UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

“Utilización de Tarjeta Inteligente en la Facultad de Ingeniería AZUL y ORO”

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

YADIRA CEPEDA DE LA CRUZ

JAZIEL SANTILLÁN ARZATE

DIRECTOR: M.I. Adolfo Millán Nájera

MÉXICO, D.F. a de Octubre del 2006

Agradecimientos

A mi Madre,

Por tu amor incondicional y tu lucha incansable con la vida. Gracias por ser mi amiga y por vivir conmigo mis tristezas y alegrías, mis desamores y locuras, quien si no tú para comprenderme, mujer triunfante a pesar de los destrozos en tu vida, te amo mamá.

A ti, Papá (q.e.d),

Por tu ausencia. Me hiciste una mujer dependiente de cariño pero una mujer que lucha día a día por ser un poco más feliz…espero algún día poderte abrazar muy fuerte, y platicar... cuanta falta me haces, te quiero mucho.

A mis hermanos,

***Normis, Ale, Pato, Mina, Coca, Enano**, ustedes saben que sobra decir gracias por su apoyo, porque ha sido incondicional. Sólo nosotros sabemos todo lo que hemos pasado y lo mucho que nos hemos dolido, sé que han sido testigos de amargas tristezas, de recuerdos no muy gratos, pero son mis hermanos, fuertes, grandes, únicos, que luchan también a diario por un momento más de felicidad.*

A mis sobrinos,

Porque serán siempre una alegría en mi vida, son pedacitos de carne formados con esperanza pura de tener una nueva familia.

A mis tíos y primos,

Por el apoyo y bondad que sólo ustedes saben brindar, capaces de sacrificar si es necesario su propia felicidad porque no conocen el egoísmo, gracias por el amor tan grande que nos dado.

A Riga y Armando,

Por ser mis ángeles. Nunca sabré cuando es que fué que los llegue a querer tanto, no tengo manera de agradecerles su infinito apoyo. En verdad gracias por quererme como lo hacen, por estar conmigo, no me imagino mi vida sin ustedes y saben? Estoy aquí!

A mis amigos,

Qué digo mis amigos, mis hermanos!...

Por esa familia hermosa que se ha ido formando con cada experiencia vivida, que se ha alimentado con recuerdos únicos, experiencias algunas tristes pero otras muy felices, créanme, tengo una sola convicción: envejecer con ustedes. Gracias por dejarme ser parte de su vida, ustedes son desde hace mucho, parte de la mía, gracias por apoyarme en los momentos tan difíciles que he padecido y por brindarme siempre su apoyo y amor incondicional, los quiero!

Ivette Loyo Pastrana, Coma
Erika M. Castillo, Werita
Yhalí Ruiz, Yhalita
Jaziel Santillán, Jaz
Darío O. Torres, Daris
Mauricio Ramos, Mau Mau
Jorge A. Monroy, Cory
Cuauhtemoc A. Guzmán, Temo
Alberto Cortéz, Wero
Eduardo Nuñez, Lalo
Ismael Huerta Huerta, Huehue
León Felipe Arteaga, Leoncito
Gilberto Basilio, Gil
Noel Aróstegui, Noelcito
Edgar I. Alpizar, Edi

Y muy especialmente a ti,

Amor de mi vida... por hacerme inmensamente feliz con el amor que me das, gracias por querer caminar y construir a mi lado, por planear tu vida junto a la mía. Te amo, y quiero que sepas que mucho de tus alientos están aquí reflejados, que todo en la vida es un medio para llegar a donde realmente debemos estar, gracias amor por ser tú, Luis Santillán...

Por todo lo que aún nos falta por caminar...

Yadira Cepeda De La Cruz.

A mis padres:

Gracias por su apoyo incondicional durante este largo camino, porque en los momentos mas difíciles supieron darme las palabras y los ánimos para seguir adelante, porque cada triunfo lo compartimos juntos y de cada error aprendimos la lección para no lo volverlo a cometer. No existen palabras para reflejar la felicidad y el orgullo que siento por ustedes.
Es por eso que solo me resta decir:

Gracias Patuchis y TETE

A mi hermano:

Gracias por abrir camino al andar. Por los incontables momentos que compartimos y todas los veces que me apoyaste. Por soportar desvelos y enojos y aun así extenderme tu mano cuando lo necesite. Por escucharme en momentos de incertidumbre y darme tu punto de vista sincero. Por esto y por todo lo que nos falta recorrer:

Gracias Marica.

A mis tíos y primos

Porque siempre estuvieron pendientes de mí, por ser un motivo más para no darme por vencido. Por su apoyo y su comprensión:

Gracias Familia.

Jaziel Santillán Arzate.

A nuestro director,

M.I. Adolfo Millán Nájera.
Ingeniero gracias por aceptar ser nuestro asesor en esta tesis, por ayudarnos a cumplir este sueño, más aún, gracias por la paciencia y dedicación que mostró hacia nosotros, tuvimos la oportunidad de conocer a una persona que además de tener el don de la enseñanza, es dedicada y fiel a su carrera.

A nuestros maestros,

A nuestros profesores de la Facultad de Ingeniería les agradecemos sus enseñanzas, su dedicación. Cada uno de ustedes dejó en nosotros una imagen única, una anécdota incomparable. Gracias por contribuir a nuestra formación, no sólo profesional, además personal.

A nuestra Alma Mater,

Por albergarnos en su cuna, de donde han salido profesionistas ansiosos, que al igual que nosotros soñaron algún día gritar llenos de euforia un Goya!, después del juramento a nuestra máxima casa de estudios. Eternamente orgullosos de ser universitarios y de que corra por nuestra sangre ese color azul y oro, Gracias UNAM....!

Yadira Cepeda
Jaziel Santillán

PRÓLOGO

Actualmente se observa un importante crecimiento en aplicaciones de Tarjetas Inteligentes, esta tecnología esta difundiéndose en nuestras actividades debido a sus múltiples beneficios, esto nos ha motivado para implementar una solución que integran las Tarjetas Inteligentes, pues encontramos que, utilizar esta tecnología optimiza recursos económicos, administrativos, humanos en los diferentes servicios que presta la Facultad de Ingeniería.

Es por ello que la Universidad como fuente generadora de conocimiento y en particular la Facultad de Ingeniería como una de sus extensiones tecnológicas, debe incorporarse a las nuevas normas mundiales de seguridad electrónica.

El objetivo de este trabajo es ingresar a la Facultad de Ingeniería el concepto de Tarjeta Inteligente con dos aplicaciones base, una como medio de pago y la otra como identificación, esto nos permitiría tener un control más seguro en información sobre el alumnado e introduciría a la universidad al mundo de las transacciones electrónicas en la modalidad de prepago y en consecuencia a las ventajas que éstas conllevan. Esta implementación se basará en el sistema de administración que hemos denominado AZUL y ORO.

Nuestra tesis consistirá en el análisis, diseño y desarrollo de este sistema, el cual nos permitirá comunicarnos con la tarjeta, y llevar a cabo las transacciones que el usuario desee realizar.

En las terminales se contará con la interfaz que interactue, por un lado con el servidor y la base de datos, y por otro con el lector de tarjetas y el usuario.

El diseño de la base de datos y las tablas correspondientes serán prototipos, pero totalmente funcionales, y al igual que las interfaces serán elaboradas como parte de este trabajo. Es importante hacer notar que las aplicaciones implementadas ejemplifican realmente la manera en la que trabajan las soluciones de Tarjetas Inteligentes. Pues la intención es mostrar los alcances que éstas pueden tener, el fin es hacer una extracción muy precisa de su utilización: se desarrollará un sistema que actualice las identificaciones de los alumnos pero que además nos sirva como medio de pago dentro de la facultad.

Para llevar a cabo un proyecto de este tipo es necesario considerar puntos como son: comprobantes, permisos, cuestiones administrativas, infraestructura y en general situaciones ajenas al desarrollo del sistema y que por ende estarían fuera del alcance de este documento.

En el Capítulo 1, se proporciona una introducción al funcionamiento de las Tarjetas Inteligentes. En él, se hablará sobre la fabricación y los entes relacionados en una aplicación de Tarjeta Inteligente y los distintos elementos que interactúan con ella.

