el lector envía el número de la credencial de identificación al panel de control. Si la información no es válida entonces el lector indica que el acceso es denegado.

La respuesta a una tarjeta no válida es definida por las políticas y procedimientos de seguridad de la compañía. El servidor de control de acceso o el panel de control pueden ignorar los datos y no enviar ningún código a la cerradura de la puerta, o puede enviar una señal para que el lector emita un sonido diferente indicando que el acceso ha sido denegado, también puede notificar y activar otros sistemas de seguridad, por ejemplo, circuitos cerrados de televisión o alarmas, indicando que una tarjeta no autorizada ha sido presentada al sistema.

5.2.3 Formato de los datos del sistema de control de acceso

El formato de los datos del sistema de control de acceso es un elemento crítico de diseño y se refiere al patrón de bits que el lector transmite al panel de control. Especifica cuantos bits componen la cadena de datos y qué representa cada bit, por ejemplo, los primeros bits podrían indicar el código del edificio, los siguientes, un número de identificación de la credencial, la paridad, etc.

Muchos fabricantes de sistemas han desarrollado sus propios formatos haciéndolos únicos. Los formatos se conservan en secreto para prevenir que alguna persona o compañía no autorizada duplique una tarjeta.

5.2.4 Consideraciones de seguridad

Para reducir los riesgos de acceso no autorizado o ataques deliberados, la seguridad de todo el sistema debe ser considerada. Esto empieza con el proceso inicial de emisión de tarjetas e incluye los componentes actuales del sistema como la red, bases de datos, software, hardware, cámaras, lectores y las tarjetas; los procesos del sistema, por ejemplo, los procedimientos del personal de vigilancia; y por último la protección de los datos dentro de los componentes y durante su transmisión.

5.2.4.1 Seguridad de la tarjeta inteligente

La TI ayuda por sí misma a disuadir su falsificación, frustrar un atentado con una tarjeta de identificación y prevenir el uso de una tarjeta no autorizada. Las tarjetas inteligentes incluyen varias capacidades de hardware y software, que detectan y reaccionan a los intentos de falsificación bloqueándose a sí mismas.

Cuando las TI's pueden ser utilizadas para una verificación manual de identidad, se le pueden adicionar características de seguridad al cuerpo de la tarjeta como tipos de letra únicos, tintas de color especial, arreglos multicolores, micro impresión, tinta ultravioleta de alta calidad ya sea en el frente o en el reverso, imágenes fantasma (una segunda fotografía más tenue del usuario en otra posición), y hologramas multicapa incluyendo imágenes tridimensionales.

Cuando se diseñan e implementan apropiadamente las TI's, es casi imposible duplicarlas o falsificarlas, y los datos en el circuito integrado no pueden ser modificados sin la autorización apropiada utilizando contraseñas, autenticación biométrica o llaves de acceso encriptadas. Si la implementación del sistema tiene políticas efectivas de seguridad e incorpora los servicios de seguridad necesarios proporcionados por las TI's, organizaciones y usuarios pueden tener un alto grado de confianza en la integridad de la información de la identificación y de su uso autorizado.

5.2.4.2 Protección de los datos

Uno de los argumentos más firmes para el uso de sistemas basados en TI's para el control del acceso físico, es la capacidad de usar datos protegidos o encriptados para resguardar la información en el circuito y durante la transmisión. La seguridad y validez de la información

requerida para identificar individuos, sus derechos y privilegios son clave para el éxito de un sistema de control de acceso físico.

Las TI's soportan algoritmos criptográficos simétricos los cuales aseguran sustancialmente la protección y proporcionan excelentes tiempos de procesamiento. La llave de criptografía simétrica es ampliamente utilizada para el control de acceso físico y utiliza la misma llave para encriptar y desencriptar, haciéndola extremadamente rápida y confiable.

Cuando un sistema de control de acceso incluye acceso lógico y privilegios de llave pública y el tiempo de procesamiento no es vital, los algoritmos de criptografía asimétrica pueden ser utilizados. Varias llaves pueden ser almacenadas en un sólo circuito para cubrir los requerimientos de seguridad para su uso en aplicaciones múltiples.

5.2.4.3 Autenticación de la tarjeta y los datos

Un sistema seguro de acceso físico debe cerciorarse de que la tarjeta presentada al lector y de que los datos que contiene son auténticos. En algunos casos, es importante verificar también que el lector sea auténtico para prevenir que terminales falsas sean utilizadas para extraer datos.

Además del uso de un PIN y características biométricas, las cuales desbloquean la tarjeta o autentican la persona, las tarjetas inteligentes tienen la capacidad única de ofrecer características de autenticación interna escritas en el circuito. Cuando la autenticación se basa en el uso de PIN, el propietario debe insertar la TI en el lector para digitar a continuación el código numérico correspondiente. La autenticación hace uso de la llave pública y la llave privada, descritas en el inciso 3.5 Seguridad.

5.2.4.4 Comunicación entre la tarjeta y el lector

Como cualquier proceso que involucra señales electrónicas, la transmisión de datos entre componentes puede ser monitoreada. Esta posibilidad debe ser considerada en el diseño del sistema de seguridad en términos del ambiente, por ejemplo, si el área está siendo observada o alguien físicamente puede insertar otro dispositivo de monitoreo de la señal.

Dependiendo del ambiente y perfil de riesgo, una organización puede considerar que los datos enviados de una tarjeta con contactos o inalámbrica a un lector pueden ser monitoreados, permitiendo un acceso ilegal si se utiliza una tarjeta falsificada o con dispositivo para duplicar los datos. Las tarjetas inteligentes poseen técnicas de seguridad que hacen confiable la comunicación entre la tarjeta y el lector y permiten métodos de autenticación entre ellos.

5.2.4.5 Comunicación entre el lector de tarjetas y el panel de control

En un punto de acceso que no está siendo vigilado o que no tiene un cableado físicamente seguro, un intruso podría remover un lector de tarjetas de su montaje y leer la cadena de datos enviada al panel de control o colocar una computadora personal u otro dispositivo a esos cables y reproducir la inserción de una tarjeta válida para lograr la autorización.

La mayoría de los lectores actualmente transmiten datos al panel de control utilizando uno de dos formatos, el formato Wiegand o el de cinta magnética. El formato Wiegand utiliza dos líneas de señales: D0, para transmitir los pulsos de datos cero y D1, para transmitir los pulsos de datos uno. El formato de cinta magnética utiliza dos líneas de señales, una para datos y otra para el reloj.

La comunicación del lector al panel de control puede hacerse de una manera similar a la utilizada para hacer seguro el canal entre la tarjeta y el lector. El intercambio de datos entre los dos dispositivos puede ser encriptado para máxima seguridad, el lector y el panel pueden ser autenticados durante la transacción.

Debido a que la conexión entre el panel de control y el sistema de acceso está dentro de un edificio o localizado en un cuarto seguro, éste generalmente no es susceptible a ataques. Si se desea, esta conexión puede hacerse segura utilizando las técnicas descritas anteriormente y tener así un canal de datos de un extremo a otro.

La Figura 5.4 muestra un ejemplo de cómo un sistema de acceso físico basado en TI's puede proporcionar seguridad de extremo a extremo.

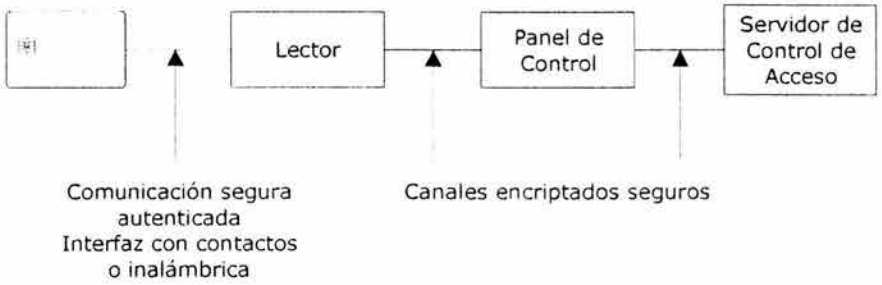


Figura 5.4 *Esquema de la seguridad en un sistema de control de acceso*

5.2.5 Acceso

Una vez autenticado el usuario de la TI, éste puede acceder a las instalaciones o servicios a los que tiene derecho. Además de controlar el acceso físico y dependiendo de los requerimientos de la aplicación, el sistema de seguridad puede llevar un registro de la fecha y la hora en que se verificó la autenticación del usuario y se le permitió el paso por dicha puerta.

En aplicaciones de alta seguridad es común utilizar esclusas en lugar de puertas o torniquetes para controlar el paso, el usuario entra a una cabina de doble puerta donde se encuentran el lector de tarjetas inteligentes y un lector biométrico. Al iniciar el proceso de autenticación se cierra la puerta por donde ingresó el usuario y después de autenticarse se abre una segunda puerta para permitirle el acceso, en caso contrario, pueden permanecer cerradas ambas puertas hasta que llegue personal de seguridad. Este tipo de puertas normalmente incorporan elementos de seguridad adicional como detectores de metal.

De las aplicaciones basadas en las TI's, relacionados con el acceso físico se pueden mencionar en:

- Edificios u oficinas gubernamentales o corporativas.
- Clubes deportivos.
- Hoteles.
- Bibliotecas.
- Centrales de cómputo y comunicaciones.

5.2.6 Soluciones en el mercado

En la Tabla 5.2 se muestra la referencia de algunas aplicaciones existentes en el mercado.

Producto	Aplicación	Proveedor
SIMmate 2000	Control de acceso	ACS Advanced Card Systems LTD
Passage	Control de acceso	RSA Security
Manage PKI	Control de acceso	VeriSing
Dexa.Badge	Control de acceso	Schlumberger
eToken	Control de acceso	Aladdin
SecurEnterprise	Control de acceso	SecurSoftware
Diversos Productos	Control de acceso Servicios Financieros	Gemplus
Datakey CIP	Control de acceso	Datakey
Datakey Axis	Control de acceso	Datakey
.smartsing	Control de acceso	Labcal
.smartprint	Control de acceso Labcal	Id Biométrica
Trinity	Control de acceso Activ Card	Id Biométrica
ChipCert	Control de acceso	CardBase Technologies

Tabla 5.2 *Aplicaciones para el control de acceso existentes en el mercado*

5.3 TELEFONÍA MÓVIL

Actualmente, la aplicación mundial más grande de las TI's es en tarjetas de prepago para el servicio de telefonía pública. Ésta es seguida por la telefonía móvil GSM (*Global System for Mobile Communications*), el estándar de telefonía móvil más popular. Con la llegada de las redes de última generación y la convergencia hacia el Servicio Universal de Telefonía Móvil (UMTS, *Universal Mobile Telephone Service*), toda la telefonía celular digital eventualmente incorporará tarjetas inteligentes.

5.3.1 Arquitecturas de telefonía móvil

5.3.1.1 Telefonía inalámbrica (CT, *Cordless Telephony*)

La telefonía inalámbrica fue desarrollada en la segunda mitad de 1970 y se extendió principalmente en Europa para su utilización en los hogares. El principal inconveniente con estos teléfonos era que utilizaban frecuencias que ya estaban designadas a la marina, a la transmisión televisiva y a otros usos, y estos aparatos causaban interferencias, además de que no había seguridad en el marcado, lo que significaba que una persona podía con relativa facilidad utilizar el servicio telefónico de otra. En 1981, British Telecom (BT), emitió la Especificación para Telefonía Inalámbrica 1 (CT1, *Cordless Telephony 1 Specification*) y en 1983 el mercado adoptó esta norma, de forma paralela el resto de Europa con excepción de Francia, que admitió una solución diferente bajo los auspicios de la CEPT (*European Conference of Postal and Telecommunications*).

La telefonía inalámbrica fue originalmente diseñada como una extensión a las líneas telefónicas domésticas fijas ya existentes, un paquete normal de teléfono inalámbrico incluía una base y su correspondiente aparato.

Con la norma CT2 una característica adicional era la posibilidad de adicionar más teléfonos inalámbricos a una misma base, o adicionar un teléfono temporal "visitante" a la base.

También fue prevista la posibilidad de tener bases públicas "Telepuntos CT" a los cuales los usuarios se podían conectar para realizar llamadas, para este servicio era necesaria una suscripción. Este esquema no cubrió las expectativas que se tenían y fue desapareciendo.

5.3.1.2 DECT (*Digital European Cordless Telephone*)

DECT es un servicio de telefonía inalámbrica desarrollada para utilizarse en hogares y oficinas. Desde un principio DECT fue especificado para proveer una amplia gama de aplicaciones para negocios de comunicaciones, aplicaciones de telepunto y domésticas. Se hicieron previsiones para voz y datos, y los servicios ISDN (*Integrated Services Digital Network*) serían integrados en un futuro, estos incluían circuitos de conmutación de voz y datos, además de conmutación de datos empacados.

La norma DECT es más integral que la especificación CT2 pero también más compleja y requiere el soporte de más software.

5.3.1.3 GSM (*Global System for Mobile communications*)

La telefonía móvil GSM apareció con el propósito de servir como estándar a los operadores móviles europeos y simplificar de manera significativa los procesos de tránsito (*Roaming*) entre redes de servicio y países.

El servicio de GSM está basado en una serie de radio células contiguas las cuales proveen una cobertura completa del área de servicio y permiten la operación del suscriptor en cualquier lugar contenido en esta área. Anterior a este concepto celular, los radio teléfonos estaban limitados a un único transmisor que cubría toda el área de servicio.

La telefonía celular es diferente al servicio de radio teléfono ya que en lugar de tener un transmisor muy grande, muchos transmisores pequeños son utilizados para cubrir la misma área. El problema básico de la telefonía móvil es manejar la situación en la que una persona utilizando el teléfono en una célula se mueve fuera del rango de dicha célula, en el caso del servicio de radio teléfono no existe solución y la llamada se pierde, por eso el área de servicio del transmisor es muy grande.

En telefonía celular el problema es resuelto pasando la llamada a la siguiente célula. Este proceso es totalmente automático y no requiere de intervención por parte del usuario, pero es una función técnica compleja y requiere de un significativo poder de procesamiento para lograr una respuesta rápida.

La razón para la utilización de muchas células pequeñas y limitar la potencia de salida de cada una es la de reducir la interferencia de una célula con las otras circundantes. Cada

llamada es asignada a una frecuencia diferente a la de sus vecinos, esto puede ocasionar que las frecuencias disponibles sean rápidamente utilizadas, esto se evita permitiendo que células no adyacentes utilicen la misma frecuencia. Ya que dos células empleando la misma frecuencia están lo suficientemente alejadas para no causar interferencia entre ellas, las mismas frecuencias pueden ser usadas varias veces, así el servicio utiliza de forma eficiente un recurso muy limitado, el espectro de radiofrecuencias.

Cada célula de GSM tiene una estación base transmisora receptora (BTS, *Base Transceiver Station*), la cual transmite y recibe en las frecuencias asignadas a la célula; una estación base controladora (BSC, *Base Station Controller*) que opera con un grupo de BTS's y es la responsable de la manipulación entre las BTS's y de los niveles de potencia de transmisión; y el control principal que es el centro móvil de intercambio (MSC, *Mobile Switching Center*) y es el responsable de la administración del tráfico que incluye:

- Establecimiento de la llamada.
- Ruteo.
- Terminación.
- Cargos e información de las cuentas.

El MSC es interfaz entre las redes GSM y el servicio de telefonía pública (PSTN, *Public Service Telephony Network*) tanto para voz como para datos.

La estación móvil (MS, *Mobil Station*) representa el único equipo que el usuario ve de todo el sistema, la MS consiste del equipo móvil (ME, *Mobil Equipment*) y del módulo de identificación del suscriptor (SIM, *Subscriber Identification Module*). El ME provee las funciones genéricas de radio y procesamiento para acceder a la red a través de la interfaz de radio, así como también sirve de interfaz para el usuario, micrófono, bocina, pantalla y teclado, junto con una interfaz a algún otro equipo terminal, fax o computadora personal.

El SIM es una tarjeta inteligente que contiene toda la información relacionada con el suscriptor, almacenada en el lado del usuario de la interfaz de radio, en la Figura 5.5 se muestra el esquema del módulo SIM.

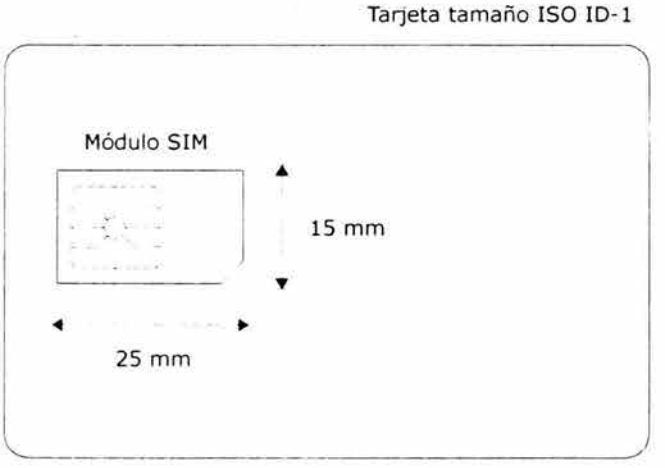


Figura 5.5 *Esquema del módulo SIM*

El MS es operacional sólo cuando un SIM válido es colocado en el equipo móvil. La Figura 5.6 muestra el esquema operacional de la tecnología GSM.