En el Capítulo 2, se encontrará la definición de lo que es una Tarjeta Inteligente, la clasificación que se tiene de ellas y del estándar que las rige, dando una explicación global de éste.

En el Capítulo 3, se dan a conocer los diferentes ámbitos en los cuales la Tarjeta Inteligente puede aplicarse, así como la seguridad que ésta misma ofrece.

En el Capítulo 4, se encuentra el desarrollo del sistema Azul y Oro, sistema que nos permitirá entender el funcionamiento de la Tarjeta Inteligente aplicada como identificación y medio de pago.

En el Capítulo 5, se dan a conocer las conclusiones y las aplicaciones propuestas a futuro, que se pudieron visualizar después de haber realizado este trabajo.

Esta tesis pretende ser pionera en la creación de nuevos procesos automatizados a través de la Tarjeta Inteligente en la Facultad de Ingeniería, dejando abierta toda la gama de posibilidades que se tendría si se decidiera usarla de manera cotidiana en todos los servicios que la Facultad ofrece y que por ende se hacen necesarios para llevar a cabo la operación de la misma. Podemos mencionar algunos procesos como el de inscripción, asistencia, pago de servicios, etcétera.

ÍNDICE

Pág.

Capítulo I. INTRODUCCIÓN

Debido al desarrollo de la Informática y los medios de almacenamiento digitales nos es posible automatizar procesos y obtener información de control al momento de llevarse acabo éstos.

En nuestra Universidad se pueden detectar nichos de información para los cuales es necesario llevar a cabo un proceso de registro de la información generada, así como de su transacción, de manera eficiente y segura cotidianamente.
Estas características son uno de los principales ámbitos de acción de las Tarjetas Inteligentes (TI).

Un sistema en el cual se utiliza una Tarjeta Inteligente debe de contener varios elementos (generalmente aplicaciones cliente-servidor), *ver figura 1.1*, los cuales se enuncian a continuación y serán tratados durante el desarrollo de este trabajo.

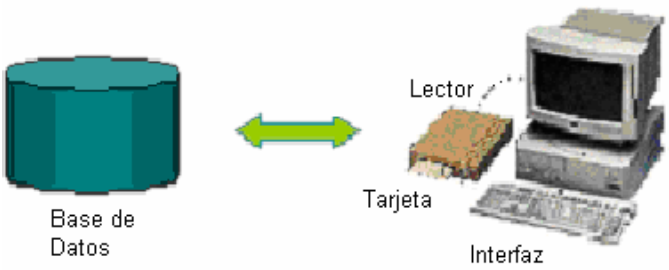


Figura 1.1 Elementos en las aplicaciones con TI

Lectores. Se incorporan a la computadora personal (PC) mediante algún puerto o bien puede estar acoplado de manera física en una terminal. El lector es el que hace la interacción directa con la tarjeta

Terminales. Se pueden entender como la interfaz con el usuario. Pueden ser una PC o bien un dispositivo especialmente diseñado para este fin.

Tarjetas Inteligentes. Dispositivos de almacenamiento en donde radica la información de la aplicación.

Medios Físicos de Comunicación. Es el canal por el cual se transmite la información de la tarjeta hacia el sistema central

Servidores. Dispositivos en donde se establece todo el ambiente de parámetros e información general de los cardholders (usuarios de la tarjeta), así como de las propias aplicaciones.

El requerimiento principal en este tipo de sistemas es tener seguridad en cada uno de los eslabones que conforman la cadena de información. Esto se logra mediante el uso de la criptografía en conjunción con una seguridad de accesos y controles perfectamente establecidos para la determinación de agentes de seguridad (son las personas responsables de la definición de los métodos por los cuales se llevan acabo la definición de llaves).

Por ejemplo para hacer la transmisión de datos se puede hacer uso de mensajes cifrados con algún algoritmo o bien mediante la utilización de dispositivos de seguridad. Y siempre se deben observar tres puntos muy importantes:

AUTENTICACIÓN: La entidad que envió los datos es quien dice ser.

INTEGRIDAD: Asegurarse que la información no fue alterada (intencionalmente o sin intención) entre el emisor y el receptor o entre el momento que fue generado y el momento recibido.

CONFIDENCIALIDAD: Asegurarse que no cualquier entidad puede tener acceso a esa información que fue generada intencionalmente para una sola entidad.

De acuerdo al esquema de encripción que se desee aplicar es como se van obteniendo los puntos anteriormente citados. El sistema que origina la comunicación aplica un proceso de encripción de los datos a ser enviados viajando de manera segura a través del canal de comunicación y cuando el destino recibe esta información aplica el método inverso mediante el cual se obtendrán nuevamente los datos originales. En conjunción con esto es posible agregar procesos de certificados y firmas digitales.

Además de proteger la información al momento de generarla es necesario mantenerla de manera segura, esto se logra mediante lugares físicos de acceso restringido y acceso protegido a los datos en los dispositivos de almacenamiento como en la mayoría de los casos se hace.

¿Pero qué hay de las tarjetas y la seguridad que pueden ofrecer al almacenar los datos?

Las Tarjetas Inteligentes mantienen sus datos de manera segura mediante el uso de algoritmos criptográficos, reglas de seguridad en los accesos a los archivos y protecciones físicas para evitar una intrusión mediante algún agente externo, así como también utilizan claves de acceso para ser utilizadas por el usuario final.

Antes de detallar este tema del manejo de la seguridad interna, es necesario hablar un poco del ciclo de vida de las tarjetas para comprender la manera en que son elaboradas y los entes que actúan en este proceso, ver la *figura 1.2*