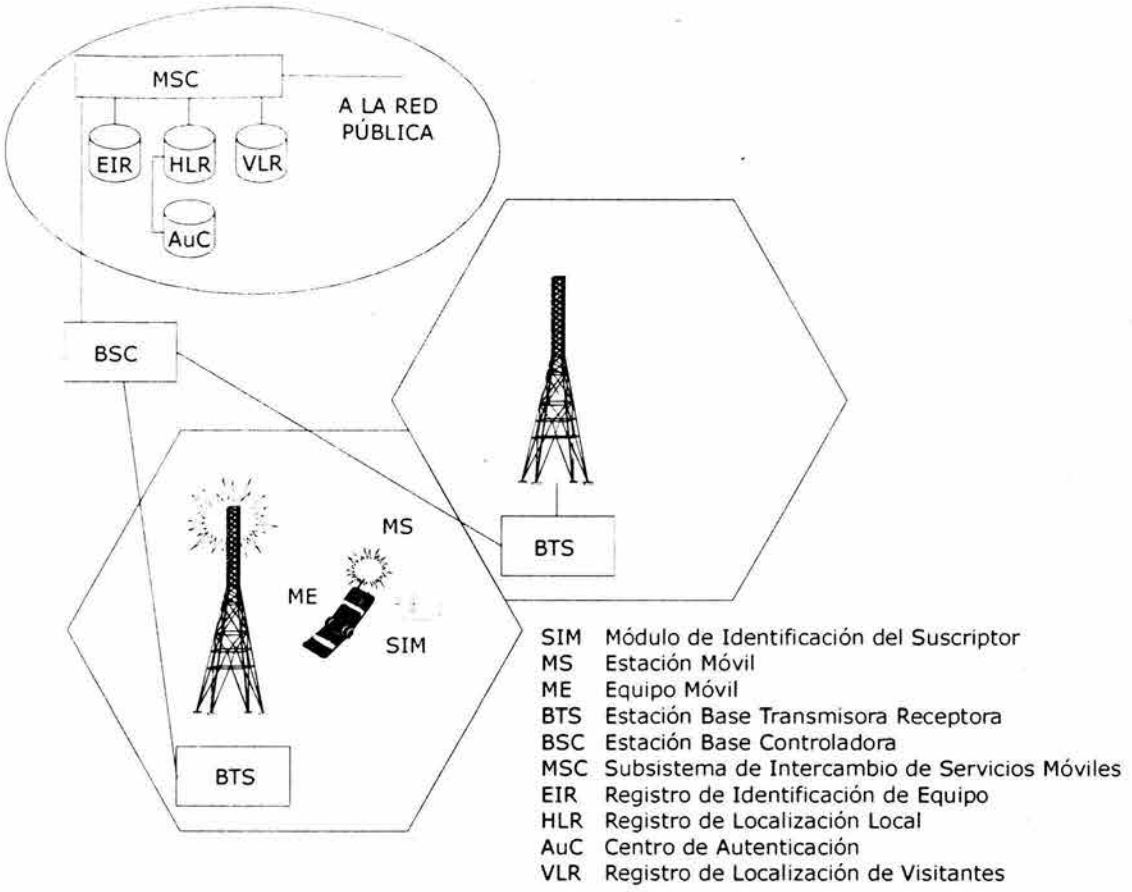


Figura 5.6 *Esquema de la tecnología GSM*

5.3.1.4 PCN (*Personal Communications Network*)

Cuando se inició el servicio GSM en Europa ya había una gran demanda latente del mismo, los operadores de GSM no imaginaron que la demanda presentara un incremento tan grande y tuvieron muchos problemas para cubrirla, además la calidad del servicio no fue lo esperado, una excusa fue la falta de espacio en el espectro disponible. Si más células eran colocadas para cubrir la misma área, el tamaño de cada célula tenía que reducirse.

Hay un límite práctico en el tamaño de las células, en áreas urbanas las señales pueden viajar a mayor distancia de lo deseado debido a las reflexiones en los edificios, sin embargo, la solución es costosa. Otra manera de colocar más suscriptores en la red celular es la de incrementar el espectro disponible y poner más canales en él. Para este propósito un nuevo espectro fue abierto por los gobiernos europeos, este fue el servicio PCN en el rango de 1710 MHz a 1880 MHz (1.8 GHz). Este nuevo estándar también es conocido como DCS 1800 (*Digital Communication System 1800 MHz*).

En un futuro se espera que los sistemas CT, DECT, GSM y PCN converjan en un servicio de telecomunicaciones móviles universal o UMST (*Universal Mobile Telecommunications Service*). En la Figura 5.7 se muestra el desarrollo de los estándares.

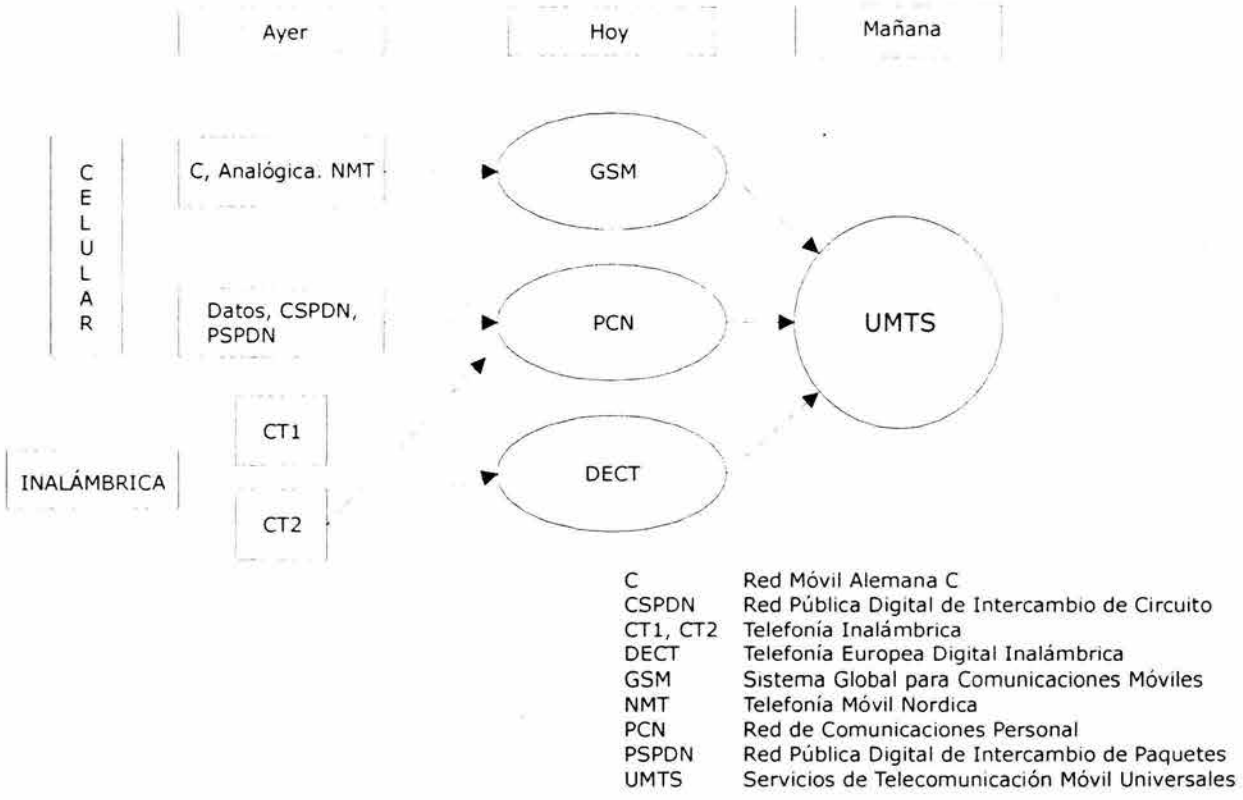


Figura 5.7 *Tendencia hacia el UMTS*

5.3.2 Uso de la tarjeta inteligente en GSM

En el desarrollo inicial de GSM en 1988, las ventajas de contar con un módulo de identificación separado desmontable (SIM), el cual fuera capaz de insertarse en cualquier equipo GSM, fue previsto para proveer los siguientes beneficios a los operadores de redes y a la administración de suscriptores:

- El SIM contendrá la identidad del usuario, es decir, su número telefónico y otra información necesaria para el acceso a la red. Este SIM común deberá permitir un procedimiento idéntico para la programación de esta información sin importar el tipo particular de aparato telefónico (ME) con el cual el SIM después será asociado.
- El módulo proveerá los medios necesarios para la administración de los datos requeridos en la estación móvil (MS), relacionados a la seguridad del sistema, por ejemplo, la autenticación del suscriptor y la encriptación de la conversación.

En 1988 no se previó que la reducción del tamaño de los aparatos telefónicos de GSM ocurriera tan rápido. Los teléfonos analógicos disponibles entonces no tenían el tamaño de

bolsillo como el que se tiene actualmente. Se esperaba que los usuarios de GSM no viajarían siempre con un aparato telefónico pero sí con su identificador de suscripción (SIM) y pedir prestado o contratar un equipo móvil (ME) en su destino, el cual podrían personalizar insertando su SIM.

Una vez que las tarjetas telefónicas fueron reconocidas como la plataforma ideal en la cual basar el SIM, su desarrollo avanzó rápidamente. Ya que las especificaciones progresaron, se diseñaron dentro del SIM más servicios de suscripción y habilitadores para la operación en red, además de los requerimientos de identificación básicos originales. Más tarde, ya con los objetivos básicos del servicio cubiertos, el SIM está siendo reconocido como un medio importante, el cual puede ser utilizado por los operadores de red para proveer diferenciadores en el servicio frente a su competencia.

No todos los fabricantes de equipos telefónicos estaban de acuerdo en adoptar el concepto de un módulo removible, e incluso menos para proveer una ranura para una tarjeta inteligente del tamaño ISO de una tarjeta de débito/crédito, y presionaron para que la funcionalidad del SIM se incorporara en los mismos aparatos telefónicos. Dos argumentos fueron presentados:

- La necesidad de proveer espacio para el módulo SIM y una interfaz complicaría el diseño de los aparatos telefónicos. Esta objeción fue solventada con la introducción de un segundo tamaño para el SIM (conocido como plug-in SIM) el cual es un módulo de aproximadamente 25 mm x 15 mm cortado de una tarjeta inteligente de tamaño ISO completo, ver Figura 5.5, conteniendo el chip en el entendido de que el plug-in SIM será removido del aparato con muy poca frecuencia, sin embargo, conserva las ventajas de la programación de la información del usuario y la seguridad de los datos por el emisor de la tarjeta.
- Las capacidades de memoria de los productos semiconductores disponibles para su uso en TI's eran muy pequeñas. Esto se solucionó duplicando algunas características de GSM directamente en el aparato telefónico, por ejemplo, los números abreviados de marcado se graban en el SIM y si se agota la memoria continúa la grabación de números en el aparato.

Actualmente, los circuitos para tarjetas SIM tienen una EEPROM de 8 Kbytes la cual es más que adecuada para los usuarios.

Aunque es muy factible que la funcionalidad del SIM para la operación básica de GSM sea incorporada y administrada como parte integral del aparato telefónico, los beneficios de un módulo removible residen en la creación potencial de servicios adicionales y para el desarrollo de GSM como una de varias aplicaciones de una tarjeta inteligente multiaplicación.

Las especificaciones actuales del SIM están definidas en el documento ETS 300.608 de la ETSI (*European Telecommunications Standards Institute*) conocido también como GSM 11.11. Este documento global define:

- La interfaz y protocolos a cada nivel (físico, eléctrico, lógico) entre el ME y el SIM.
- Los atributos lógicos necesarios para la operación de la red como el almacenamiento de la identidad del suscriptor.
- Características de seguridad y procedimientos.
- Características para incrementar la funcionalidad del MS.
- La funcionalidad del SIM para servicios de red que requieren soporte del MS.

Las características clave del suscriptor que proporciona actualmente el SIM son:

- Almacenamiento de los números telefónicos abreviados. Permite la memorización de los números usados frecuentemente y su almacenamiento asociado con etiquetas alfanuméricas.
- Almacenamiento de mensajes cortos. El servicio de mensajes cortos de GSM permite la transmisión de mensajes de texto de hasta 160 caracteres para ser enviados entre la red y el MS. Este mensaje puede ser almacenado en el SIM.
- Almacenamiento de operadores de red preferidos. Para permitir al suscriptor preseleccionar las redes a las que desea acceder cuando está en tránsito, ya que el MS automáticamente tratará de usar Roaming.
- Aviso de cargo. Para permitir que las unidades de llamado del suscriptor sean almacenadas en el SIM. Esta característica puede ser utilizada sólo para avisar al usuario o como base para la renta de un servicio SIM/Teléfono.
- Números telefónicos fijos. Para restringir los números que el suscriptor puede usar a sólo aquellos almacenados en una lista dentro del SIM.

Estas características son adicionales a los requerimientos primarios del SIM que son el manejo de los datos relacionados a acceso de red y seguridad.

Las interacciones operacionales entre la red, el ME y el SIM están definidas por los protocolos y procedimientos a través de las interfaces.

No existe una vía de comunicación directa entre la red y el SIM, los comandos para el SIM son generados siempre por el ME, o el ME reempaqueta los datos que recibe de la red antes de enviarlos al SIM.

La interfaz SIM/ME utiliza el protocolo definido en la norma ISO 7816/3 conocido como T=0. El protocolo opera como una relación estricta maestro/esclavo, el ME es el maestro y el SIM es el esclavo, por lo tanto no es posible para el SIM dar instrucciones al ME, la Figura 5.8 muestra la interacción actual entre la red, el ME y el SIM.

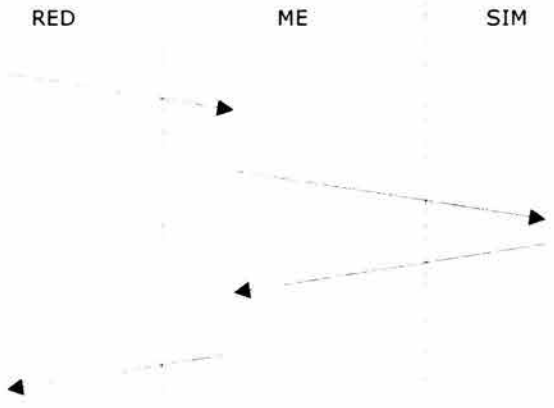


Figura 5.8 *Interacción entre la red, el ME y el SIM*

5.3.3 El papel de la tarjeta inteligente en la seguridad de GSM

La información del usuario es guardada en el registro HLR (*Home Location Register*) y por lo menos uno de estos es parte de cualquier red GSM, ver Figura 5.9.

Cuando el aparato móvil es encendido, se establece un interrogatorio entre el SIM y el MSC (*Mobile Switching Center*) para probar su validez y permitirle usar el sistema, además de encontrar la localización del equipo móvil.

El IMSI (*International Mobile Subscriber Identity*) del suscriptor es utilizado por el MSC local para obtener el registro HLR independientemente de donde se encuentre, y una prueba con una respuesta confirman el SIM. La información relevante es transferida al registro VLR (*Visitors Location Register*) y se realiza otra prueba al SIM del equipo móvil. Si la respuesta es correcta, el equipo es aceptado en la red.

En el momento en que el suscriptor se une a la red se emite una llave de autenticación Ki junto con el IMSI. La llave Ki es almacenada en el centro de autenticación en una base de datos y en el SIM del equipo móvil. En el centro de autenticación la llave es utilizada junto con un número aleatorio y dos algoritmos para producir tres piezas de datos para el sistema.

Estas tres piezas de datos son: una llave para codificar Kc (*Ciphering Key*), una respuesta firmada por el sistema SRES (*Signed REsponse System*) y un número aleatorio RAND. Estos son almacenados en el registro local y se les llama comúnmente tripleta.

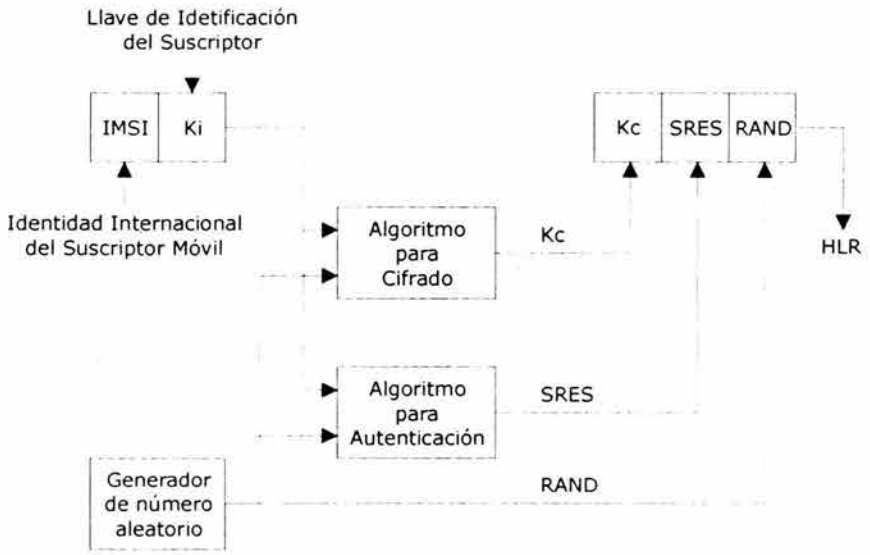


Figura 5.9 *Centro de autenticación*

La respuesta firmada es utilizada cuando la autenticación es requerida y esto sucede con cada proceso de registro, establecimiento de llamada, actualización de localización y antes de que se provean servicios suplementarios. La respuesta del equipo móvil debe ser correcta, de otra forma el equipo no es aceptado en la red. En la Figura 5.10 se muestra el procedimiento de autenticación.

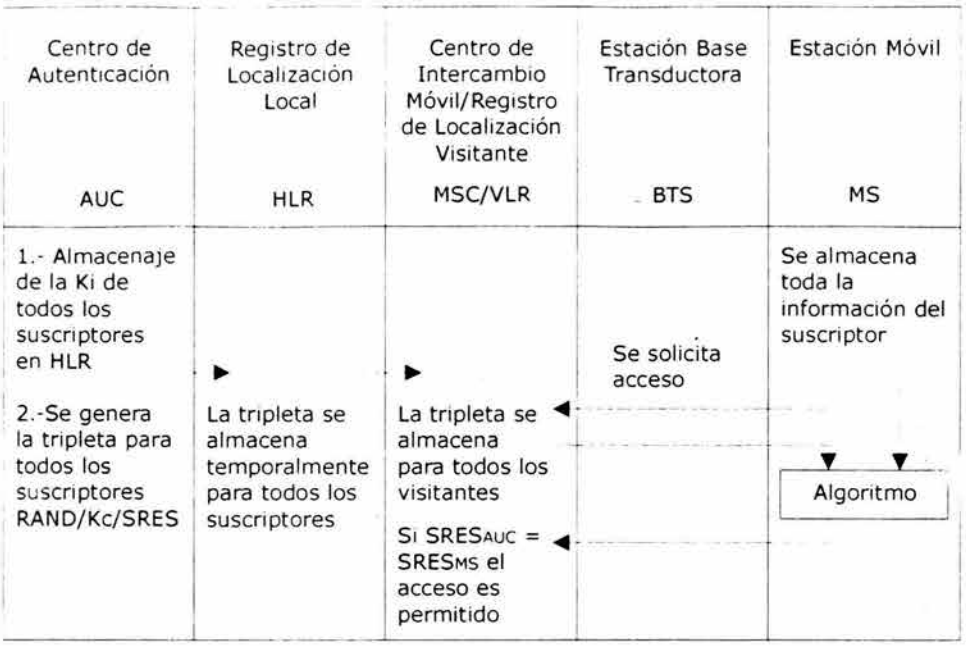


Figura 5.10 *Procedimiento de autenticación*

5.3.4 Aplicaciones futuras de la tarjeta inteligente en GSM

Para solucionar algunas desventajas del uso de un módulo SIM en la tecnología GSM, un grupo de características conocidas como "SIM Application Toolkit" está actualmente bajo estudio de un comité subtécnico responsable del SIM. La finalidad de estas características es la de proveer la funcionalidad primaria que será soportada por todos los ME en el futuro. Estas funcionalidades deberán incluir:

- Una ruta de datos entre la red y el SIM, y viceversa.
- Un mecanismo para permitir que la información ingresada a través del teclado del ME pase directamente al SIM.
- Un mecanismo para que el SIM inicie procedimientos en el ME.

En la Figura 5.11 se muestra la relación entre la red, el equipo móvil y el SIM proactivo.

Figura 5.11 *Principios del SIM proactivo*

Por consiguiente, el SIM y el ME son capaces de emitir comandos entre ellos, pero dentro de la reglamentación y en estricta concordancia con el protocolo T=0. Esto reduce los cambios requeridos en el ME para soportar el SIM proactivo.

Los operadores de red han reconocido el valor de considerar el SIM como extensión de su estructura de red inteligente. Los mecanismos anteriores dan la oportunidad a los operadores de red de controlar e influenciar el comportamiento del equipo y manejar la presentación de sus servicios al usuario.

Una vez que estos mecanismos estén completamente desarrollados, será posible que los operadores de red realicen aplicaciones en el SIM, las cuales podrán o no interactuar con el servicio de red para ejecutar la aplicación. La aplicación funcionará con cualquier ME que soporte el SIM Application Toolkit y el ME no tendrá que ser fabricado para alguna aplicación en especial. Estas aplicaciones definidas hasta el momento son descarga de perfil, SIM proactivo, descarga de datos al SIM, ingreso de datos al SIM por el teclado, control de la llamada por el SIM y envío de mensaje seguro los cuales se detallan a continuación.

5.3.4.1 Descarga de perfil

La descarga de perfil provee un mecanismo al ME para decir al SIM de lo que es capaz de hacer. El SIM puede entonces ajustar sus acciones a las capacidades del ME. El ME sabe cuales son las capacidades del SIM a través de la tabla de servicio del SIM (SIMST, *SIM Service Table*)

5.3.4.2 SIM proactivo

Las acciones que tomará el ME iniciadas por el SIM incluyen:

- Despliegue de texto del SIM al ME.
- Enviar un mensaje corto.
- Establecer una llamada de voz a un número contenido en el SIM.
- Establecer una llamada de datos a un número y sus capacidades portadoras contenidas en el SIM.
- Envío de controles o cadenas.
- Tocar un tono en el audífono.
- Iniciar un diálogo con el usuario.

5.3.4.3 Descarga de datos al SIM

La descarga de datos provee los mecanismos de transporte para transferir mensajes cortos (SMS, *Short Message Service*) punto a punto y mensajes transmitidos por la célula al SIM.

5.3.4.4 Ingreso de datos al SIM por teclado

Ha sido identificada la necesidad del usuario de iniciar una comunicación con el SIM. Si sólo una cadena ha sido definida, el ME necesita enviar el contenido al SIM, si es más de una, entonces el ME necesita también indicar al SIM cuál cadena será utilizada. El protocolo de

transporte básico ya ha sido definido, una vez iniciado el diálogo puede ser continuado a través del SIM proactivo.

5.3.4.5 Control de llamadas por el SIM

Cuando se active este servicio todas las cadenas de dígitos marcadas primero pasarán por el SIM antes que el ME establezca la llamada. El SIM tiene la habilidad de permitir, bloquear o modificar la llamada.

5.3.4.6 Envío de mensaje seguro

La especificación técnica depende de cómo sea requerida la autenticación. El uso del SIM en este aspecto será un elemento crítico de la red en la creación de servicios adicionales y se empezará a explotar al máximo las capacidades de procesamiento del SIM, inherentes a una tarjeta inteligente.

5.3.5 Tarjetas multiaplicación con funcionalidad SIM

En los años recientes se ha discutido mucho sobre las tarjetas multiaplicación y el SIM como una de las principales aplicaciones de la tecnología de las TI's. Es importante considerar el alcance de las interacciones entre las posibles aplicaciones que coexistirían en una tarjeta inteligente, y la complejidad de la administración de la tarjeta. Algunos de los aspectos que se deben considerar son:

- Dos o más aplicaciones en una tarjeta sin interactuar y/o compartiendo el acceso a datos comunes.
- Cargar aplicaciones junto con la personalización inicial.
- Agregar aplicaciones cuando se requiera en una tarjeta que ya contenga a otras.

Hay ciertas aplicaciones que serían incompatibles en una tarjeta multiaplicación y otras que son técnicamente compatibles y que ofrecen beneficios comerciales. En particular la compatibilidad con las especificaciones de EMV (*Europay*, *Mastercard*, *Visa*) será esencial para tener éxito en la fusión de los servicios de pagos y telecomunicaciones.

5.4 TARJETA TELEFÓNICA

El número de tarjetas telefónicas vendidas en el mundo supera el billón de unidades, ninguna otra aplicación se acerca a tal cantidad.

El desarrollo de las tarjetas inteligentes comenzó con la iniciativa de France Telecom de introducir TI's de prepago telefónico, seguido de la decisión de ETSI de adoptar el estándar GSM basado en tarjetas inteligentes.

Las tarjetas telefónicas de prepago fueron inventadas en Europa a mediados de los años setenta y tomó once años en llegar a Estados Unidos, desde entonces la industria de las tarjetas telefónicas ha tenido un crecimiento exponencial a nivel mundial.

5.4.1 Historia de las tarjetas telefónicas

1975. Las tarjetas telefónicas fueron inventadas en este año. La compañía involucrada no estaba en el ramo de las telecomunicaciones, era una empresa fabricante y proveedora de máquinas expendedoras.

1976. Se producen las primeras tarjetas de prepago y se ponen en el mercado de Italia para combatir el vandalismo en los teléfonos públicos. De hecho hubo una escasez de monedas en Italia y el robo de teléfonos fue muy común. Las tarjetas fueron introducidas con una banda magnética en el reverso para usarse en teléfonos especiales y combatir el robo de monedas. Las primeras tarjetas fueron muy delgadas y se atoraban frecuentemente.

1977. La utilización de las tarjetas de prepago de banda magnética se extendió por Europa, en particular en Austria, Suecia, Francia e Inglaterra. Llegaron a ser razonablemente populares.

1978. La tecnología inductiva fue inventada por Nelson G. Bardini en Brasil. El sistema usa una serie de bobinas insertadas en la tarjeta las cuales se quemaban cuando la tarjeta era utilizada. La tarjeta se mostró por primera vez en una exhibición en 1982.

1982. En Japón la Nippon Telephone and Telegraph introduce la primera tarjeta telefónica de prepago japonesa. Los pasajeros japoneses tenían que utilizar una gran cantidad de monedas para utilizar los teléfonos de los trenes subterráneos. La tarjeta japonesa fue considerablemente más conveniente y pronto se vendió a decenas de miles de pasajeros de los trenes de Osaka y Tokio.

1984. Francia experimenta con la tarjeta inteligente basada en un chip.

1987. El grupo World Telecom es la primera compañía en lanzar significativamente las tarjetas telefónicas en Estados Unidos. GPT un consorcio formado por las compañías Siemens y General Electric Company, desarrollaron y emitieron tarjetas con su propia tecnología magstripe. Esta es ahora la tecnología mas comúnmente usada en tarjetas magnéticas.

1988. El primer catálogo de tarjetas telefónicas para coleccionistas fue publicado por el Dr. Steve Hiscocks en Inglaterra.

1989. AT&T entra en el mercado de las tarjetas de prepago. Las primeras tarjetas telefónicas remotas aparecen en Hawaii.

1990. NYNEX ofrece la primera tarjeta no magnética en Estados Unidos. Estas eran tarjetas de prepago que utilizaban un PIN a manera de identificación. La tarjeta NYNEX permitía al usuario marcar un número 800 e ingresar su PIN para hacer llamadas de larga distancia. Este método permitió hacer llamadas desde cualquier teléfono en los Estados Unidos sin la necesidad de monedas o cargos por llamadas en los hoteles.

1992. Todas las compañías telefónicas más grandes regionales y de larga distancia incluyendo Sprint y muchos portadores pequeños ofrecen tarjetas de prepago. Los ingresos de esta industria alcanzan los 12 millones de dólares con la proyección de duplicar la cifra en los próximos años. Esta cifra resultó corta en el futuro.

1993. Las ventas de tarjetas telefónicas exceden los 25 millones. Más del doble que el año anterior.

1994. En un crecimiento exponencial la venta de tarjetas telefónicas excede los 250 millones de dólares.

1995. Las ventas llegan a 650 millones de dólares. La compañía US West provee la primera tarjeta telefónica basada en un chip. Sprint libera su "FONCARD" y Bell Atlantic descontinúa sus esfuerzos en tarjetas telefónicas.

1996. Las ventas de tarjetas telefónicas alcanzan el billón de dólares. American Express experimenta con una tarjeta de prepago de prueba.

1997. Las ventas alcanzan los 2 billones de dólares.

2000. Las ventas llegan a 3 billones sin que se vea fin a la expansión de las tarjetas. Las ventas proyectadas de la industria llegan a los 10 billones de dólares para el año 2010.

2001. Aparece la primera combinación de tarjetas celulares y telefónicas desechables.

2002. La empresa I-Link establecida como portadora de larga distancia, ofrece tarjetas telefónicas, correo de voz y llamadas en conferencia y otros servicios mejorados. Le fue otorgada la patente de voz sobre IP (VoIP, *Voice Over Internet Protocol*).

2002. Enhancecom lanza servicios de larga distancia incluyendo tarjetas telefónicas, correo de voz gratuito a través de su relación con I-Link.

2003. La compañía fabricante de tarjetas telefónicas Gemplus entrega su tarjeta número 3,000 millones a la compañía Telmex la cual vende aproximadamente 300 millones de tarjetas telefónicas al año siendo el primer consumidor de tarjetas inteligentes en el mundo seguido por China con 200 millones de tarjetas telefónicas al año.

5.4.2 ¿Por qué tarjetas telefónicas?

Las tarjetas telefónicas con un valor almacenado son una aplicación natural de las TI's, si se considera la alternativa de los teléfonos públicos de monedas, se deben tener en cuenta las siguientes desventajas para el operador del servicio y los usuarios:

- Se tendrían que construir teléfonos públicos o puntos de venta que soportaran determinados ataques de vandalismo.
- Se debería disponer de un mecanismo para vaciar los teléfonos con el consecuente riesgo de asalto.
- Las llamadas serían terminadas prematuramente cuando el usuario se quedara sin monedas.
- El operador del servicio sólo estaría cobrando por las llamadas realizándose actualmente.

Sin embargo, con las tarjetas inteligentes se pueden instalar teléfonos públicos menos costosos, colocarlos en lugares en los cuales no se consideraría colocar uno de monedas, se reduce el costo de la operación y el mantenimiento de los aparatos telefónicos y del personal ya que el dinero se vuelve "electrónico".

Muchos usuarios prefieren los teléfonos de tarjeta porque no tienen que preocuparse de llevar suficiente cambio para realizar una llamada. También, la TI cuenta con los mecanismos y técnicas necesarias de autenticación de tarjetas y teléfonos para evitar fraudes al sistema telefónico.

Pero una de las ventajas más importantes que vieron los operadores es que los usuarios pagan antes de que utilicen el servicio, e incluso algunos llegan a pagar por llamadas que nunca realizan, el valor de las llamadas pagadas por los usuarios y que aún no se realizan normalmente se denomina "flotante".

Además de todo esto, si se emiten tarjetas con un diseño e imagen atractivo se puede incrementar el ingreso considerablemente por medio de la venta del espacio en la tarjeta a anunciantes.

5.4.3 Generaciones de tarjetas telefónicas

5.4.3.1 Primera generación: EPROM

La primera tarjeta telefónica inteligente fue introducida en Francia a mediados de los años 80. Esta contenía una memoria EPROM la cual podía ser programada una sola vez.

Básicamente, una tarjeta telefónica de primera generación contiene en su interior una memoria de tipo EPROM de acceso serial. Las memorias de este tipo están formadas por una serie de fusibles, los cuales se queman o se dejan intactos para que posteriormente se interpreten como unos o ceros lógicos. Una vez que se quema un fusible, éste no puede volver a su estado inicial.

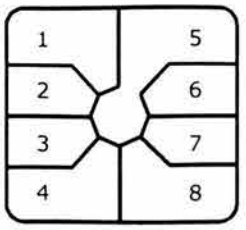
Cuando se inserta una tarjeta en una cabina, esta hace una serie de verificaciones iniciales y cuenta los fusibles que quedan sin quemar. Cada vez que se consume un tiempo determinado en las llamadas se quema uno de estos fusibles, hasta agotar el total de los disponibles.

Como no se pueden regenerar, las tarjetas originales son imposibles de recargar. La memoria de las tarjetas originales cuenta con una capacidad de 256 bits, es decir, 256 fusibles numerados del 0 al 255.

Poseen asimismo una entrada de reloj (CLOCK) que se usa para la selección de los fusibles deseados, una entrada de alimentación positiva (Vcc), una entrada de referencia (GND), una entrada de control de lectura y/o grabación, una entrada de RESET y por último, un contacto de salida de datos. En la Figura 5.12 se muestra la designación de los contactos en la tarjeta telefónica.

De los 256 bits disponibles, los primeros 96 están protegidos contra escritura; en esta zona se guarda la información correspondiente a la cantidad de pulsos a grabar, número de serie de la tarjeta, fabricante, país, empresa, etc.

De los 160 restantes, 10 se queman en fábrica a modo de prueba y los últimos 150 conforman el área de datos. La capacidad real de la tarjeta se basa en 150 unidades.



Pin 1 - Vcc +5 Volts de CD
Pin 2 - Din Entrada de Datos (También conocido como R/W)
Pin 3 - Entrada de Reloj
Pin 4 - Reset
Pin 5 - Tierra física (GND)
Pin 6 - Vpp +21 Volts.
Pin 7 - Dout Salida de Datos (También conocido como I/O)
Pin 8 - Sin uso

Figura 5.12 *Asignación de los contactos en la tarjeta telefónica*

5.4.3.2 Segunda generación: EEPROM

La memoria EEPROM es una tecnología más reciente, la cual permite que en el área de memoria del chip se pueda leer y escribir. Típicamente tiene una capacidad de conteo mucho mayor que la tarjeta EPROM, y el área extra puede ser utilizada para almacenar códigos secretos, lo cual reduce las posibilidades de que sea defraudado el operador del servicio.

5.4.3.3 Tercera generación: Eurochip/T2G

Nuevos circuitos de memoria de fabricantes como Siemens y Thomson han adicionado la capacidad de un algoritmo de prueba-respuesta al chip, permitiendo la autenticación del dispositivo en el cual se ha insertado la tarjeta.

Cada tarjeta es programada con un número de serie único y su propia llave secreta. Estos dispositivos tienen contadores no recargables capaces de contar hasta 20,000 unidades.

5.4.4 Futuro de las tarjetas telefónicas.

Las tarjetas telefónicas actualmente incluyen servicios adicionales, por ejemplo, cuentas de Internet prepagadas, servicios de correo electrónico, envío de mensajes cortos (SMS), correo de voz, servicio de telefonía celular, etc.

El futuro de las tarjetas telefónicas está ligado al desarrollo de las tarjetas inteligentes y sus aplicaciones. Ya existen hoy en día proyectos basados en tarjetas inteligentes que permiten utilizarlas como monederos electrónicos o como tarjetas telefónicas, por lo que en algunos años se podrá tener una sola tarjeta para utilizarla en aplicaciones de telecomunicaciones (telefonía pública, celular, etc.), bancarias y de débito/crédito, además de servir como elemento de seguridad y control de acceso.