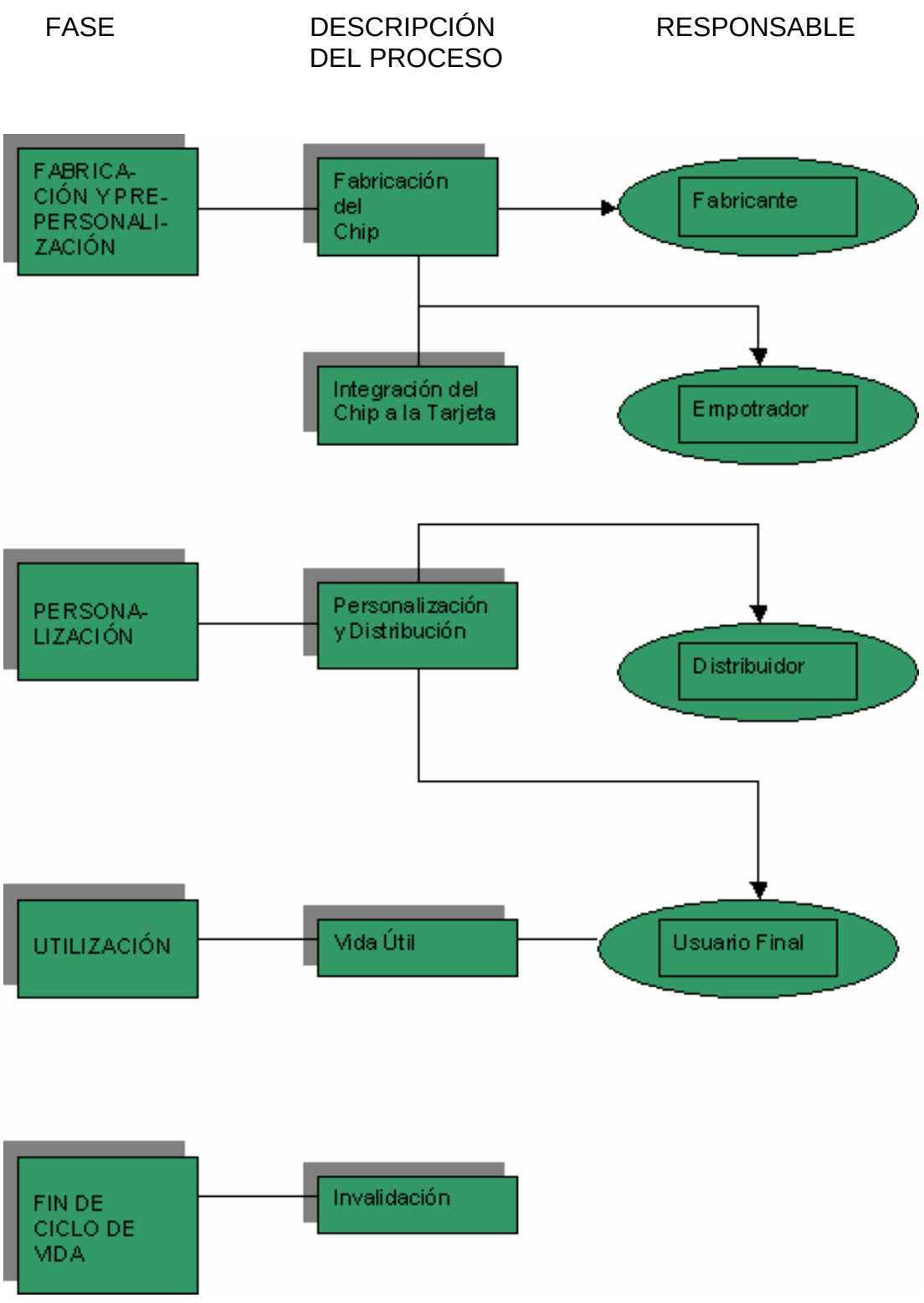


Figura 1.2 Ciclo de vida de las TI

FABRICANTE: Es la empresa que realiza físicamente el chip, es decir que lo implementa (realiza la máscara) y carga el sistema operativo. Generalmente este mismo ente es el encargado de acoplar el chip con el PVC (plástico donde va empotrado el CHIP), para conformar lo que es físicamente la tarjeta.

PERSONALIZADOR: Es el ente encargado de grabar en el chip la estructura de los archivos, llaves, y en general todos los datos de la tarjeta para conformar toda la aplicación.

EMISOR: Es el ente propietario de la aplicación y la tarjeta. Generalmente son las instituciones financieras si habláramos de aplicaciones de débito y crédito.

CARDHOLDER: Es el usuario final de la tarjeta.

Al observar la *figura 1.3*, se aprecia la interacción que existe entre estos entes, y el lector puede intuir que el intercambio en la información es necesario, por lo que tenemos que explicar cómo se mantiene la seguridad en la información a través de esta mencionada interacción.

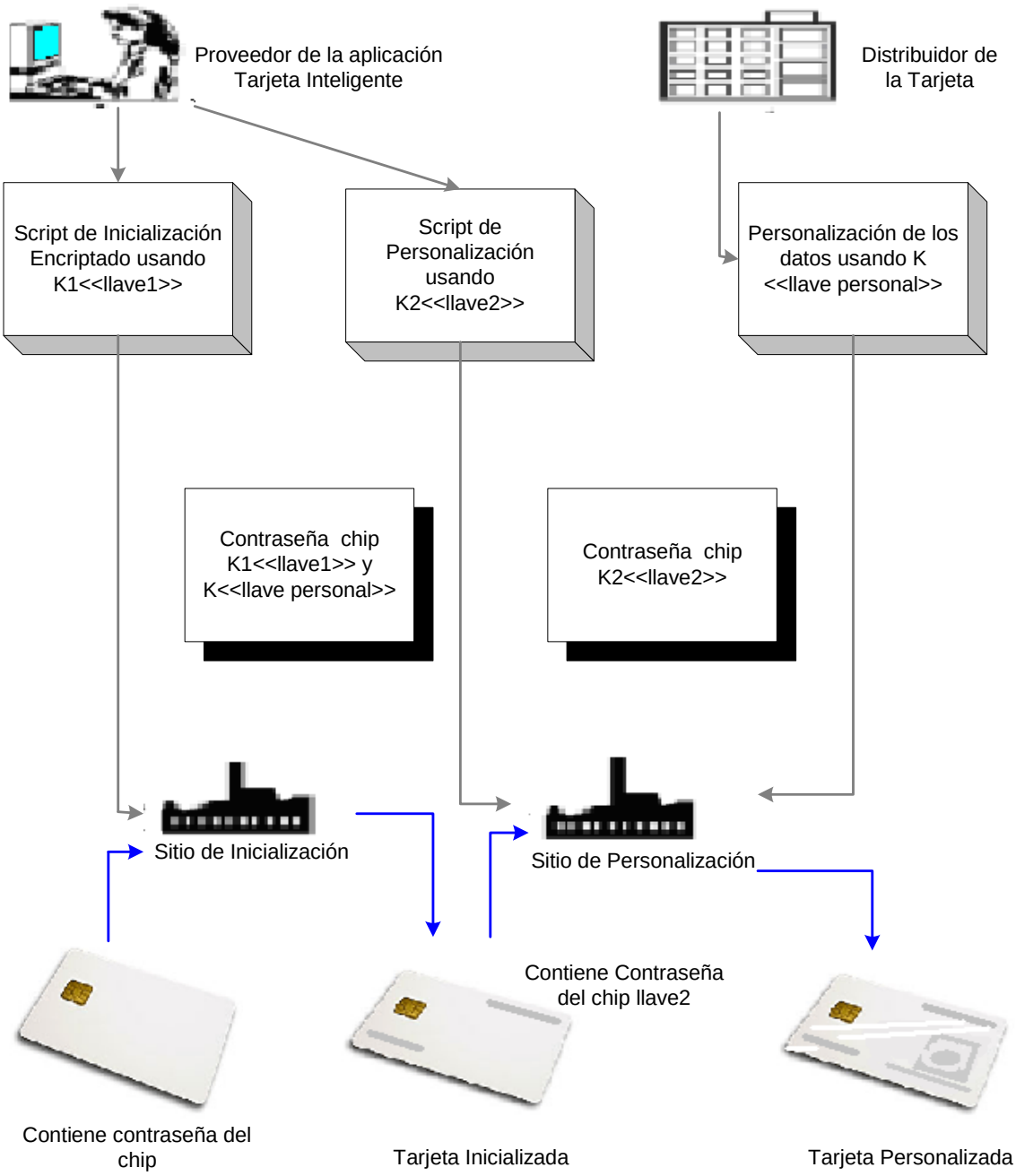


Figura 1.3 Proceso de Seguridad en una Tarjeta Inteligente

Como se puede apreciar en el diagrama la información concerniente a la aplicación es protegida mediante la utilización de llaves como las de transporte, personalización y contraseñas propias de los sistemas. El almacenamiento de estas llaves es realizado por el emisor de la tarjeta (propietario de la aplicación), para evitar una intrusión en las mismas, además de que en la mayoría de los casos se realizan en dispositivos de seguridad para la encripción de datos.

Adicionalmente a estos procedimientos de seguridad electrónica es necesario imprimir las tarjetas con elementos de seguridad como son:

-Hologramas

-Impresión prismática. Cambios sutiles de colores a través de la credencial.

Existen diferentes diseños, los cuales son detalladamente fabricados y difíciles de copiar, a continuación mencionamos algunos:

-Diseño de líneas finas. Diseño detallado compuesto de varias líneas finas que logran que el documento sea difícil de falsificar.

-Tinta fluorescente invisible. Una tinta que a primera vista es invisible al ojo humano y sólo puede apreciarse bajo una luz ultravioleta.

-Tinta fluorescente visible. Una tinta que a primera vista es visible al ojo humano.

-Microtexto invertido. Un texto tan pequeño (.2mm) que dificulta el copiado y la digitalización por medio de aparatos de alta resolución. El microtexto puede ser incorporado en diseño de imágenes, guilloches, líneas, etc. Puede ser invertido y contener errores escondidos que no podrán ser detectados por un falsificador.

-Diseño tipo guilloche. Sólo puede ser producido con software especial de seguridad. Puede crearse utilizando diferentes anchos de líneas y colores opuestos. Es una característica típica que impide la falsificación.

-Tinta óptica variable. Tinta que cambia de un color a otro cuando varía el ángulo de reflexión de luz.

-Diseño de línea variable. Se puede incorporar en los patrones de guilloche, la fabricación de ellos resulta muy difícil de reproducirse. Puede hacer que un color parezca tener variaciones de densidades, y puede crear la ilusión del "arcoiris" sutil del gradiente; a través de unos o más colores. Este efecto se puede reproducir solamente con software especial de la seguridad.