5.5 APLICACIONES DE LA TARJETA INTELIGENTE EN MÉXICO

Las principales aplicaciones de las tarjetas inteligentes en México se pueden encontrar en los siguientes sectores y de las cuales se presentan algunos de sus ejemplos más importantes:

- Tarjetas bancarias de débito/crédito y monedero electrónico.
- Tarjetas de lealtad.
- Tarjetas de identificación multifuncionales.
- Tarjetas de control de acceso.
- Tarjetas prepagadas para teléfonos públicos.
- Pago y acceso a servicios.
- Internet/Redes.

5.5.1 Tarjetas bancarias de débito/crédito y monedero electrónico

El uso del chip en el sector financiero comenzó en México en mayo de 1998, cuando BBV, Serfin, Citibank-Confia, Bancrecer y Banorte arrancaron con un programa piloto en el municipio de San Pedro Garza García en Monterrey.

Las cuarenta sucursales de los cinco bancos participantes inicialmente emitieron 10,000 tarjetas VisaCash recargables, para ser utilizadas en los negocios afiliados. El mercado primario de usuarios fueron jóvenes entre 15 y 24 años, el cual se consolidó con los proyectos universitarios y representó alrededor de un 90% de las tarjetas.

El propósito de este proyecto fue que los bancos miembros dieran el primer paso en la migración de la tecnología de la banda magnética hacia el circuito integrado, además de analizar la respuesta de los comercios y los consumidores ante un nuevo medio de pago diseñado para el mercado de las compras menores. En una siguiente etapa se planea incorporar las funciones de débito/crédito, tarjeta telefónica, libretas de ahorro o inversión, vales de restaurante o despensa y programas de lealtad, entre otras. A este proyecto se incorporará el Banco Santander Serfin para aplicarlo entre estudiantes de la Universidad Anáhuac en el estado de México.

Visa International, líder mundial en sistemas de pago, calculó que el sistema bancario mexicano requiere al menos 100 millones de dólares para comenzar la migración de la banda magnética al chip. Esto, para adecuar los 12,650 cajeros automáticos y los lectores de las 70,000 terminales que los bancos tienen distribuidas en los comercios que reciben tarjetas bancarias en todo el país.

El mayor reto, es hacer compatibles las plataformas operativas existentes en México. Por un lado, está VisaCash que domina el mercado internacional de monederos electrónicos y cuya plataforma fue la primera que empezaron a usar los bancos mexicanos en Monterrey.

En segundo lugar, está el sistema operativo de Inbursa y Telmex, que arrancó en Plaza Cuicuilco en la ciudad de México. Y la más reciente, a punto de ser lanzada, es la de Mondex, perteneciente a una subsidiaria de MasterCard que busca acaparar la mayor parte del mercado nacional de TI's.

Cuando la homologación de esas tres se logre, el poseedor de una tarjeta inteligente en México podrá identificarse porque incluye fotografía, pagar consumos cotidianos como transporte, gasolina, etc. y portar datos personales u otra información. Este mercado en México asciende a 306,000 millones de dólares anuales, de los cuales apenas 5% se pagan con tarjeta de crédito.

5.5.1.1 B-Smart

Banamex tras su fusión con Citigroup, dio a conocer la primera tarjeta de crédito de este grupo financiero que incluye un chip. La tarjeta B Smart ofrece beneficios económicos y de seguridad ya que incorpora, independiente a la banda magnética, las facilidades de la tarjeta inteligente, la cual almacena y procesa información con un alto nivel de seguridad para compras por Internet, incluyendo una línea de crédito, infraestructura de llave pública (PKI) e identificador de Internet (*Internet ID*). Los usuarios pueden solicitar sin costo un lector para la tarjeta facilitando las operaciones por Internet.

Es importante mencionar que la banda magnética se sigue utilizando para realizar pagos en establecimientos afiliados, ya que la mayoría de los negocios no cuentan con terminales para la lectura de la TI.

B-Smart es una membresía con beneficios que incluyen los siguientes conceptos: Smart Value, que ofrece descuentos automáticos al momento de la compra; Smart Key, llave integral de acceso al crédito; y Smart Credit, que ofrece al cliente una pre-aprobación crediticia.

En la Figura 5.13 se muestra la tarjeta B-Smart de Banamex.

Figura 5.13 *Tarjeta Banamex B-Smart*

5.5.1.2 Cuenta con Telmex

Cuenta con Telmex es una tarjeta de débito/crédito, y en un futuro será monedero electrónico, que promueve el banco Inbursa y la compañía telefónica Telmex. Es una tarjeta inteligente que brinda una mayor seguridad al momento de efectuar operaciones. Es aceptada en establecimientos afiliados al sistema de Telmex, en cajeros automáticos del Banco Inbursa, en cajeros del sistema Red y Plus, y en los aparatos de teléfonos públicos de Telmex, para llamadas tanto locales como de larga distancia.

Esta tarjeta se puede cargar de dos formas diferentes:

- A través de una clave asignada, se puede cargar la tarjeta en cualquiera de los 150,000 teléfonos públicos habilitados para ello y la cantidad de dinero que se ocupó, aparecerá en el recibo telefónico, esta cantidad podrá ser de $50 hasta $1,000 pesos.
- También se puede cargar la tarjeta realizando depósitos en cualquiera de las 370 sucursales de Telmex.

Una vez que se tiene saldo en la tarjeta, se pueden realizar disposiciones de efectivo en cajeros automáticos Inbursa, en el sistema Red y Plus, y realizar llamadas telefónicas, nacionales e internacionales.

En un futuro, esta tarjeta funcionará como monedero electrónico, es decir se podrán realizar pagos en establecimientos afiliados al sistema y se estima que para el segundo semestre del año en curso, se podrán pagar impuestos, así como diversos servicios, por ejemplo, el pago en gasolineras o en cines.

Hoy en día el programa ha establecido alianzas con 110 socios comerciales entre los que destacan Sanborns, MixUp, Gigante, DirecTV, Mexicana, Fiesta Americana y Blockbuster.

También funcionará como una tarjeta de lealtad ya que el usuario recibirá puntos por consumo los cuales podrán ser utilizados para hacer llamadas, o comprar productos en la tiendas Telmex. En la Figura 5.14 se muestra una imagen de esta tarjeta.

Figura 5.14 *Tarjetas Telmex-Inbursa*

5.5.1.3 Uni-K

El Grupo Santander Serfin puso en el mercado otra tarjeta de crédito inteligente, pero más enfocada a ofrecer beneficios en el cobro de comisiones, la tarjeta Uni-K no cobra comisión anual de por vida, siempre y cuando se utilice al menos una vez al mes. Entre los beneficios de Santander Serfin, destacan que a través de la Uni-K pueden elegir la fecha de pago que más convenga, si se quiere que tenga o no aceptación en cajeros, o si se requiere una Tarjeta Adicional Virtual para comprar con mayor seguridad en Internet o por catálogo.

5.5.1.4 Bancomer Infinite

La tarjeta de crédito Bancomer Visa Infinite, es el producto más exclusivo de la familia de tarjetas de crédito Bancomer. Está dirigida al segmento de clientes de la Banca Patrimonial y ofrece altos estándares de funcionamiento, operación y seguridad.

Es un producto ampliamente conocido y aceptado en Latinoamérica y el mundo, el cual se emite bajo el respaldo de la marca Visa. El monto máximo que se puede retirar en los

cajeros automáticos es de $4,000 pesos por día y el monto máximo a retirar en sucursales Bancomer es de 10,000 dólares por día. El retiro diario máximo en el extranjero es de 5,000 dólares. En la Figura 5.15 se muestra la tarjeta Bancomer Infinite.

Figura 5.15 *Tarjeta Bancomer Infinite*

5.5.2 Tarjetas de lealtad

El objeto de un programa de lealtad es el de retener clientes regulares, acrecentar el compromiso y acercamiento de clientes ocasionales y captar nuevos clientes. Al desarrollar programas de lealtad para los clientes se puede tener un mejor entendimiento de sus necesidades y guiarles mejor para satisfacer las mismas, logrando con ello:

- Lograr que los clientes regulares compren artículos de mayor precio.
- Atraer más clientes, con condiciones de pago óptimas.
- Hacer sentir al cliente que es parte importante de la empresa.
- Identificar inmediatamente al cliente preferencial.
- Ofrecer y realizar transacciones rápidas y convenientes sin demoras.
- Hacer que las transacciones y pagos automatizados sean simples y seguros.
- Ser más competitivo con base al servicio y valor agregado, y no con precios.
- Desarrollar segmentación de clientes para ventas orientadas.
- Proporcionar servicios "a la medida" de acuerdo a las preferencias individuales.
- Desarrollar estrategias de promoción y publicidad directa y personalizada.

Cinemark ha puesto en operación campañas publicitarias para otorgar premios a sus clientes constantes, ofrecen la opción de acumular puntos y ganar productos a través de esta herramienta. A los clientes se les entrega una tarjeta donde se registra el número de veces que compran un boleto o consumen productos en la dulcería.

El procedimiento para adquirirla es presentar en las taquillas cinco boletos de entradas diferentes en un mes, lo que les da derecho a seguir acumulando puntos por cada compra que se realice. Cinemark invirtió alrededor de $1 millón de pesos para adquirir la máquina que crea las tarjetas. También hay lectores en las taquillas y dulcerías. Entre los premios que ofrece se encuentran palomitas de maíz, entradas gratis, camisas y aparatos electrodomésticos. Al momento, cuentan con más de 5,000 clientes distinguidos, quienes son invitados especiales en los estrenos de películas.

Cinemex lanzó una estrategia similar basada también en tarjetas inteligentes. El programa Invitado Especial Cinemex es un programa de recompensas que permite acumular puntos, los cuales se pueden canjear por diversos productos como palomitas de maíz, refrescos, y

boletos de cine, además de otros beneficios exclusivos para los miembros de este programa. Desde que el usuario se inscribe al programa Invitado Especial, se puede hacer uso de la tarjeta acumulando puntos por cualquier compra que se realice, ya sea en taquilla, dulcería, cafetería y compras en Internet o en la línea Cinemex. En la Figura 5.16 se muestra la tarjeta Invitado Especial.

Figura 5.16 *Tarjeta de lealtad Cinemex*

5.5.3 Tarjetas de identificación multifuncionales

5.5.3.1 Tecnológico de Monterrey

El Tecnológico de Monterrey utiliza una credencial inteligente dentro de sus campus, la cual además de contener los datos, fotografía y un PIN del alumno también sirve de monedero electrónico.

El monedero electrónico permite realizar transacciones electrónicas para efectuar pagos de forma rápida y segura. Son utilizados como un reemplazo de moneda fraccionaria para pago de fotocopias, libros y otros artículos.

Dentro de los beneficios para el Tecnológico de Monterrey, se encuentran:

- La continuidad del programa Campus Seguro, ya que con la credencial inteligente, se logra al 100% identificar a cada una de las personas que ingresan al campus, ya que ésta es portada por los alumnos, así como personal administrativo y docente, convirtiéndose en la única llave de acceso a las instalaciones.
- Agilizar los cobros y el control administrativo en los establecimientos del campus, así como el proceso de control de asistencia.

Los beneficios para el alumno al utilizar el monedero electrónico son:

- Pago de productos y servicios en cafeterías, laboratorios de cómputo, biblioteca, y otros.
- Permite llevar una mejor administración de los gastos efectuados dentro del campus.
- Facilidades para recibir transferencias desde una cuenta bancaria a través del depósito en cualquier sucursal Bancomer.
- Rapidez de pago de productos y servicios.
- Generación de un historial bancario.

En la Figura 5.17 se muestra un ejemplo de la credencial inteligente del Tecnológico de Monterrey.

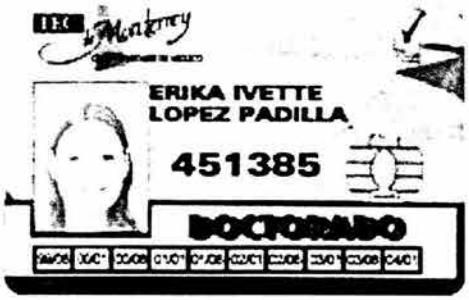


Figura 5.17 *Credencial inteligente del Tecnológico de Monterrey*

5.5.3.2 Tarjeta Inteligente Universitaria Bital

Es una tarjeta de identificación para estudiantes y maestros de las escuelas participantes que los acredita como miembros de la comunidad universitaria del sistema. Esta puede ser utilizada para efectuar funciones universitarias, bancarias, pagos o compras.

Ha sido desarrollada con la tecnología de la TI, que brinda una variedad de servicios, posee los mecanismos de control que garantizan confidencialidad en la información y la seguridad necesaria, tanto para la escuela como para los estudiantes y maestros.

La Tarjeta Inteligente Universitaria Bital puede ser utilizada por estudiantes y maestros a manera de:

- Identificación.
- Control de accesos físicos y lógicos.
- Acceso a áreas restringidas.
- Acceso a información del expediente académico.
- Préstamo de libros en las bibliotecas.
- Toma de asistencia.
- Medios de pago con banda magnética y monedero electrónico.

Es una tarjeta Visa/Electron aceptada nacional e internacionalmente, cuenta con monedero electrónico que permite pagar los servicios dentro del plantel (fotocopias, cafetería, etc.) y también con banda magnética que permite pagar en todos los establecimientos que acepten tarjetas Visa. Además, permite retirar efectivo en cajeros automáticos.

5.5.3.3 Súper cuenta universitaria Santander Serfin

Es una cuenta bancaria que se liga a una credencial inteligente y funciona como identificación personal de alta seguridad para el control de acceso a edificios e instalaciones universitarias, ya que además de ser una tarjeta plástica representativa de la institución, incorpora la fotografía del usuario ya sean alumnos, administrativos o docentes; también tiene una banda magnética y código de barras para que pueda ser empleada en las actividades diarias del campus.

Ofrece la posibilidad de ser utilizada como monedero electrónico dentro de las instituciones de educación superior formalizadas por el programa Universidades. Con este monedero electrónico se pueden pagar consumos por montos pequeños. Los pagos y consumos con el monedero electrónico no generan ninguna comisión y se puede retirar dinero en efectivo en las sucursales designadas por Santander Serfin, según la universidad.

Este monedero permite portar desde $100 hasta $1,500 pesos para el pago de servicios y consumos dentro del Campus Universitario en establecimientos afiliados a VisaCash, además, permite disponer de efectivo en ventanilla de las sucursales designadas por Santander Serfin hasta por el monto total existente en el chip. Para depositar y retirar dinero del monedero se debe acudir a la sucursal designada a la institución.

El monedero electrónico está exento de comisiones, sin embargo, en caso de pérdida o robo de la credencial inteligente, el dinero que se encuentre cargado en el monedero electrónico al momento de la pérdida no se puede recuperar ya que es como perder dinero en efectivo.

Esta tarjeta también ofrece recompensas por uso en compras, se puede pagar por el momento el recibo de teléfono y sólo puede ser contratada si la institución universitaria formaliza un convenio con el programa Universidades de Santander Serfin.

Un ejemplo de este programa es la Universidad del Mayab que ya cuenta con la credencial inteligente, ver Figura 5.18, la cual se utiliza como identificación oficial dentro de las instalaciones del campus como la biblioteca y centro de cómputo, además de utilizarla como monedero electrónico para consumos dentro de la universidad. Existe también un programa piloto para establecer esta credencial en la Universidad de Guadalajara.

Figura 5.18 *Credencial inteligente de la Universidad del Mayab*

5.5.3.4 Tarjeta inteligente del sistema de bibliotecas de la UASLP

En la Universidad Autónoma de San Luis Potosí se utiliza la tarjeta inteligente Unicard que por el momento sirve para tener acceso al servicio de Internet en las bibliotecas y como monedero electrónico.

Si se requiere utilizar una computadora conectada a Internet en alguna de las bibliotecas, se debe insertar la tarjeta en una ranura que la computadora tiene para este fin. El costo del uso de Internet y las impresiones que hagan se descuentan de la cantidad de dinero que se tiene en la tarjeta. El depósito de dinero en la tarjeta se realiza a través del centro de cómputo.

5.5.4 Tarjetas de control de acceso

Uno de los mayores campos de aplicación de las TI's en México es la del control de acceso físico, son utilizadas generalmente en instituciones de gobierno, corporativos, estacionamientos, etc. Algunas dependencias que utilizan estas tarjetas son: el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, la Secretaría de Hacienda y Crédito Público, la Secretaría de Gobernación etc., y corporativos como: 3M de México, Xerox Mexicana, y otros.

5.5.5 Tarjetas prepagadas para teléfonos públicos

Sin duda, el mayor éxito de las TI's en México ha sido su uso en las tarjetas telefónicas de prepago, donde la mayor participación la tiene la compañía Teléfonos de México con las tarjetas Ladatel. Cuando se incursionó en esta aplicación se vendían 11 millones de tarjetas Ladatel por año, hoy en día se consumen 300 millones de tarjetas telefónicas colocando a México como el mayor consumidor del mundo.

El 80% de las tarjetas telefónicas vendidas son tarjetas de $30 pesos, el 18% son tarjetas de $50 pesos y el 2% restante es de tarjetas de $100 pesos. En la Figura 5.19 se muestra una imagen de este tipo de tarjetas.

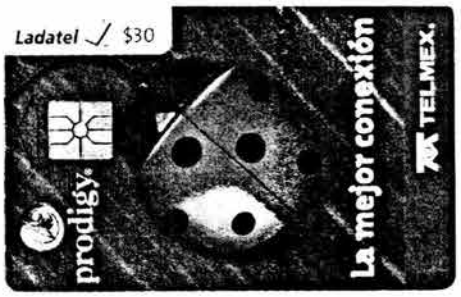


Figura 5.19 *Tarjeta telefónica Ladatel*

5.5.6 Pago y acceso a servicios

Algunas de las aplicaciones de pago y acceso a servicios con tarjetas inteligentes utilizadas en México, son los servicios de televisión directa al hogar vía satélite que proporcionan las compañías DirecTV y Sky cuyos equipos de recepción requieren de una TI para poder tener acceso a la señal, y el pago de servicios en gasolineras de las compañías Hidrosina y Grupo Mexicano los cuales ofrecen a sus clientes tarjetas inteligentes para el control de consumos por día, por mes, por litros, etc.

Otro ejemplo, es la TI para el pago de servicios de transporte Caminante la cual sirve para pagar tarifas de transporte en estos autobuses.

Es importante mencionar que se reactivó el proyecto para poner en funcionamiento el uso de la tarjeta inteligente en el servicio de transporte colectivo Metro en el año 2004, estas tarjetas serán recargables por números de viajes.

5.5.7 Internet/Redes

Un ejemplo de este tipo de aplicación es el cyber-café, donde el acceso a Internet o a la computadora se valida con una tarjeta inteligente además de que pueden ser cargadas con tiempo de navegación.

5.6 PROVEEDORES DE SOLUCIONES EN MÉXICO

Los fabricantes ofrecen una gran variedad de TI's que abarcan varios niveles de seguridad para diferentes aplicaciones. Poseen también diversas capacidades de memoria, pudiendo almacenar un gran número de datos e información. En México se fabrican tarjetas inteligentes, y también son introducidas en el mercado por medio de proveedores de soluciones o representantes de las empresas fabricantes extranjeras.

A continuación, se presentan algunos de los proveedores de TI's y soluciones en México.

5.6.1 Gemplus

Gemplus es una empresa francesa, principal proveedora mundial de soluciones para tarjetas inteligentes, en México lleva más de diez años trabajando con Telmex.

Ofrece una amplia gama de soluciones personalizadas que incluyen servicios de datos móviles, banca interoperativa, identidad, WLAN, comercio móvil, entre otras. En 2002, Gemplus fue el líder mundial en la fabricación de TI's.

Entre los 80 clientes mundiales de Gemplus se encuentran CANTV, Venezuela, China NetCom, China Telecom, Deutsche Telekom, France Telecom, Menatel y Telmex México; este último es el mayor cliente de este campo. Gemplus cuenta con una planta para la fabricación de TI's en la ciudad de Jiutepec, Morelos.

Página web: www.gemplus.com

5.6.2 Schlumberger

Ofrece servicios y soluciones en tecnología. La empresa se divide en tres áreas principalmente. Schlumberger Oilfield Services, suministra una amplia gama de servicios para la industria del petróleo y gas. SchlumbergerSema, es proveedor de tecnologías de información, integración de sistemas y redes, servicios de infraestructura a la industria de energía, así como al sector público, telecomunicaciones y mercados de finanzas. WesternGeco, asociado con Baker Hughes está enfocada a los estudios de superficies sísmicas.

Página web: www.slb.com

5.6.3 ProSoft2000

ProSoft 2000, S.A. de C.V., inició operaciones en el año 1990. Entre las soluciones de la TI que ofrece ProSoft2000 están las de débito/crédito, identificación personal, monedero electrónico, lealtad, accesos y certificados digitales.

Página web: www.prosoft2k.com

5.6.4 SignusCard

Empresa mexicana con operaciones en Chihuahua, Chihuahua, es representante exclusivo para Estados Unidos y México de Global Magnetic Card Company, la compañía fabricante de tarjetas magnéticas e inteligentes más grande de Asia. Tiene una producción anual superior a los 300 millones de unidades.

Página web: www.signuscard.com

5.6.5 Giesecke & Devrient

Giesecke & Devrient

Hace más de 25 años que G&D produce tarjetas de pago, como por ejemplo, tarjetas Eurocheque y tarjetas bancarias de débito/crédito. En 1984 inició la producción de TI's a gran escala. Participa activamente en el desarrollo de proyectos que involucran pagos electrónicos y de soluciones multifuncionales seguras para:

- Tarjetas de débito/crédito.
- Monederos electrónicos.
- Plataformas de desarrollo para tarjetas.
- Comercio electrónico y tarjetas multimedia.
- Soluciones en telecomunicaciones.

Página web: www.gdmex.com

5.6.6 Acerta

ACERTA

Acerta distribuye y provee soluciones basadas en las TI's fabricadas por American Pacific. Se encarga desde la planeación de la aplicación, el diseño de las tarjetas, la implementación de los sistemas de seguridad y la venta de los lectores, hasta el arranque del sistema.

Página web: www.acerta.net

5.6.7 Afina

Fundada en 1990, inició su trayectoria especializándose en el entorno de los sistemas operativos Unix. Afina, en alianza con la empresa española Secuware, provee soluciones con TI's para control de accesos de máxima seguridad. A lo largo de sus más de diez años de experiencia, se ha introducido en nuevos mercados, estando presentes en España, Portugal, México, EEUU, Colombia y Venezuela.

Página web: www.afina.com.mx

5.6.8 BarMax

BarMax es una compañía que comenzó sus operaciones en 1995 con sistemas de recolección de datos. Es distribuidor de sistemas de control de acceso y ofrece la línea Radio Key que son unidades para el control de acceso por proximidad, es decir, a través de TI's sin contactos.

Página web: www.barmax.com

5.6.9 Qualtec

Por más de 9 años Qualtec México ha estado aplicando soluciones de identificación automática a todo tipo de negocios. Qualtec ofrece QTime que es una solución integral para el control de personal de una empresa y cuenta entre sus productos con sistemas de fotocredencialización con TI's.

Página web: www.qualtecmx.com.mx

5.6.10 Datatec

Sistemas y Accesorios Datatec S.A. de C.V. es una compañía mexicana fundada en 1983 en Guadalajara, Jalisco. En 1995 inició con la venta de soluciones relacionadas con tarjetas de identificación, básicamente hardware y software para el control de accesos.

Posteriormente, amplió sus aplicaciones entrando en el campo de monederos electrónicos enfocándose al segmento educativo, concretamente universidades.

Página web: www.datateccards.com

5.6.11 Identicod

Identicod

Entre sus productos se encuentran las terminales para el control de acceso y asistencia con tecnologías de código de barras, banda magnética, tarjeta inteligente, identificación de palma e identificación de huella dactiloscópica.

Página web: www.identicod.com.mx

Modelo para la Aplicación de la TI

- Propuesta para la Facultad de Ingeniería
- Modelo para la aplicación de la TI en el Departamento de Ingeniería en Computación
- Propuesta del tópico para la asignatura de temas especiales

Capítulo 6

CAPÍTULO 6. MODELO PARA LA APLICACIÓN DE LA TARJETA INTELIGENTE

Tradicionalmente en un campus los estudiantes necesitan portar varias credenciales. La mayoría de estas son requeridas para propósitos de autorización e identificación. Esto no sólo conduce a una sobre carga administrativa al tener que llevar un control de todas ellas, sino también el reto de manejarlas y validarlas, y en muchas ocasiones por sistemas administrativos independientes.

La Facultad de Ingeniería de la UNAM, además de utilizar la credencial como medio de identificación común para estudiantes, docentes y administrativos, podría implementar un sistema basado en tecnología de tarjetas inteligentes que permite el manejo de varias aplicaciones distintas dentro de la misma tarjeta.

Además, se puede expandir su uso para facilitar el acceso a ciertos recursos (préstamo de libros, laboratorios, centros de cómputo, etc.), o también, se pudiera utilizar como monedero electrónico y tarjeta de débito. Aplicaciones más avanzadas incluirían el registro de historiales académicos, horarios, tira de materias y entrada a servicios educativos en línea. También tiene la ventaja de que su renovación, generalmente semestral o anual, puede realizarse de forma automatizada sin necesidad de nuevos trámites administrativos.

6.1 PROPUESTA PARA LA FACULTAD DE INGENIERÍA

Es necesario definir el alcance que una aplicación como ésta puede tener para satisfacer las necesidades de las personas que acuden a la Facultad, debido a que son varias las actividades que se realizan dentro de ella, algunos ejemplos se enlistan a continuación en la Tabla 6.1.

	Usuarios		
Necesidades	**Docente**	**Administrativo**	**Estudiantil**
Identificación	✓	✓	✓
Asistencia	✓	✓	
Nómina	✓	✓	
Pago de servicios escolares			✓
Trámites	✓		✓
Centros de cómputo	✓		✓
Préstamo de libros	✓		✓
Fotocopiado			✓
Librería			✓
Laboratorios	✓	✓	✓
Oficinas		✓	
Cubículos	✓	✓	
Comedor	✓	✓	✓
Estacionamiento	✓	✓	
Sanitarios	✓	✓	
Monedero electrónico	✓	✓	✓
Cajeros automáticos	✓	✓	✓

Tabla 6.1 *Posibles usos de la TI dentro de la Facultad de Ingeniería*

Con base en lo anterior se presenta el modelo conceptual de un sistema basado en la tecnología de tarjetas inteligentes considerando los siguientes objetivos:

- Ser un medio de identificación confiable.
- Contar con un mecanismo de seguridad para el acceso a distintas áreas.
- Servir como instrumento para el pago o cobro de diversos servicios.

A cada alumno y/o empleado se le proporcionaría una tarjeta inteligente como su credencial. Esta tarjeta llevaría impresos los datos necesarios como: nombre, carrera, fotografía, número de cuenta/trabajador, CURP y firma.

Dentro de la TI se grabarían los datos del alumno o docente, la información de las áreas a las que tiene acceso y se prepararía un área para el control de los libros en préstamo de la biblioteca y del material de laboratorio. Adicionalmente se podría cargar en la tarjeta una aplicación de monedero electrónico en alianza con una institución bancaria. Algunas de las aplicaciones que podría tener la TI en un ambiente multiaplicación se muestran en la Figura 6.1.

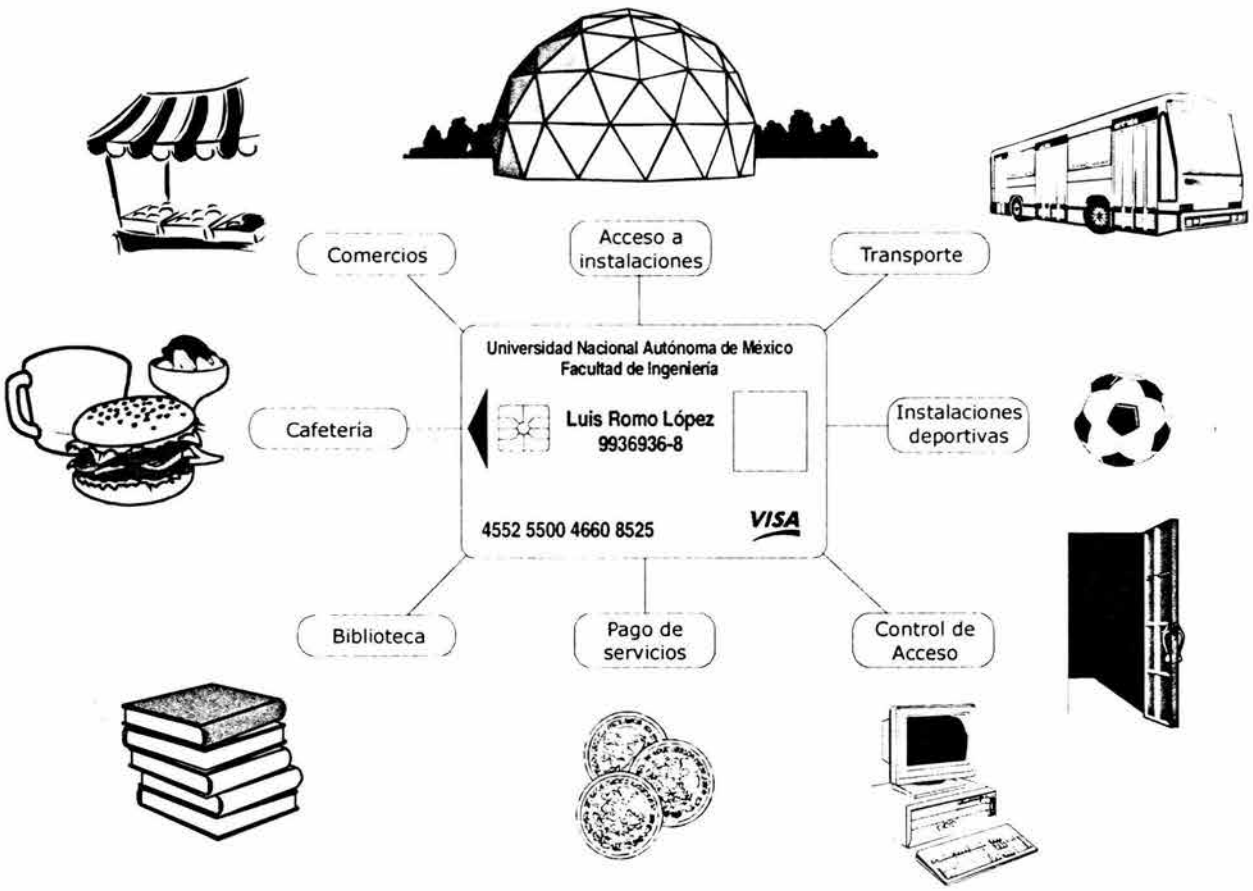


Figura 6.1 *Utilización de la TI*

Los diferentes puntos en los que se dan servicios dentro de la Facultad, se deberán equipar con un lector de tarjeta inteligente para poder atender los pagos y los controles que se lleven a cabo por medio de la credencial inteligente.

Una vez que se termine el ciclo escolar, la tarjeta ya no será válida para el alumno hasta después de la inscripción al siguiente período escolar. Además, podrá invalidarse la tarjeta en el momento que se prescriban las fechas de entrega de los libros en préstamo de la biblioteca o adeudo de material de laboratorio, hasta que se efectúe el pago de la deuda correspondiente.

El alumno o empleado puede pagar cualquiera de los servicios ofrecidos (telefonía pública, máquinas expendedoras) por la facultad a través del monedero electrónico.

La integración de la TI a las actividades de la facultad puede ser planeada para incorporarse o reemplazar eventualmente las credenciales emitidas para las diferentes actividades (identificación, biblioteca, acceso físico, acceso a redes, etc.).

Para llevar a cabo un proyecto como el propuesto, se requiere la participación de diferentes compañías involucradas en el ciclo de vida de la TI dentro de la aplicación para la facultad, en la Figura 6.2 se muestra este ciclo de vida.

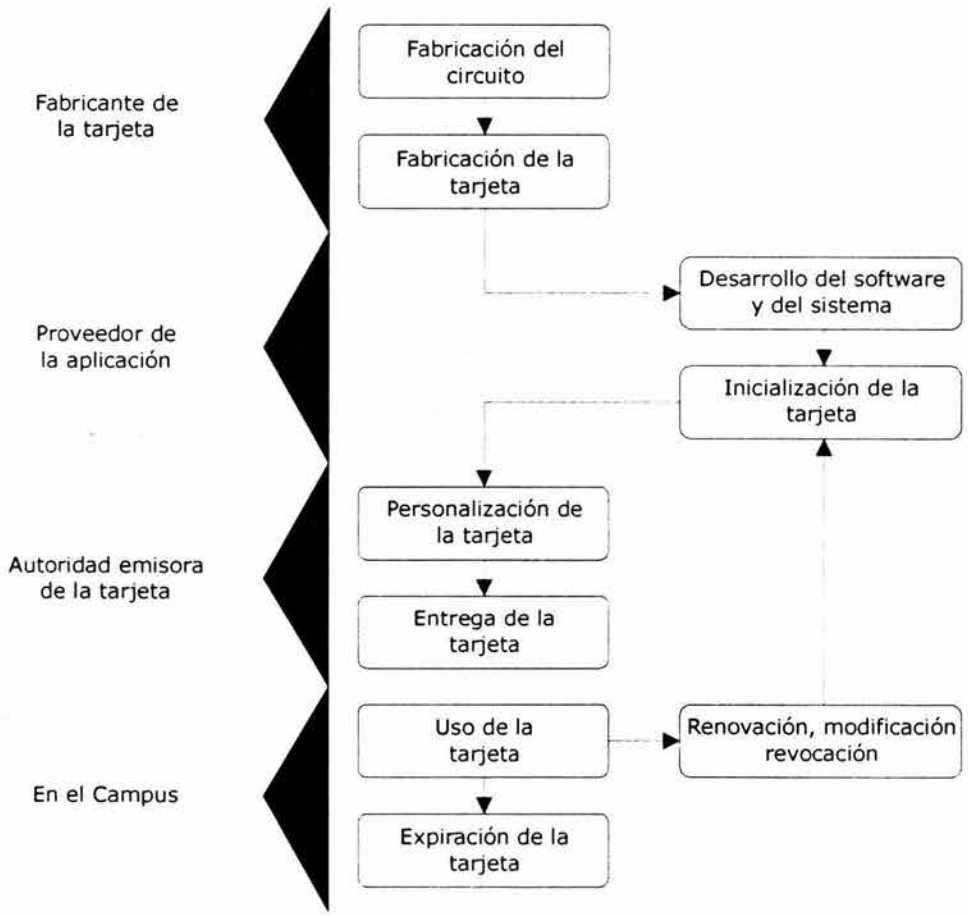


Figura 6.2 *Ciclo de vida de la TI en un campus*

- Fase de manufactura de la tarjeta. Es llevada a cabo por el fabricante de la TI.