A estas alturas el lector se puede preguntar, pero, ¿y tanta seguridad es necesaria?

Esta pregunta dependerá del tipo de aplicación para la cual se va a utilizar la tarjeta.

En la actualidad los estándares para transacciones bancarias son muy exigentes con los niveles de seguridad que manejan ya que la información a la que se tiene acceso es sumamente delicada, debido a esto es que es necesario extremar los procedimientos.

En cambio existen otras aplicaciones más sencillas como podrían ser controles de acceso en los que una rápida respuesta tiene mayor prioridad que un gran nivel de seguridad. O bien el ambiente de interacción es muy controlado y una excesiva seguridad elevaría costos administrativos.

Lo que es importante recordar siempre es que una Tarjeta Inteligente tiene tres funciones principales:

- *ALMACENAR DATOS*
- *ENCRIPTAR*
- *LEER Y ESCRIBIR DATOS*

Es decir, es un dispositivo de almacenamiento de información en la que la seguridad es su principal atributo. Es por eso que es ideal para el manejo de datos sensibles como dinero electrónico, información personal o identificación.
Además de que la información contenida en la tarjeta puede ser actualizada después de la emisión de la misma.

Capítulo II . DEFINICIÓN

II.1 ¿Qué es una Tarjeta Inteligente?

Para definir el concepto de tarjeta inteligente es necesario conocer el concepto de tarjeta:
Una tarjeta es un dispositivo de plástico o papel de dimensiones determinadas que sirve para guardar información de manera segura.
La primera tarjeta digital en surgir fue la conocida Tarjeta de Banda Magnética. Fue desarrollada con una principal intención, permitir que los bancos ofrecieran a sus clientes operar de forma rápida y de manera efectiva en cajeros automáticos y así mismo lograr tener puntos de venta específicos.

Este medio electrónico-magnético es uno de los sistemas de identificación automática más utilizado debido a su bajo costo, su utilización se ha generalizado de tal forma que, al año se producen y utilizan una media de 1400 millones de tarjetas magnéticas en el mundo, regularmente para lo que se utiliza este medio es para las tarjetas de débito o crédito.

Tal cual era su finalidad, las tarjetas magnéticas siguen produciendo importantes resultados en el mercado de las finanzas, pues recordemos que en México los mismos bancos han reportado incrementos en su cartera de clientes y que en general la gente ha optado por manejar alguna tarjeta de crédito o débito, en vez de manejar efectivo.

Sin embargo no ofrecen soluciones para los nuevos mercados y servicios que están surgiendo: la televisión interactiva, telefonía digital, monedero electrónico y en general todas aquellas aplicaciones que requieren cada vez más un sistema de seguridad en las transacciones electrónicas.

A continuación explicaremos en forma breve el funcionamiento de una Tarjeta de Banda Magnética.

Su tecnología esta basada en el mismo concepto de los discos magnéticos: partículas de ferrita de bario u óxido de hierro, es lo que está contenido en la banda de color negro.

La información está contenida en las pistas o tracks, ver *figura 2.1*

Figura 2.1 Tarjeta de Banda Magnética

La banda angosta en la banda magnética que corre paralela al borde de referencia en el cual se codifican los datos es llamada pista o track. Regularmente es de unos 2.5 milímetros y puede localizarse a cualquier distancia del borde de referencia. El número de pistas es determinado enteramente por el ancho de la banda magnética.

Típicamente, las tarjetas son codificadas con 5 bits por carácter, por lo que pueden almacenar hasta 80 caracteres por pista.

Las tarjetas de banda magnética son reguladas por estándares, y a continuación explicaremos qué estándares las rigen y comentaremos brevemente que contienen sobre la definición de la estructura en la tarjeta:

Una sola banda magnética puede contener varias pistas de datos (o *tracks*), los cuales pueden ser reescritos y modificados para su actualización. La serie de estándares ISO 7810, 11, 12 y 13 especifican un formato de tres pistas, esquema

de codificación y densidad de bits para todas las aplicaciones financieras con tarjetas.
Existen estándares para muchas localizaciones de pistas, las más conocidas son los tracks ISO #1, #2 y #3 en las tarjetas de crédito. Las densidades y formatos de tarjetas de crédito ISO son además los más ampliamente utilizados, conteniendo 42 Decimales en Código Binario (DCB o *BCD*) ó 30 caracteres alfanuméricos por pulgada a 210 BPI (bits por pulgada), y 15 DCB por pulgada a 75 BPI (bits por pulgada). Es importante hacer notar que la banda magnética no está limitada a estas localizaciones de pistas de tarjetas o densidades y muchas otras se utilizan de manera común.

El objetivo principal de una tarjeta de banda magnética es identificar a un cliente para acceder a una base de datos remota con la que se establece una conexión. Realmente la información la tiene una base de datos, quien es la que permite aceptar o rechazar las transacciones que el cliente realiza. En la actualidad el problema que se tiene es que las tarjetas de banda magnética ya no satisfacen la demanda de problemas que se están presentando debido a que la tarjeta magnética ofrece muy baja densidad de datos, es de baja fiabilidad y existe muy poca seguridad en la información que lleva, así que, es entonces que, para solucionar los problemas que presenta el uso de una tarjeta de banda magnética es como surge otra nueva tecnología: Sistemas Embebidos (“Embebed System”), que es la tecnología en la que está basada la Tarjeta Inteligente.

Así pues, podemos entonces entrar de lleno y conocer lo que es una Tarjeta Inteligente:

"Una tarjeta inteligente ("SmartCard") es una tarjeta de plástico, como las que conocemos y acostumbramos usar para pagar la compra, con la única diferencia de que tiene incrustado un circuito integrado, que no llega a los 10 mm de lado", ver *figura 2.2 y figura 2.3*