- Fase de la aplicación de la tarjeta. Es realizada por el proveedor de la aplicación quien se encarga del desarrollo del sistema y del software. Este proveedor trabaja en conjunto con la facultad para determinar las características necesarias del chip y la tarjeta, también lleva a cabo la inicialización de la misma.

- Fase de emisión de tarjetas. Es conducida por la autoridad designada por la facultad, se realiza la personalización y entrega de las tarjetas.

- Fase de utilización. En este periodo el alumno y/o empleado hace uso de la tarjeta, pueden realizarse procesos de renovación, modificación y revocación. La última etapa en la vida de la tarjeta es la expiración.

Las fases de manufactura y aplicación de la tarjeta se detallan en el apartado 2.6, las fases de emisión y uso se explican a continuación.

6.1.1 Personalización y entrega

El alumno o empleado acuden al área designada por la facultad, ver Figura 6.3, donde solicita la expedición de su tarjeta inteligente. El responsable de este servicio, verifica la validez de la petición y registra en el sistema el número de alumno/empleado. Emite la solicitud de tarjeta y la entrega al solicitante.

Se graba en la tarjeta la información concerniente específicamente al portador de la tarjeta, cada tarjeta es registrada en una base de datos para su administración y manejo en una institución bancaria, esto es, se envían los datos del usuario al banco para que se le asigne un número de cuenta para utilizar su tarjeta como monedero electrónico.

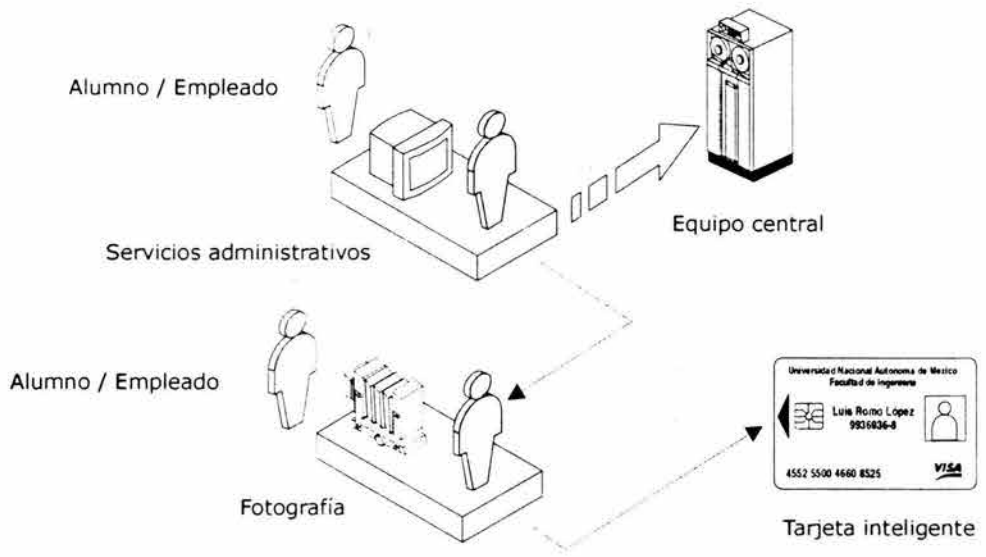


Figura 6.3 *Expedición de la tarjeta inteligente*

6.1.2 Utilización

Una vez que han sido emitidas las tarjetas, es necesario llevar a cabo ciertos procesos para la administración de las mismas, como control de saldos, emisión de estados de cuenta, modificación, renovación, y cancelación de tarjetas asimismo la emisión de algunos reportes de interés para la facultad, ver Figura 6.4. La autoridad designada por la facultad determinará bajo que condiciones expira la tarjeta.

Figura 6.4 *Administración de procesos*

6.2 MODELO PARA LA APLICACIÓN DE LA TI EN EL DEPARTAMENTO DE INGENIERÍA EN COMPUTACIÓN

El departamento de Ingeniería en Computación de la Facultad de Ingeniería cuenta con una importante infraestructura de equipo, indispensable para desarrollar sus actividades académicas y de investigación, pero es necesario un sistema que controle el acceso a las instalaciones de manera confiable. Por lo que es de suma importancia diseñar una solución que resuelva este problema.

El uso de una tarjeta inteligente como identificación garantiza un acceso autenticado a recursos tanto físicos como virtuales. La credencial puede autorizar el acceso a laboratorios, cubículos, redes de cómputo, archivos o computadoras personales. En adición, en un futuro la misma tarjeta podría ser utilizada para aplicaciones de pago de servicios, control de asistencias, etc. El objetivo del presente estudio es introducir la tecnología de TI's para el control de acceso físico a las zonas que comprenden el departamento de Ingeniería en Computación como un primer paso a implementaciones más elaboradas.

Los pasos listados a continuación se tomaron como referencia para el desarrollo del sistema de control de acceso:

- Determinar el objetivo del sistema.
- Identificar los requerimientos.

- Especificar los niveles de seguridad.
- Seleccionar el equipo requerido.
- Describir el sistema de administración.

6.2.1 Determinar el objetivo del sistema

El objetivo del sistema es el control eficiente del acceso físico del personal docente, administrativo y de intendencia a las áreas de laboratorios, cubículos, baños y zonas de acceso mediante TI's, así como también contar con un sistema que permita la administración de la información y las tarjetas, y además la obtención de reportes para un análisis posterior.

6.2.2 Identificar los requerimientos

El departamento de Ingeniería en Computación se encuentra localizado en la planta baja y en el segundo piso del edificio Valdés Vallejo del anexo de la Facultad de Ingeniería, los accesos a las áreas que deberán ser controlados se detallan en la Tabla 6.2 para los ubicados en la planta baja y en la Tabla 6.3 para los ubicados en el segundo piso. En la Figura 6.5 y Figura 6.6 se muestran los planos de la ubicación de las áreas que componen este departamento.

Planta Baja:

No.	Área	Código
1	Laboratorio de Redes	LR
2	Laboratorio de PLD's	LPLD
3	Laboratorio de Multimedia	LMM
4	Laboratorio de Interfaces Inteligentes	LII
5	Laboratorio de Computación Salas A y B	LCAB
6	Baños mujeres	BM1
7	Baños hombres	BH1

Tabla 6.2 *Accesos planta baja*

Segundo piso:

No.	Área	Código
8	Laboratorio de Microcomputadoras	LMC
9	Laboratorio de Memorias Periféricos	LMP
10	Puerta de acceso cubículos sección A	CSA
11	Puerta de acceso cubículos sección B	CSB
12	Laboratorio de Computación Sala C	LCC
13	Baños mujeres	BM2
14	Baños hombres	BH2

Tabla 6.3 *Accesos planta alta*

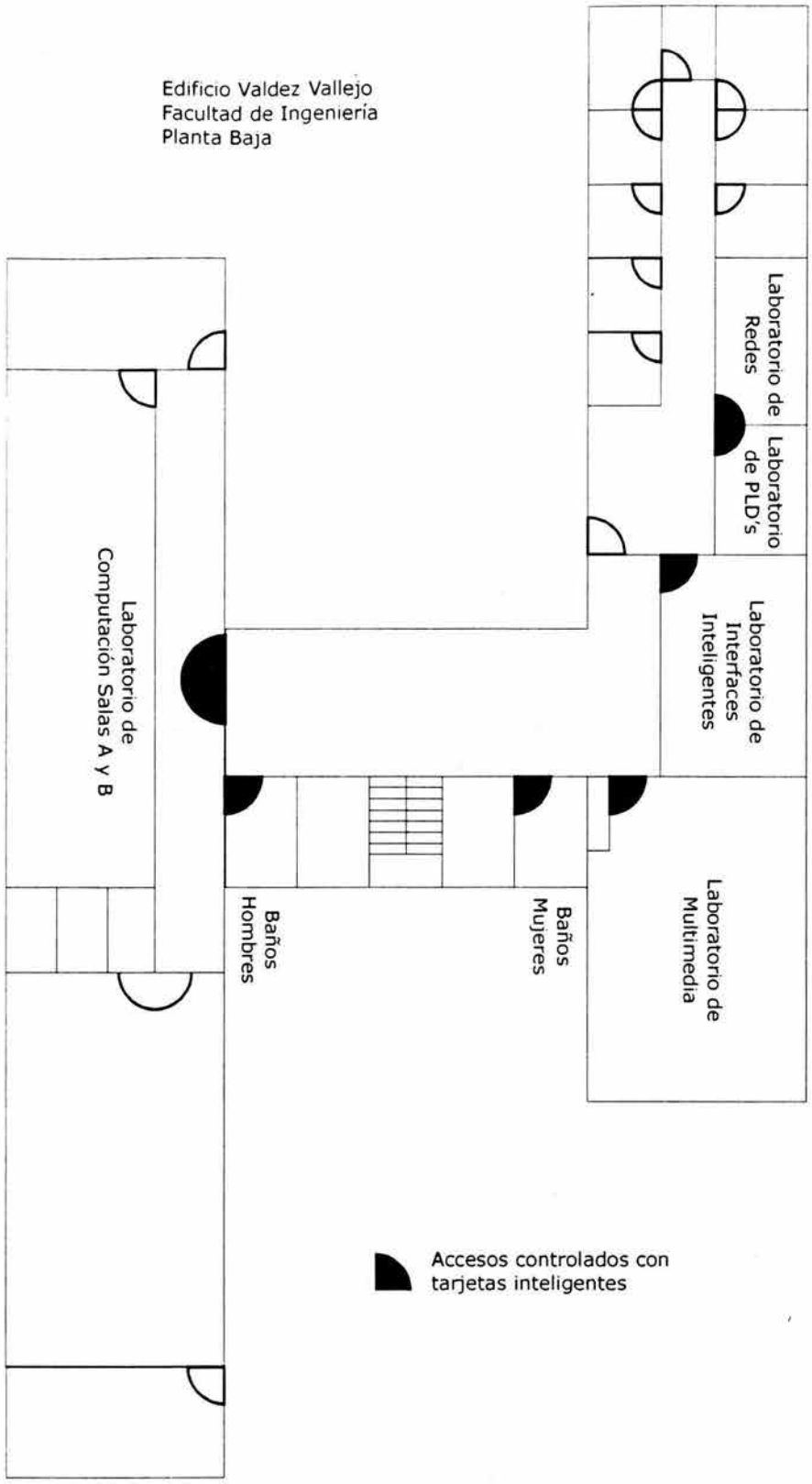


Figura 6.5 *Plano de la planta baja del edificio Valdez Vallejo*

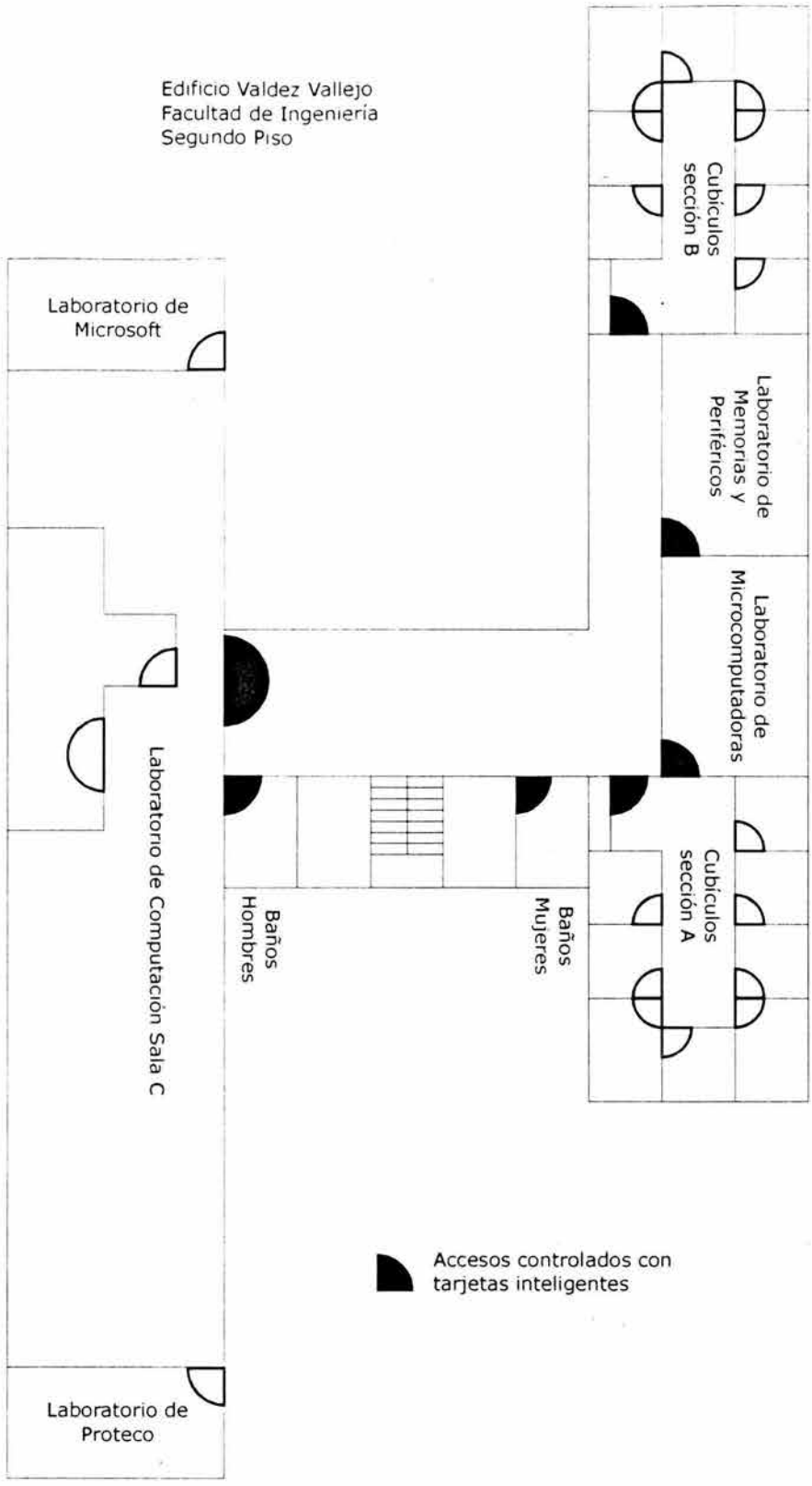


Figura 6.6 *Plano del segundo piso del edificio Valdez Vallejo*

El personal que labora en este departamento y que contará con una tarjeta para obtener acceso es el docente, secretarias, encargados de laboratorios, de intendencia y también será necesario que una persona funja como administrador del sistema.

Además de tener un control del acceso físico a las instalaciones, es necesario contar con un sistema de administración informático que permita el manejo tanto de los usuarios como de los accesos, que lleve un registro preciso del número de veces que una tarjeta ha sido presentada a un lector y de las ocasiones en que los usuarios han obtenido autorización de acceso.

6.2.2.1 Requerimientos del sistema de control de acceso (SCA)

El SCA deberá contar con una computadora central donde resida el Sistema de Administración, tendrá un lector/grabador de TI's para registrar los datos del usuario en su tarjeta. En un sistema de control de acceso físico se requiere de un panel de control, para esta aplicación se necesita uno para la planta baja y otro para el segundo piso. Su conexión con la computadora, los lectores, cerraduras y alarmas se realiza mediante una red de datos como se muestra en la Figura 6.7.

El SCA tendrá la facilidad de accionar la apertura de puertas en caso de una contingencia.

El panel de control almacena información actualizada procedente de la base de datos de la computadora central, lo que le permite determinar la validez del acceso, y sólo en aquellos casos en los que no cuente con información tendrá que realizar la consulta a la computadora central. El control de cerraduras y alarmas, así como la actualización de información en las tarjetas es parte de las funciones de este dispositivo.

Para tener acceso a un área controlada es necesario que el titular inserte su TI en el lector y digite su PIN. Una vez autenticada la tarjeta y el usuario, el SCA accionará la apertura de la cerradura correspondiente.

En el caso de los laboratorios, los cuales permanecen abiertos durante el día, el encargado insertará su TI en el lector para realizar la apertura. Al finalizar las labores deberá cerrar la puerta e insertar su tarjeta para registrar su salida.

En el acceso a los cubículos se instalará una extensión telefónica para facilitar la comunicación entre el personal administrativo/docente y los visitantes. El titular de la tarjeta permitirá el acceso a los visitantes insertando su TI en el lector, adicionando una clave especial que le indique al sistema que el acceso es de visitantes y no del titular.

Cuando se inserte en el lector una tarjeta no válida, se registre un PIN incorrecto o se trate de salir sin tener un registro de entrada o bien entrar teniendo registros pendientes se activará una alarma sonora y se desplegará un mensaje en la computadora central para conocimiento del administrador del sistema.

Los eventos de entrada, salida, intento fallido, etc., serán registrados en la bitácora del sistema.