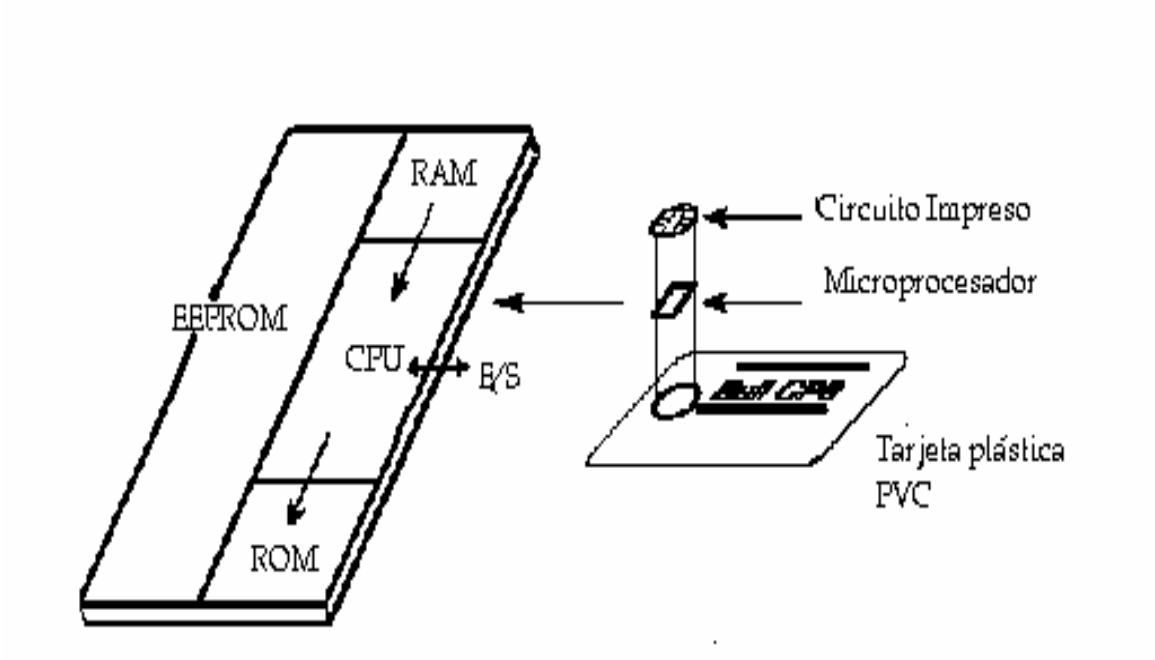


Figura 2.2 Tarjeta Inteligente

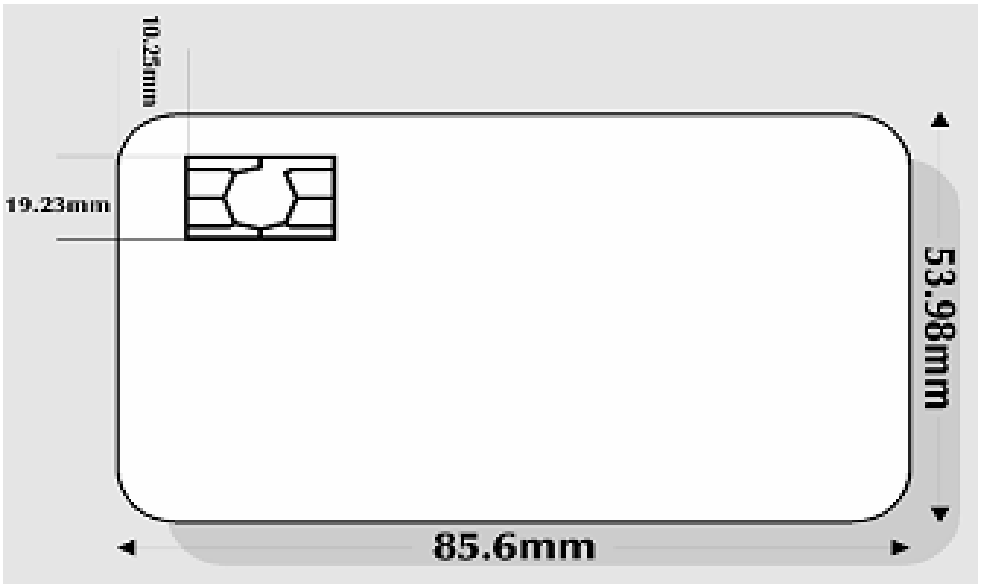


Figura 2.3 Dimensiones de una tarjeta con chip

La Tarjeta Inteligente surge de la evolución de la tarjeta de plástico convencional en combinación con un circuito integrado. La incorporación de un chip ofrece tres nuevos elementos que pueden favorecer su utilización en general:

Miniaturización. Las densidades de integración de controladores y memorias que se alcanzan en la actualidad, permiten ofrecer un panorama de posibilidades y de funciones, lo que origina su expansión en el mercado y un nuevo medio de intercambio de información.

Lógica programable. La Tarjeta Inteligente incorpora la potencia de las computadoras, incluyendo las funciones lógicas y de control que se aplican a los negocios, junto con funciones avanzadas de seguridad y nuevas aplicaciones.

Interfaz directa de comunicaciones electrónicas. Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las Tarjetas Inteligentes.

Por su tipo de interfaz existen dos tipos de Tarjetas Inteligentes, sin contacto (contactless) y con contacto, las cuales se explicarán en el apartado siguiente.

Dentro de cada tipo de Tarjetas Inteligentes se puede tener también diferencia en cuanto a estructura. Se distinguen dos tipos principales de Tarjetas Inteligentes:

- El primero está formado por las tarjetas que sólo tiene memoria. Se utilizan para reemplazar a las monedas en los teléfonos, como medios de acceso prepagado para circular, aparcar u otras actividades similares.
La forma en como se almacena información en las tarjetas de memoria en ellas es de la siguiente manera:

La Memoria se construye a base de transistores bipolares. Para introducir la información se hace circular una corriente que rompa uno de los conductores. De esta manera se puede almacenar información binaria.

Por ejemplo, conductor roto es un 0 y el conductor entero un 1. Y éste es teóricamente otro de los puntos débiles de cualquier sistema: mediante técnicas de afinamiento se puede ir adelgazando la capa de metal que protege los circuitos hasta que éstos queden a la vista. Después, con un microscopio electrónico se puede determinar la topología del "chip".

- El segundo tipo de Tarjetas Inteligentes contiene un circuito integrado con memoria y un microprocesador. Esto añade funciones de seguridad, permite el control de aplicaciones múltiples y ofrece la posibilidad de actuar como interfaz de comunicaciones.

El chip genera la diferencia entre las llamadas tarjetas de memoria y las tarjetas con microprocesador, ya que en las de memoria no es posible actualizar datos ni procesar información.

La tarjeta requiere de una interfaz externa para obtener la información, es decir, un lector, pues los datos contenidos sólo los podemos accesar a través del cajero, por ejemplo, hablando de una tarjeta con aplicación débito / crédito.

Las Tarjetas Inteligentes son introducidas en la ranura del lector y se activan al recibir el comando de encendido, a través del bus de datos, a partir de este momento la comunicación es administrada por el sistema operativo de la tarjeta y la interfaz externa, siguiendo los protocolos del estándar ISO 7816.

La *figura 2.4* nos muestra una arquitectura típica de un microprocesador para Tarjetas Inteligentes.

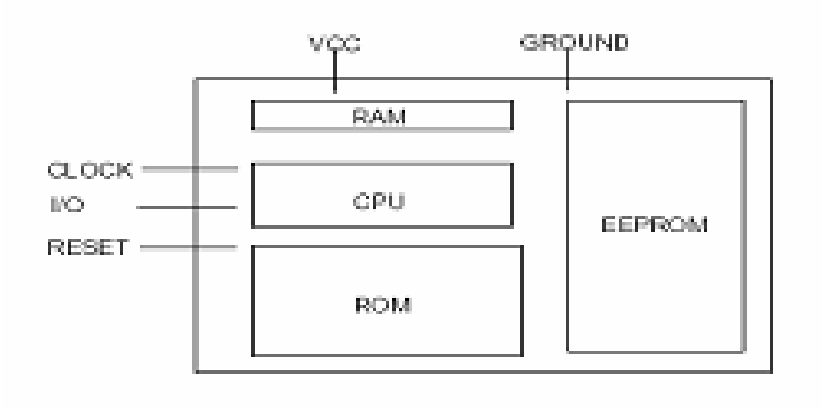


Figura 2.4 Arquitectura de un microprocesador en Tarjetas Inteligentes

RAM: Usada para almacenar registros temporales.

ROM: Contiene el Sistema Operativo

EEPROM: Usada principalmente para aplicaciones de Usuario aunque también es utilizada por el Sistema Operativo.

CPU: Controla el sistema operativo, así como los buses de comunicación y el acceso a las memorias.

Con base en la *figura 2.4*, podemos ver que la Tarjeta Inteligente contiene las funcionalidades de un ordenador, tomando en cuenta que el chip contiene un sistema operativo, y esto nos permite contener aplicaciones diversas a diferencia de una tarjeta de banda magnética o una de sólo memoria.

II.2 Tipos de Tarjetas Inteligentes.

II.2.1 Tarjetas Inteligentes sin contacto (contact-less)

Tarjetas Inteligentes sin contacto

Poseen además del chip una antena de la cual se valen para realizar transacciones.

Ideales cuando las transacciones tienen que ser realizadas muy rápidamente
Definición: ISO 14443

A las tarjetas sin contacto se les hace pasar frente a una antena para poder ejecutar una transacción, una lectura. A simple vista se parecen una tarjeta con contacto o sin contacto, pero la diferencia está en que tiene un microchip y una antena embebida dentro del chip, componentes que le permiten a la tarjeta comunicarse con una unidad acopladora de antenas sin un contacto físico. Este tipo de tarjetas ofrecen la solución ideal para aquellas operaciones en las que se requiere de un proceso rápido, de una lectura instantánea; algo así como la entrada a algún sitio de manera masiva, entrada y salida de automóviles (estacionamientos), o como lo sería algún sistema de transporte público, por citar algunos ejemplos.

Un sistema de este tipo, sin contacto, está compuesto por:

Un chip (microcontrolador + interfaz de radiofrecuencia),
Una tarjeta que contenga antena, y
Un lector

La interfaz de radiofrecuencia debe de proveer al microcontrolador energía estable, una señal de reloj y los datos recibidos del lector, a su vez la interfaz de radiofrecuencia debe de recibir del microcontrolador datos que serán enviados al lector y por último una señal de reset.

El esquema de la *figura 2.5*, nos permite hacer una pequeña comparación entre un sistema con contacto y uno sin contacto:

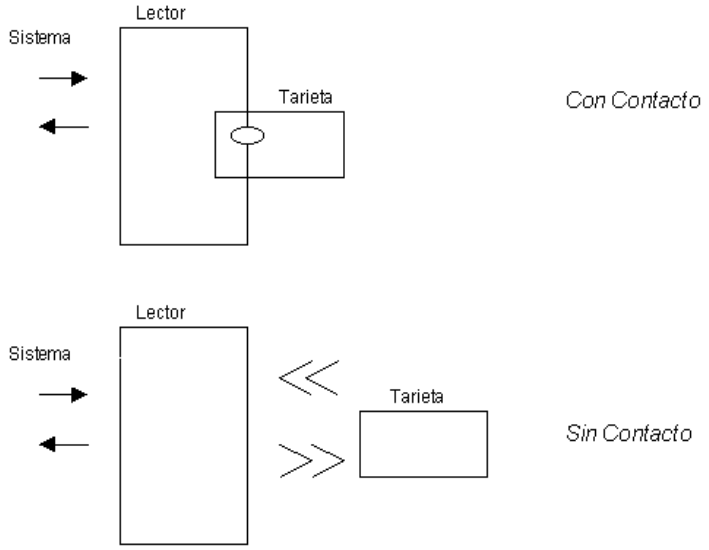


Figura 2.5 Comparación entre una TI con contacto y una TI sin contacto

La comunicación que se realiza con chips *sin contacto (contactless)*, se da de acuerdo con los cambios de corriente que experimentan tanto la antena de la tarjeta como la antena del dispositivo receptor, y son estos cambios los que se interpretan como la información que está siendo intercambiada entre ambos elementos. Ahora para prevenir que exista dos o más tarjetas intentando realizar una operación al mismo tiempo sobre el mismo lector, se utiliza el método conocido como *anticolisión*, que permite que una y sólo una tarjeta sea la que realice su intercambio de datos con el lector en un mismo diferencial de tiempo, con el fin de no mezclar y confundir información; este método lo que hace es identificar las tarjetas presentes en el campo y permite *direccionamientos* (instrucciones) sobre una y sólo una tarjeta seleccionada.

El estándar que rige las tarjetas sin contacto es el ISO 14443 y consta de las siguientes secciones:

Parte 1: Características Físicas.

Parte 2: Potencia para Radiofrecuencia y señal para la interfaz.

Parte 3: Inicialización y anticolisión.

Parte 4: Protocolos.

El diseño con tarjetas contactless está limitado significativamente por la energía disponible para energizar y operar un chip en un campo de radiofrecuencia. El factor importante en tarjetas sin contacto es el tamaño de las antenas, pues el tamaño de la antena determina la cantidad de energía que puede ser inducida a la tarjeta y limita los rangos de lectura/escritura en la misma.

Las aplicaciones con tarjetas sin contacto por lo general van desde simplemente detectar la tarjeta en el campo de Radio Frecuencia a la interpretación de un mensaje que puede ser actualizado por una tarjeta. Los datos intercambiados están limitados a unos cuantos bytes.
Los diseños para tarjetas sin contacto, tienen las siguientes consideraciones:

- Distancias y rangos amplios en campos de radio frecuencia
- Detección de colisiones.
- Velocidades de proceso.
- Seguridad al transmitir datos.

II.2.2 Tarjetas Inteligentes con contacto

Tarjetas inteligentes con contacto

Poseen una placa de contactos además del chip

Necesitan de un dispositivo lector/grabador para comunicarse con el exterior

Definición: ISO 7816

Las tarjetas de contacto son las que deben de ser insertadas en un lector de tarjetas. Tienen un plato sólido dorado de alrededor de media pulgada de diámetro en el frente, en vez de una banda magnética en la parte trasera como las tarjetas de débito y crédito, aunque puede contenerla.

Cuando la tarjeta es insertada en el lector se hace el contacto eléctrico necesario con los puntos que permiten transferir datos de y hacia el chip. Este tipo de tarjetas son las que se usan más comúnmente en casi cualquier aplicación, aunque en algunas otras, tal como es el transporte, son de uso más frecuente y eficaz, las tarjetas sin contacto.

El estándar ISO 7816 establece los parámetros para Tarjetas Inteligentes con contacto y se compone de varias secciones en donde se especifican los requerimientos mínimos tanto para las características físicas, técnicas de acceso a los datos y técnicas de almacenamiento de datos.

La *tabla 2.1* nos ayuda a entender como están conformadas las secciones del ISO 7816:

Sección	Nombre de la Sección
1	Características físicas
2	Tamaño y localización de los contactos
3	Señales electrónicas y protocolos
4	Comandos
5	Identificadores de aplicaciones
6	Elementos de los datos para intercambio
7	Comandos mejorados para intercambio de datos

Tabla 2.1. Secciones de ISO 7816

La idea de tener secciones dentro de ISO 7816, se debe a la probable evolución por partes, y de acuerdo con las demandas que se vayan presentando en el mercado y los propios avances tecnológicos necesarios.
A continuación se dará una síntesis de lo que contiene cada sección:

En la *sección 1* se describen las características físicas de las Tarjetas Inteligentes (el ancho del plástico, por ejemplo) y diferentes métodos usados para probar su concordancia con los requerimientos.

En la *sección 2* se definen las dimensiones y las posiciones de los contactos eléctricos:

Cada contacto debe tener un área rectangular mínima de 2 (mm) de ancho por 1.7 (mm) de largo y debe de estar aislado de los demás contactos. En la *tabla 2.1.1* se definen 8 contactos, desde C1 hasta C8:

Contacto	Función
C1	Voltaje de alimentación (+5 [V])
C2	Reset (RST)
C3	Reloj (CLK)
C4	Sin conexión y reservado para uso futuro
C5	Tierra (0 [V])
C6	Vpp (Voltaje de programación)
C7	I/O
C8	Sin conexión y reservado para uso futuro

Tabla 2.1.1 Dimensiones y Posiciones de los contactos

Los diseños de los chips son variados, pero mantienen los contactos en la posición indicada en el estándar. Algunos diseños de chips, pueden lucir como los de la *figura 2.6*, y el dibujo depende del fabricante:

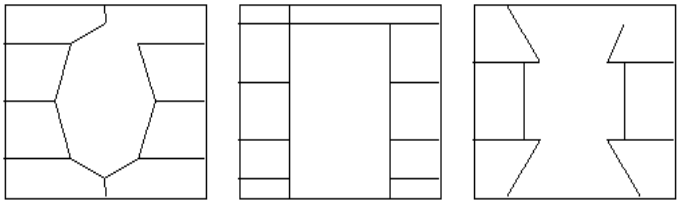


Figura 2.6 Tipos de diseño de chip

Sección 3. Trata sobre las señales electrónicas y protocolos de transmisión. Así también describe en qué dirección se entabla la comunicación terminal-tarjeta. Cabe mencionar que la función de reset de la tarjeta corresponde al primer contacto eléctrico que se da al introducir la tarjeta en una terminal, la justificación a esta norma se describirá posteriormente.

Para poder pasar a la sección siguiente es necesario revisar cada uno de los contactos y su uso:

Vcc: Este contacto es usado para proveer de energía a la tarjeta con la fuente de alimentación. La corriente máxima está definida por la tarjeta misma. La interfaz debe ser capaz de entregar esta corriente dentro del rango especificado para los valores de voltaje.

I/O: Este contacto es usado como entrada (modo de recepción) o salida (modo de transmisión). La información intercambiada usa los siguientes estados lógicos, definidos en ISO 1177:

- Estado Z.- Si la tarjeta y el dispositivo de interfaz están en modo de recepción o si el estado es impuesto por el transmisor.

- Estado A.- Si este estado es impuesto por el transmisor.

Cuando ambos extremos de la línea estén en modo de recepción, la línea deberá estar en estado Z (estado alto). Cuando ambos extremos no estén igualados en modo de transmisión, el estado lógico de la línea puede estar indeterminado. Durante la operación, el dispositivo interfaz y la tarjeta no deben de estar en modo de transmisión.
El dispositivo de interfaz debe de ser capaz de enviar la corriente definida dentro de los rangos establecidos y en los voltajes predeterminados.