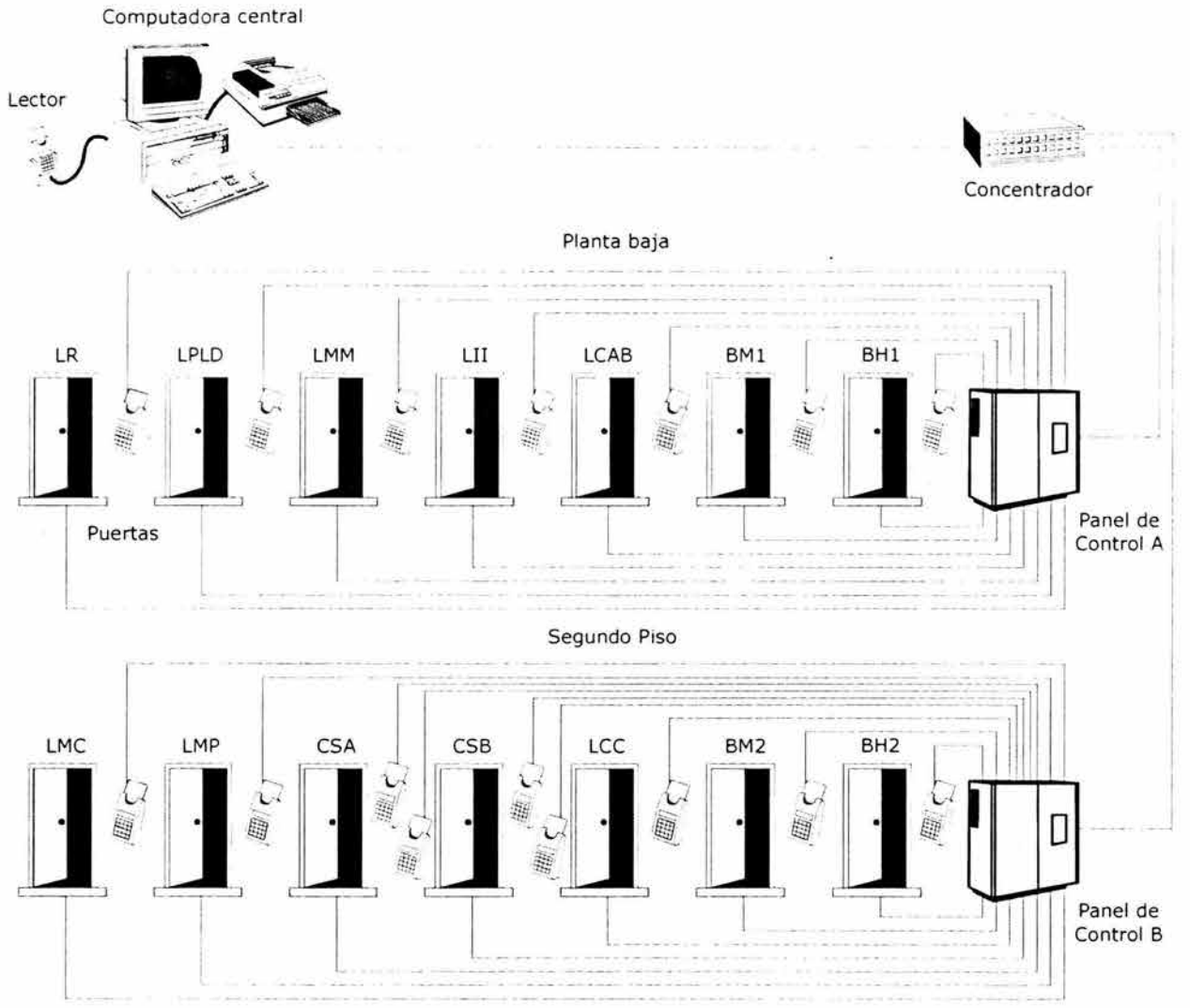


Figura 6.7 *Diagrama del Sistema de Control de Acceso*

6.2.3 Especificación de los niveles de seguridad

El sistema prevé el manejo de los siguientes tipos de usuario:

- Administrador de sistema. Es el encargado del manejo del sistema de control de acceso (SCA), entre las actividades que realiza está el mantenimiento a los registros de usuarios, el monitoreo de bitácoras de accesos y el mantenimiento a los catálogos del sistema.
- Personal docente. Es el personal académico que cuenta con un cubículo en el edificio mencionado.
- Personal administrativo. Son los encargados de laboratorios y secretarias del departamento.
- Personal de intendencia. Es el encargado del mantenimiento de las instalaciones.

- Personal temporal. Es el que por la naturaleza de sus actividades tendrá acceso a las instalaciones por un periodo de tiempo determinado, por ejemplo, tesistas, contratistas o instructores externos.

Los accesos a los que tiene autorización cada usuario se detallan en la Tabla 6.4.

Usuario	Baños	Laboratorios	Puertas de Acceso
Administrador	✓		✓
Secretaria	✓		✓
Personal docente sección A	✓	✓	✓
Personal docente sección B	✓	✓	✓
Intendencia	✓		
Encargado de laboratorio	✓	✓	
Temporal			✓

Tabla 6.4 *Accesos autorizados*

6.2.4 Selección del equipo requerido

Como se explica en el apartado 5.2, los componentes principales de un sistema de control de acceso físico son las tarjetas inteligentes, los lectores, las cerraduras, los paneles de control, el servidor de control de acceso, la impresora, el software de control de acceso y la base de datos, ver Figura 6.7.

La selección de la tecnología de tarjetas inteligentes para un sistema de acceso físico deberá ser determinada con base en las necesidades actuales y futuras. El equipo necesario para esta solución se muestra en la Tabla 6.5. Los pasos para la elección del equipo necesario para la implementación son:

Equipo	Cantidad
Servidor de control de acceso	1
Lector de tarjetas	17
Tarjetas	50
Concentrador	1
Extensiones telefónicas	2
Panel de control	2
Impresora	1

Tabla 6.5 *Equipo necesario*

6.2.4.1 Elección del panel de control

Éste debe ser elegido dependiendo del número de puertas que se necesitan controlar, depende también si se requiere un registro de quién ingresa por las puertas, si se quiere establecer un horario para que la puerta pueda ser abierta, del método de lectura y finalmente del número de usuarios que tendrá el sistema.

Para esta aplicación se requiere tener el control sobre 14 puertas, se necesita tener un registro de los accesos, se va a utilizar un lector de tarjetas con contactos con teclado

numérico para el ingreso de un PIN y el número de usuarios que utilizarán el sistema es de 50 aproximadamente.

6.2.4.2 Elección de la cerradura

Existen básicamente dos tipos de cerradura, de golpe o magnética. Una cerradura magnética es un electroimán grande que mantiene la puerta cerrada o permite su apertura, mediante una placa de metal colocada en la puerta. La fuerza de atracción varía de 300 a 1200 lb. Una fuerza de 300 a 600 lb es apropiada para puertas interiores, generalmente con marcos de madera. Para puertas exteriores de marcos metálicos, es conveniente utilizar unidades de 1200 lb.

Si se tiene una puerta exterior que utiliza cerraduras magnéticas es necesario considerar la dirección de apertura de la puerta, la mayoría de las puertas abren hacia adentro es decir hacia el interior del edificio.

En una puerta con contra mecánica se reemplaza la contra metálica en la parte interna de la puerta la cual la mantiene cerrada, en lugar de esto existe un mecanismo de liberación electromecánico el cual permite su apertura.

Para esta aplicación se recomiendan cerraduras de contra mecánica ya que poseen una fuerza de cierre de 1000 lb.

6.2.4.3 Elección del lector

Se debe seleccionar el lector de TI's apropiado para las características del panel de control. Normalmente los lectores, se adquieren junto con los paneles de control de un mismo fabricante.

6.2.4.4 Elección de las tarjetas

Se pueden elegir tarjetas con contactos o inalámbricas. Se recomiendan tarjetas inalámbricas cuando el tráfico en las puertas de acceso es elevado o bien cuando los lectores están expuestos a condiciones ambientales adversas como, por ejemplo, lluvia, nieve o hielo. Las tarjetas con contactos son utilizadas cuando el volumen de tránsito es bajo o cuando la velocidad de acceso a las áreas no es un aspecto prioritario.

En este caso, se recomiendan las tarjetas con contactos ya que la tecnología de este tipo está más avanzada que el caso de las inalámbricas, además de que el volumen de tránsito es bajo y existe la posibilidad de que se puedan integrar otras aplicaciones al uso de la tarjeta. Otra de las razones por la que se recomienda esta tarjeta es que su precio es menor al de las inalámbricas.

6.2.4.5 Cableado del sistema

Se debe prever el cableado necesario para el sistema así como sus especificaciones dependiendo del tipo de interfaz de cada componente. Generalmente se considera el:

- Cableado del lector al panel del control.
- Cableado del panel de control a la cerradura de la puerta
- Cableado del panel de control a la computadora central.

6.2.4.6 Equipo complementario

Por la naturaleza del sistema es necesario habilitarlo con equipo o funciones especiales como son:

- Batería de respaldo. Permite garantizar la continuidad de la operación en caso de interrupciones de energía eléctrica, sólo si las instalaciones no cuentan con este dispositivo.
- Apertura automática de accesos en caso de incendio o sismo.
- Alarma sonora. Indica cualquier condición inválida del sistema.

6.2.5 Descripción del sistema de administración (SA)

Este sistema deberá estar compuesto por los siguientes módulos, ver Figura 6.8:

- Administración de usuarios. En este módulo se darán de alta, baja y se modificará la información de los usuarios o su número de PIN. Servirá también para la administración de las tarjetas. Al tratarse de una sola aplicación, el ciclo de vida de la tarjeta estará relacionado directamente con los diferentes estados del usuario.

- Reportes y consultas. En este módulo se podrán obtener reportes de accesos por usuario, reportes de usuarios por acceso, indicando en ambos la hora y fecha de cada evento.

- Catálogos. En este módulo se podrán hacer modificaciones a las tablas de niveles de usuario y de administración de accesos, de días inhábiles de la base de datos y el inventario de tarjetas.

El SA contará con el registro del inventario de TI's adquiridas por el Departamento, ya sean asignadas o sin asignar. Cuando se registre un usuario en el sistema se le asignará la tarjeta correspondiente registrando en la Base de Datos (BD) el estatus de la tarjeta asignada así como la vigencia de la misma. Posteriormente se procederá a definir los accesos a los que tiene derecho el usuario en función a sus actividades.

El SA contempla el control de accesos con un solo lector para el registro de apertura y cierre de puertas como es el caso de los laboratorios los cuales permanecen abiertos durante su horario de servicio. De la misma forma considera el caso de accesos con lector de entrada y lector de salida como en los accesos a las áreas de cubículos.

El sistema no permitirá la reasignación de tarjetas, esto ofrecerá un mejor control de las mismas.

Toda la información que maneje este sistema deberá estar en una base de datos la cual también deberá tener sus políticas de mantenimiento como respaldos, defragmentaciones, etc.

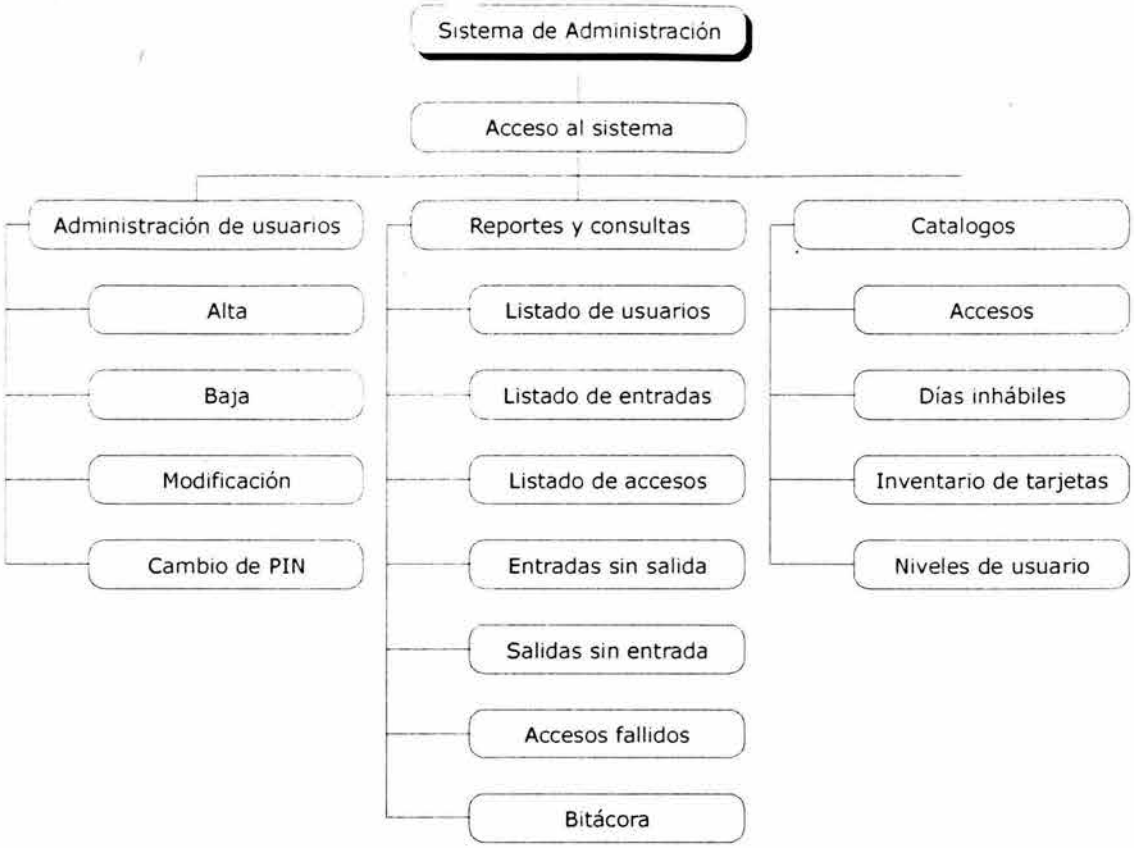


Figura 6.8 *Diagrama de bloques del Sistema de Administración*

6.3 PROPUESTA DEL TÓPICO PARA LA ASIGNATURA DE TEMAS ESPECIALES

Es importante proporcionar a los futuros egresados de la Facultad conocimientos actualizados que les permitan enfrentar los nuevos retos tecnológicos dentro de su ejercicio profesional.

En este sentido, el tema "Tecnología y Usos de la Tarjeta Inteligente" aporta las bases, estructura, funcionamiento, ventajas y servicios de una tecnología emergente con un amplio desarrollo.

La carrera de Ingeniería en Electrónica, que se imparte en la Facultad de Ingeniería de la UNAM, como parte de su plan de estudios incluye la materia optativa "Temas Especiales de Electrónica" cuya lista carece de un curso correspondiente a las tarjetas inteligentes.

Además, este tema puede ser incorporado en el plan de estudio de otras carreras que se imparten en la División, como Ingeniería en Computación e Ingeniería en Telecomunicaciones.

Lo expuesto en esta tesis sirve de base para establecer el tema como tópico de la asignatura "Temas Especiales". Entre los beneficios que el alumno puede obtener están los siguientes puntos:

- Conocer las herramientas teóricas y prácticas sobre las tarjetas inteligentes y enriquecer sus conocimientos profesionales.
- Estar a la vanguardia en cuanto a tecnologías avanzadas.
- Cubrir las expectativas del mercado laboral para participar en el desarrollo de proyectos basados en tarjetas inteligentes.
- Tener la oportunidad de ampliar su campo de acción tanto en México y en otros países.

Es importante destacar que diversas instituciones de nivel superior en otros países han incorporado en sus planes el estudio de esta tecnología. La Universidad China de Hong Kong (*The Chinese University of Hong Kong*), por medio del Centro de Servicios de Información Tecnológica (*Information Technology Services Center*) ofrece un curso acerca de este tema. Su contenido es el siguiente:

1. Tecnología de la tarjeta tradicional.
2. Introducción.
3. Lectores.
4. Aplicaciones.
5. Ciclo de vida.
6. Introducción a Culink.
7. Aplicaciones dentro de la Tarjeta.
8. Aplicaciones utilizando Culink en un Campus.
9. Aplicaciones de Tarjetas Inteligentes en el mundo.
10. Consideraciones de implementación.

Otro curso relacionado con el uso de TI´s se refiere a la "Seguridad en la Información", cuyo temario es el siguiente:

1. Seguridad básica.
2. La parte oculta.
3. Seguridad en redes.
4. Técnicas y herramientas de criptografía.
5. Soluciones.
6. Manejo de seguridad.

6.3.1 Estructura jerárquica del tema

Con base en el desarrollo de los aspectos investigados para la elaboración de este trabajo, se muestra la estructura de los temas sugeridos en el mapa conceptual de la Figura 6.9.