CLK: Este contacto es usado para proveer a la tarjeta de una señal de reloj.

RST: Este contacto es muy útil ya que nos sirve para dar una señal de reset (restauración) a la tarjeta. Como ya se mencionó, el *reset*, es la primera respuesta que una tarjeta chip nos entrega al momento de ser energizada y está compuesta por una cantidad definida de bytes los cuales nos sirven para identificar datos como qué tipo de tarjeta es, a qué proveedor pertenece o qué sistema operativo emplea.

Vpp: Este contacto actualmente está reservado para uso futuro.

Sección 4. Los intercambios de datos, entre tarjeta y lector, son descritos en esta sección. Estas instrucciones son la base de los comandos comunes que son empleados para interactuar con la tarjeta, permiten la creación de directorios dentro de la tarjeta, modificación, lectura, escritura y borrado de los datos dentro de los archivos.

La *tabla 2.2* especifica los comandos elementales dentro de ISO:

Comandos ISO 7816
Seleccionar archivo
Escritura binaria
Lectura binaria
Actualización binaria
Borrado binario
Lectura de registros
Escribir registros
Log (historial) de registros
Actualizar registros
Obtener datos
Poner datos
Verificación
Autenticación interna
Autenticación externa
Obtener challenge
Manejar canal
Obtener respuesta

Tabla 2.2 Comandos Elementales

En esta sección, se habla de dos categorías de archivos:

- DF (Archivo Dedicado, de las siglas en inglés *Dedicated File*)

- EF (Archivo Elemental, de las siglas en inglés Elementary File)

La organización de los archivos dentro de una tarjeta lleva una jerarquía, la cual consiste de un archivo principal o maestro al nivel de raíz, que también es un archivo dedicado (DF).

Los archivos elementales (EF) se dividen en:

a) EF´s que almacenan datos para manejo y para propósitos de control de la tarjeta.

b) EF´s que almacenan datos que son interpretados por la tarjeta, a estos archivos se les llaman de "trabajo".

Los archivos elementales (EF) pueden ser de diferentes tipos:

- Transparentes
- Fijos
- Variables
- Cíclicos

Dentro de éstos, los que son más ampliamente usados son los cíclicos, ya que son aquellos que nos sirven para almacenar datos que continuamente están siendo modificados; como ejemplo tenemos los archivos donde se guardan las últimas transacciones o movimientos que se han realizado con el chip, es decir funcionan como historiales o logs.

Los archivos fijos, también son de gran importancia, puesto que son éstos los que guardan datos que no requieren ser modificados, tales como nombres, fechas, números de placas, por decir algunos.

Los identificadores de archivo nos sirven para poder diferenciar entre distintos tipos de archivos de la tarjeta y niveles dentro de la misma y están compuestos por 2 bytes. Los niveles en la tarjeta son usados para poder diferenciar entre aplicaciones.

Sección 5. Se define la forma de cómo se deben reservar los identificadores de archivos correspondientes a los emisores de tarjetas.

Sección 6. Esta sección describe los elementos de los datos (como el nombre, NIP, fecha de expiración) que pueden ser manipulados por el microcontrolador. Estos elementos pueden ser manejados por los comandos mencionados en la sección 4.

Sección 7. Se encuentra en desarrollo y describe las funciones adicionales y características que estarán disponibles para mejorar comandos.

II.3 Su aplicación y ámbitos de aplicación

En la actualidad las Tarjetas Inteligentes están resultando muy utilizadas en los siguientes servicios:

- Tarjetas de Telefonía Móvil.
- Tarjetas de Salud. Puede contener aparte de información, el historial clínico o información relativa a enfermedades crónicas o alérgicas.
- Monedero electrónico bancario. El chip contiene información de tipo financiero ya que es conceptualizado como dinero electrónico.
- Tarjetas telefónicas. En este sector es donde las Tarjetas Inteligentes han tenido un mayor uso. El chip contiene información acerca del saldo pendiente de uso en casetas telefónicas preparadas para ello.
- Otros servicios entre los que destacan utilización en servicios comunes en universidades y tarjetas de pago de TV. En varias universidades europeas se ha puesto en marcha proyectos basados en esta tecnología. Cada estudiante posee un tarjeta como identificación que le permite tener acceso a todos los servicios de la universidad (fotocopias, biblioteca, etc.) y a su vez es tarjeta de crédito y monedero electrónico.

La utilización de Tarjetas Inteligentes con microprocesador presenta las siguientes ventajas:

- Presentan un costo por transacción que es menor que el de las tarjetas magnéticas convencionales. Esto es incluyendo el costo de la tarjeta, de la infraestructura necesaria y de los elementos para realizar las transacciones.
- Configuraciones múltiples que puede tener, lo que permite utilizarla en distintas aplicaciones.
- Seguridad de alto nivel.

III. APLICACIÓN

III.1 ¿Porqué utilizar esta tecnología en la aplicación AZUL Y ORO?

Para dar respuesta a esta pregunta analicemos el ámbito de aplicación, para de esta manera, comprender las ventajas y alcances que tienen estos dispositivos, y posteriormente analicemos su estructura y funcionamiento.
Es importante considerar que debido a la capacidad de almacenamiento que se tiene en comparación con las tarjetas de banda magnética o algún dispositivo de memoria es posible instalar múltiples aplicaciones en las tarjetas:

Aplicaciones Bancarias: Debido a la seguridad que las Tarjetas Inteligentes ofrecen, éstas son ideales para realizar operación de débito/crédito, o pagos vía Internet.

Monedero Electrónico: Los monederos surgen de la necesidad de los bancos de reducir el tráfico de pagos en efectivo o en cheques, especialmente para compras pequeñas.
Un Monedero Electrónico se puede definir de la siguiente manera: cualquier tarjeta o aplicación de tarjeta que contiene un valor real de dinero en forma de efectivo electrónico el cual fue recargado para la obtención de algún bien o servicio.

Las principales operaciones en los monederos son:
Pagos
Recargas
Consulta de saldos
Transferencias a otros monederos

Programas Gubernamentales: Transferencia de bienes por medio del registro del uso de la tarjeta con la gran posibilidad de agilizar trámites y optimizar recursos materiales (papelería, inventario, etc.) o bien recursos humanos.

Seguridad de Accesos Físicos: EL control a cuartos o lugares de acceso restringido puede ser controlado por la validación de la tarjeta e incluso ser completado con algún análisis de tipo biométrico como puede ser huella digitales, análisis de retina, etc.

Seguridad de Accesos a Sistemas: De la misma manera que las zonas restringidas el acceso a dispositivos electrónicos puede ser controlado mediante la implementación de este tipo de solución.

Aplicaciones de Lealtad: Para fomentar el consumo de un bien o servicio es posible guardar en la tarjeta premios o beneficios dependiendo de la frecuencia, monto, fecha, etc., de las transacciones u operaciones hechas. A este tipo de intercambio se le conoce como aplicaciones de lealtad, y es muy común encontrar estas aplicaciones en las tarjetas inteligentes ya que la información se guarda en la tarjeta y reduce los costos de comunicación y manejo de grandes dispositivos de almacenamiento para llevar el correcto registro.

Adicionalmente es necesario mencionar que además de todas las ventajas que presenta el manejo de la información electrónica en la parte gráfica como se explicó en el capítulo 1, también se pueden utilizar métodos de seguridad como son el uso de hologramas, capas de protección, etc.

Una vez que hemos comentado el gran ámbito de aplicación que tienen las tarjetas explicaremos el ambiente que rodea este tipo de aplicaciones.

Como se mencionó en el capítulo II, una Tarjeta Inteligente se puede ver como una PC, esta analogía es correcta, pero se tienen las siguientes consideraciones:

-El portador de una tarjeta no es el dueño de las aplicaciones que corren sobre ella.

-La Tarjeta Inteligente requiere de interfaces físicas ajenas a ésta para su explotación, como lo son los lectores, el software, el cableado,etc.

- Las Tarjetas Inteligentes al incorporar el microchip pueden adherir, borrar y de alguna manera manipular información en su memoria. Por ello es que decimos pueden ser vistas como una computadora en miniatura con un puerto de entrada/salida, sistema operativo y disco duro.