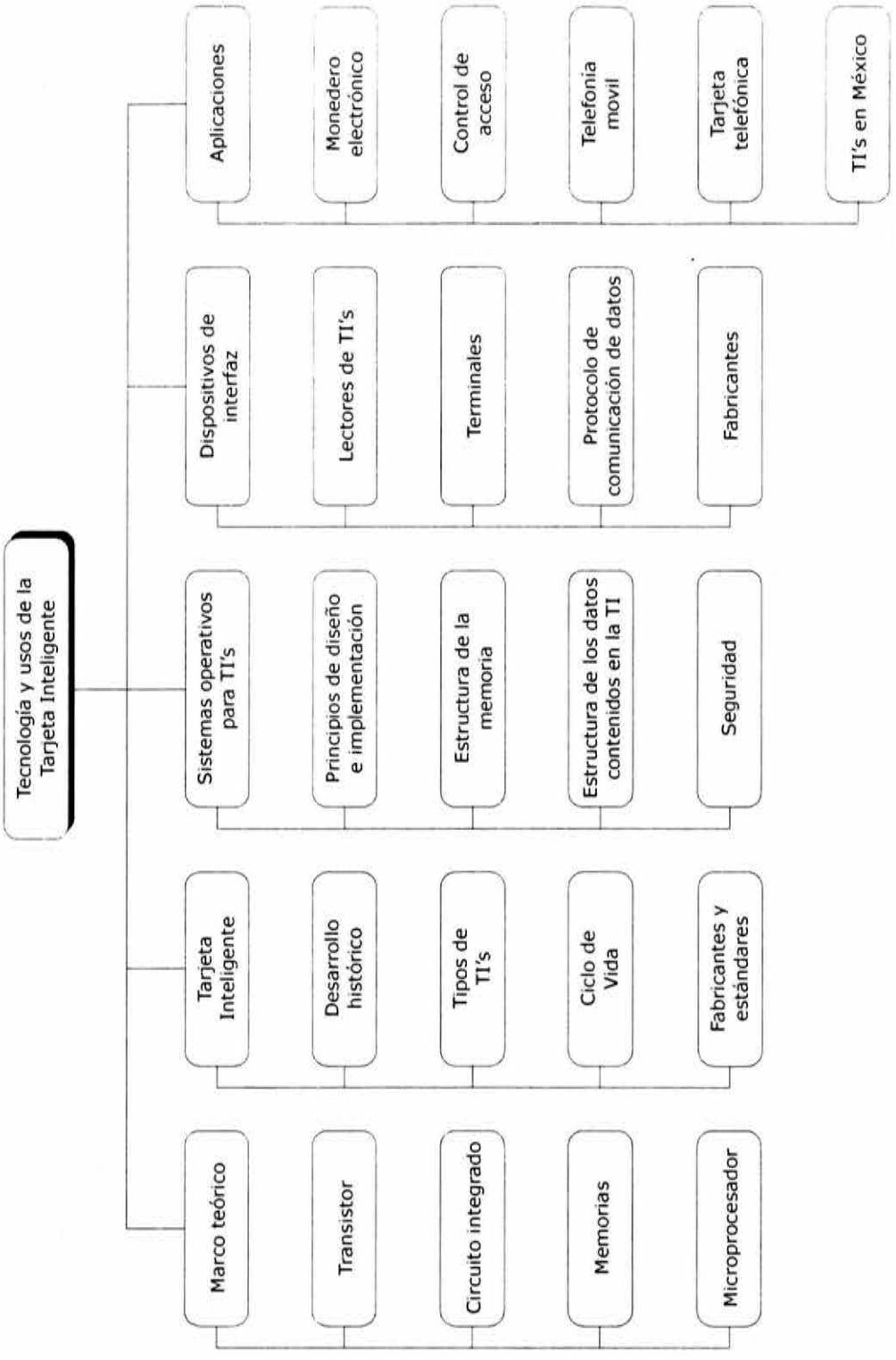


Figura 6.9 *Mapa conceptual del tema especial*

A continuación, se presenta la estructura conceptual de conocimientos que determinamos para la asignatura, así como el detalle específico de tiempos dedicados a cada tema.

6.3.2 Programa de la Asignatura

Tecnología y usos de la Tarjeta Inteligente

Número de créditos: 8
Carrera: ING. EN ELECTRÓNICA
Semestre: 10

Duración del curso:
Semanas: 16
Horas: 64

Horas a la semana:
Teoría: 4
Prácticas: 0

Asignatura opcional

Temario General
OBJETIVO
El alumno conocerá la tecnología y las aplicaciones de la tarjeta inteligente, utilizando las herramientas que se proporcionarán durante el curso.

Unidad	Contenido	Horas propuestas
1	Marco Teórico	8
2	Tarjeta Inteligente	14
3	Sistemas Operativos para Tarjetas Inteligentes	20
4	Dispositivos de Interfaz	8
5	Aplicaciones	14
	Total =	64

6.3.3 Objetivos y contenido de los temas

A continuación se muestra una tabla de análisis de tiempos para la asignatura Tecnología y usos de la Tarjeta Inteligente.

Unidad 1. Marco Teórico

OBJETIVO:

El alumno obtendrá los conocimientos fundamentales de los dispositivos electrónicos, su evolución, así como su aplicación en diferentes áreas de la tecnología.

	Contenido	Horas propuestas
1.1	Transistor	1
1.2	Circuito integrado	2
1.3	Memorias	2
1.4	Microprocesador	3
	Total =	8

Unidad 2. Tarjeta Inteligente

OBJETIVO:

El alumno conocerá la estructura y las ventajas de la tarjeta inteligente, así como comprenderá la importancia de su tecnología y evolución.

	Contenido	Horas propuestas
2.1	Desarrollo histórico	2
2.2	Tipos	2
2.3	Ciclo de vida	4
2.4	Fabricantes y Estándares	2
	Total =	14

Unidad 3. Sistemas Operativos para Tarjeta Inteligentes

OBJETIVO:

El alumno identificará las características de los sistemas operativos, su principio y estructura.

	Contenido	Horas propuestas
3.1	Principios de diseño e implementación	6
3.2	Estructura de la memoria	4
3.3	Estructura de los datos	4
3.4	Seguridad	4
	Total =	20

Unidad 4. Dispositivos de Interfaz

OBJETIVO:

El alumno conocerá los diferentes dispositivos de interfaz que existen para las tarjetas inteligentes.

	Contenido	Horas propuestas
4.1	Lectores	2
4.2	Terminales	2
4.3	Protocolo de comunicación de datos	3
4.4	Fabricantes	1
	Total =	8

Unidad 5. Aplicaciones

OBJETIVO:

El alumno identificará las necesidades de empresas que deseen utilizar la Tarjeta Inteligente y contribuirá con una adecuada implantación conociendo las aplicaciones que se explican en este capítulo.

	Contenido	Horas propuestas
5.1	Monedero Electrónico	2
5.2	Control de acceso	4
5.3	Telefonía móvil	4
5.4	Tarjeta telefónica	2
5.5	Tarjeta Inteligente en México	2
	Total =	14

Como parte de los resultados obtenidos en el desarrollo de esta tesis, estamos convencidos de que la incorporación de un Tema Especial cuyo nombre sería Tecnología y usos de la Tarjeta Inteligente en la carrera de Ingeniería en Electrónica, es sólo uno de tantos pasos que pueden y deben darse con la intención de crear y promover una cultura de aprendizaje mas amplio en la Facultad de Ingeniería.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

Programa de Asignatura

INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y EN COMPUTACIÓN — División

COMUNICACIONES Y ELECTRÓNICA — Departamento

Fecha de aprobación del

Programa de la Asignatura:	TECNOLOGIA Y USOS DE LA TARJETA INTELIGENTE			
Clave:		Número de Créditos:	08	Carrera: ING. ELECTRICO ELECTRÓNICO ING. EN COMPUTACIÓN ING. EN TELECOMUNICACIONES
Duración del Curso:	Semanas:	16		
	Horas:	64.0	Semestre:	10° 10° 10°
Horas a la semana:	Teoría:	4.0	Obligatoria:	
	Prácticas:	0.0	Optativa:	X

OBJETIVO DEL CURSO

El alumno conocerá la tecnología y las aplicaciones de la tarjeta inteligente, utilizando las herramientas que se proporcionarán durante el curso.

TEMAS

Núm.	Nombre	Horas
I.	MARCO TEÓRICO.	8.0
II.	TARJETA INTELIGENTE	14.0
III.	SISITEMAS OPERATIVOS PARA TARJETAS INTELIGENTES	20.0
IV.	DISPOSITIVOS DE INTERFASE	8.0
V.	APLICACIONES	14.0
		64.0

ASIGNATURA: TECNOLOGIA Y USOS DE LA TARJETA INTELIGENTE

ANTECEDENTES, OBJETIVOS Y CONTENIDO DE LOS TEMAS

I. MARCO TEÓRICO

OBJETIVO:
El alumno obtendrá los conocimientos fundamentales de los dispositivos electrónicos, su evolución, así como su aplicación en diferentes áreas de la tecnología.

CONTENIDO:

1.1 EL TRANSISTOR
1.2 EL CIRCUITO INTEGRADO
1.3 MEMORIAS
1.4 MICROPROCESADOR

II. TARJETA INTELIGENTE

OBJETIVO:
El alumno conocerá la estructura y las ventajas de la tarjeta inteligente, así como comprenderá la importancia de su tecnología y evolución.

CONTENIDO:

2.1 DESARROLLO HISTORICO
2.2 TIPOS DE TARJETAS INTELIGENTES
2.3 CICLO DE VIDA
2.4 FABRICANTES Y ESTANDARES

III. SISTEMAS OPERATIVOS PARA TARJETAS INTELIGENTES

OBJETIVO:
El alumno identificará las características de los sistemas operativos, su principio y estructura.

CONTENIDO:

3.1 PRINCIPIOS DE DISEÑO E IMPLEMENTACION
3.2 ESTRUCTURA DE LA MEMORIA
3.3 ESTRUCTURA DE LOS DATOS
3.4 SEGURIDAD

IV. DISPOSITIVOS DE INTERFAZ

OBJETIVO:
El alumno conocerá los diferentes dispositivos de interfaz que existen para las tarjetas inteligentes.

CONTENIDO:

4.1 LECTORES
4.2 TERMINALES
4.3 PROTOCOLO DE COMUNICACION
4.4 FABRICANTES

ASIGNATURA: TECNOLOGIA Y USOS DE LA TARJETA INTELIGENTE

ANTECEDENTES, OBJETIVOS Y CONTENIDO DE LOS TEMAS

V. APLICACIONES

OBJETIVO:
El alumno identificará las aplicaciones en las que se utilizan las tarjetas inteligentes.

CONTENIDO:

5.1 MONEDERO ELECTRÓNICO
5.2 CONTROL DE ACCESO
5.3 TELEFONÍA MÓVIL
5.4 TARJETA TELEFÓNICA
5.5 TARJETA INTELIGENTE EN MEXICO

TECNICAS DE ENSEÑANZA:

Exposición oral _____ (X)
Exposición audiovisual _____ (X)
Ejercicios dentro de clase _____ ( )
Ejercicios fuera del aula _____ ( )
Seminarios _____ ( )
Lecturas obligatorias _____ (X)
Trabajos de investigación _____ (X)
Prácticas de taller o laboratorio _____ ( )
Prácticas de campo _____ ( )
Otras: _____

ELEMENTOS DE EVALUACIÓN:

Exámenes parciales _____ (X)
Exámenes finales _____ (X)
Trabajos y tareas fuera del aula _____ (X)
Participación en clase _____ (X)
Asistencia a prácticas _____ ( )
Otras: ASISTENCIA

ANTECEDENTES

Asignatura	Clave
DISPOSITIVOS Y CIRCUITOS ELECTRÓNICOS	1618
ELECTRÓNICA DIGITAL	0583
MICROPROCESADORES Y MICROCONTROLADORES	1937
SISTEMAS OPERATIVOS	0640

ASIGNATURA: TECNOLOGIA Y USOS DE LA TARJETA INTELIGENTE

CONSECUENTES

Asignatura	Clave
Ninguna	

BIBLIOGRAFIA

TEXTO

BÁSICOS:

1.- ACOSTA, Calderon, Castro y Villavicencio
"Tarjetas inteligentes, su tecnologia y la propuesta de su aplicacion para controlar la seguridad en el Departamento de Ingenieria en Computacion"
FI, UNAM, 2003.

CONSULTA:

1.- DREIFUS, Henry
"Smartt cards. A guide to building and managing smart card applications"
John Wiley & Sons, 1999.

2.- HANSMANN, Mickloss, Schäck and Seliger
"Smart card application development using java"
Springer, 1999

3- SANDOVAL, Brito y Mayor
"Tarjetas inteligentes"
Paraninfo, 1999

Conclusiones

CONCLUSIONES

Desde su invención, la TI ha tenido un constante desarrollo y una amplia aceptación a nivel mundial sobre todo en Europa y Asia.

Haciendo uso de las TI's es posible diseñar una solución enfocada a tener en una sola tarjeta las funciones de identificación escolar y/o laboral, credencial de elector, licencia de manejo, tarjeta bancaria, telefónica, credencial del seguro social y/o de seguro de gastos médicos, de descuento, credenciales de clubes deportivos y/o asociaciones, acceso a redes, a servicios, transporte etc. Sin embargo, esto requiere de una gran infraestructura informática que permita compartir información e interactuar entre los diferentes organismos e instituciones involucradas.

Las instituciones financieras pueden mejorar la seguridad en las transacciones bancarias mediante el uso de las TI´s, ya que cuentan con mecanismos de seguridad que a diferencia de las tarjetas de banda magnética son difíciles de alterar o reproducir.

Es factible simplificar las tareas administrativas de una institución educativa, como la Universidad Nacional Autónoma de México, derivadas del control escolar y académico, así como la prestación de servicios mediante la implementación de tarjetas multifuncionales que cuenten con aplicaciones de control de acceso, pago de servicios, trámites escolares, etc.

La implementación de tarjetas inteligentes en el Departamento de Computación de la Facultad de Ingeniería podría ser una solución para controlar en forma automatizada el acceso a sus instalaciones, además podría extenderse a otras áreas vitales tanto de la Facultad como de la misma Universidad. Permitiría el acceso a las áreas en función de los permisos otorgados al usuario así como el registro detallado de las entradas y/o salidas. Posibilitaría la interconexión con alarmas que se activen cuando se trate de violar el sistema y facilitaría la revocación de los permisos para un usuario, sin la necesidad de tener a la mano su TI mediante el sistema de administración.

Es necesaria la formación de profesionales que cuenten con los conocimientos de las tecnologías emergentes, por esta razón se recomienda incorporar un tópico llamado "Tecnología y Usos de la Tarjeta Inteligente" para la asignatura "Temas Especiales".

La aplicación y definición de estándares es importante en el desarrollo de cualquier solución y/o dispositivo ya que permite su integración con otros diseños, tanto locales como mundiales.

La tecnología de tarjetas inteligentes forma parte de la era de la computación de bolsillo, la cual tiene una inmensa gama de posibilidades para su aplicación, además de las ya conocidas como son: la tarjeta de crédito, la tarjeta telefónica, el monedero electrónico, de identificación y acceso, de lealtad, etc. Sin embargo, esto marca el inicio del desarrollo que se verá en los próximos años cuando se explote el potencial que ofrece esta tecnología.

Bibliografía

BIBLIOGRAFÍA

Boylestad, Robert L. & Nashelsky, Louis
Electronica, Teoría de Circuitos y Dispositivos Electrónicos.
Pearson – Prentice Hall
México, 2003

Dreifus, Henry.
Smart Cards. A guide to building and managing smart card applications.
John Wiley & Sons.
New York, 1999.

Hansmann, Uwe. Nicklous, Martin S. Schäck, Thomas. Seliger, Frank.
Smart Card Application Development Using Java.
Springer.

Hendry, Mike.
Smart Card Security and Applications.
Artech House Publishers.
Boston, 1997.

Miranda Tello, José Raúl.
Diseño y construcción de un lector de tarjetas inteligentes.
Instituto Politécnico Nacional.
México D.F., 2000.

Rankl, W. & Effing W.
Smart Card Handbook.
John Wiley & Sons.
New York, 1999.

Sandoval, Juan Domingo. Brito, Ricardo. Mayor, Juan Carlos.
Tarjetas Inteligentes.
Paraninfo.
España, 1999.

Sayers, Ian L.
Principios de Microprocesadores.
CECSA.
México, 1998.

Woolard, Barry.
Circuitos Integrados Digitales y Computadoras.
Parainfo.
Madrid, 1985.

Zoreda, J. L., & Otón, J.M.
Smart Cards.
Artech House Publishers.
Boston, 1994

http://www.acerta.net
httP://www.acg.de
http://www.acs.com.hk
http://www.advancedcardsystems.com
http://www.afina.com.mx
http://www.allengheny.com
http://www.allsafe.com
http://www.ammismartcards.com
http://www.ascom.com
http://www.azc.uam.mx/publicaciones/gestion/num11y12/doc19.html
http://www.barmax.com
http://www.cherrycorp.com
http://cism.bus.utexas.edu/works/articles/smartcardswp.html
http://www.connect-world.com
http://www.cp8bull.net
http://www.cryptography.com
http://www.cyberflex.austin.et.slb.com
http://www.datakey.com
http://www.datateccards.com
http://www.deister.com
http://www.delarue.com
http://www.developer.intel.com
http://www.digicash.com
http://dmsweb.badm.sc.edu/798mis/Cases/Mondex/HTML/Mondex%20Case.htm
http://www.euro.dell.com/countries/eu/enu/gen/topics/vectors 2001-smartcard.html
http://www.fisc.com
http://www.fnmt.es
http://www.gdm.de
http://www.gemplus.com
http://www.giesecke&devrient.com
http://www.gis.com
http://www.gmt.com.mx
http://www.gpt.co.uk
http://www.hp.com
http://www.identicod.com.mx
http://www.incard.com
http://www.ingenico.com
htpp://www.intel.com
http://www.intellect.com.au
http://www.javasoft.com
http://www.kirkplastic.com
http://www.laminex.com
http://www.litronic.com
http://www.microsoft.com
http://www.mondexusa.com
http://www.nbstech.com
http://www.obethur.com
http://www.omnikeyag.com
http://www.orga.com
http://www.protekila.com.tr
http://www.prosoft2k.com

http://www.qsl.net/lw3eux/notas/transist.htm
http://www.qualtecmx.com.mx
http://www.rainbowtechnologies.com
http://www.santander.com.mx
http://www.schlumberger.com
http://www.scmmicro.com
http://www.siemens.com
http://www.signuscard.com
http://www.simalliance.org
http://www.simpletechnology.com
http://www.slb.com/et
http://www.smartcard.com.au
http://www.smartcardbasics.com/reader.html
http://www.smartcardsys.com
http://www.spartanics.com
http://www.spyrus.com
http://www.ssiphoto.com
http://www.sspsolutions.com
http://www.supertecsystems.com
http://www.terra.es/personal/lermon/cat/articles/evin0302.htm
http://www.tiresias.org
http://www.toshiba.co.jp
http://www.ultimaco.com
http://www.umich.edu/~newsinfo/Releases/1999/Feb99/r020999c.html
http://www.verifone.com
http://www.versacard.com
http://www.viage.com
http://www.visa.com
http://webopedia.internet.com/Hardware/Ics/Chip.html
http://www.winforms.phil.tu-bs.de/winforms/company/solaic/gsm/gsm.html
http://www.worldtronix.ca