- El microchip trae un microprocesador que está disponible en arquitecturas de 8, 16 y 32 bits, lo que nos permite procesar la información.

- Su capacidad de almacenamiento de datos varía entre 300 a 64000 bytes con expectativas de incrementar esto último con los avances tecnológicos.

Pero, si la tarjeta es sólo un componente de un sistema basado en estas tecnologías, ¿Por qué usarla?
Existen puntos fundamentales que justifican la utilización de éstas:

Portabilidad.

Las tarjetas se pueden llevar en cualquier parte ya que sus dimensiones físicas así lo permiten.

Almacenamiento de la Información.

La obtención de la información que reside en la tarjeta puede ser extraída solamente bajo ciertas condiciones de acceso. Y como la tarjeta es un medio de almacenamiento, la información que se tiene puede ser información personal, directorio, configuración de alguna PC, etc.

Disponibilidad.

Como se supone que el usuario de la tarjeta tiene a la mano su tarjeta, entonces la información esta siempre disponible, pues puede hacer uso de ella cada vez que el usuario lo disponga.

Servicios Criptográficos.

Una tarjeta inteligente puede desarrollar algoritmos criptográficos habilitando servicios como son autenticación, confidencialidad mediante llaves que se encuentran física y lógicamente protegidas

Autenticación de Usuario.

La autenticación del usuario se puede realizar fuera de línea o en línea con algún sistema central.

Almacenamiento y Pruebas de Operación.

Este punto se refiere a que al hacer algún cambio en los campos de la tarjeta se puede realizar una autenticación para validar la correcta operación.

Protección Física de Llaves de la Tarjeta.

Las tarjetas inteligentes están diseñadas para que la obtención de las llaves sea prácticamente imposible.

Control de Aplicaciones por Emisor.

Las aplicaciones que corren en la tarjeta son definidas por el Emisor de la tarjeta y no por el Usuario de ésta.

Jerarquía de Archivos.

Para la organización de la tarjeta de acuerdo al estándar ISO 7816 la información se ordena jerárquicamente en diferentes archivos. En el diagrama de la *figura 3.1* se muestra la organización de los archivos.

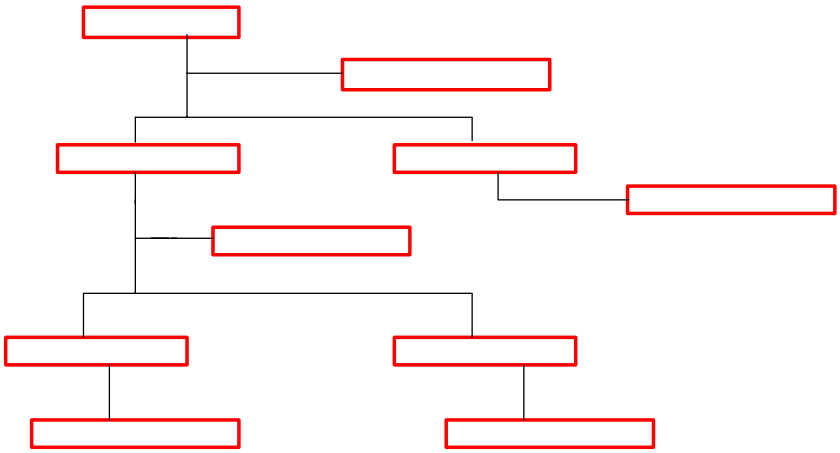


Figura 3.1 Diagrama de Jerarquía

Una vez que hemos definido estos puntos acerca de las ventajas de una tarjeta Inteligente procedamos a definir los elementos que componen un sistema con esta tecnología.

EMISOR: Es la entidad legal responsable de la administración, difusión, integridad, confidencialidad, sistema, terminalización y en general de toda la operación y logística que envuelve a este tipo de aplicaciones.

Archivo Maestro

Ar

Archivo Dedicado

Las actividades del emisor se enlistan a continuación:

-Comprar y Personalizar la tarjeta

-Administrar el sistema central para el control y la autorización de operaciones

-Asegurar las llaves que utilizan las aplicaciones

-Coordinar la instalación de terminales en las que se hará uso la Tarjeta Inteligente

USUARIO: Es el portador de la tarjeta con las aplicaciones que el emisor tenga sobre éstas

-Reportar al emisor anomalías en la aplicación

-Realizar las operaciones de las tarjetas

SISTEMA CENTRAL: Este sistema es un HOST que puede estar desarrollado bajo cualquier plataforma y que contiene el histórico de transacciones, terminales, tarjetas, además de que de acuerdo a los requisitos de seguridad se puede establecer las llaves para las aplicaciones de la tarjeta.

TERMINAL: Es un dispositivo generalmente con teclado que se encarga de energizar la tarjeta y dar la secuencia al reloj de la tarjeta.

La terminal es la encargada de comunicarse con la tarjeta, La comunicación es “Half Duplex”.

Dependiendo del diseño del sistema en los terminales también pueden estar las llaves para la generación de certificados.

La característica principal de una tarjeta inteligente es que sólo los medios que tengan los mecanismos y recursos adecuados podrán tener acceso a la información contenida en los chips.

Cabe mencionar que la seguridad es un aspecto relativo ya que ningún algoritmo criptográfico, así como medio de almacenamiento garantiza por si solo la confidencialidad de los datos, ya que se debe tener un proceso

administrativo por el cual se genera la información y éste debe estar complementado con medidas de seguridad. Como puede ser:

-Llaves segmentadas
-Firmas de contratos
-Dispositivos especializados para manejo de información confidencial

Por supuesto cabe hacer mención de que nada es absolutamente seguro, pues la seguridad se vuelve un aspecto relativo en cualquier medio donde se maneja información confidencial, es decir, por más encriptada que esté una clave, si el usuario no tiene el cuidado adecuado al manejarla, no servirá de nada contar con el mejor sistema de seguridad al que haya sido expuesta su tarjeta.
Pero si podemos decir que la seguridad que ofrecen las tarjetas inteligentes es hasta el momento inviolable.

III.2 La seguridad que ofrece

Una parte fundamental del diseño de un sistema de seguridad es garantizar que las contraseñas (passwords) y llaves (dependiendo del tipo de aplicación) puedan ser utilizados por los usuarios y dispositivos autorizados exclusivamente.

Almacenar las llaves en medios digitales puede resultar fácilmente violado, modificado, alterado o accesado por alguna persona malintencionada no autorizada.

Para dar solución a este problema existen dispositivos “tamper-resistant” el cual no tiene una traducción satisfactoria al español, estos sistemas garantizan que el acceso a los datos sea prácticamente imposible para las personas no autorizadas, ya que éstos proveen además de protección lógica, es decir, algoritmos criptográficos, proveen de una protección física de lectura, prácticamente no se puede tener acceso a los circuitos de almacenamiento.

Algunos dispositivos “tamper-resistant” no permiten bajo ninguna condición la exportación de los datos de seguridad (llaves) hacia algún otro dispositivo. Obviamente todos los dispositivos “tamper-resistant” deben ser capaces de realizar procesos criptográficos, ya que de otra manera la exposición de las llaves y datos de seguridad sería de alguna manera más susceptible a monitoreos.

Existen diversos dispositivos de este tipo entre los cuales se incluye a las Tarjetas Inteligentes.

Como se mencionó anteriormente, aparte de la protección física que tienen las Tarjetas Inteligentes existen otros mecanismos de tipo lógico que tienen su fundamento en la criptografía, antes de detallar estos procedimientos hablaremos acerca de lo qué es y cómo se utiliza la Criptología.

La Criptología se divide fundamentalmente en dos áreas: Criptografía y Criptoanálisis.
La Criptografía: Es el medio por el cual se estudian los diversos mecanismos de encripción.
El Criptoanálisis: Es el estudio de cómo descifrar o vencer los algoritmos criptográficos.
El objetivo principal de la Criptología es mantener en secreto un mensaje.
Para cumplir con esta misión la Criptología tiene que pasar por dos pasos fundamentales. ENCRIPCIÓN y DECRIPCIÓN.

La encripción es la transformación de datos en alguna forma (conocido como datos cifrados o criptograma) mediante la cual se tenga la menor posibilidad de ser leída o extraída sin el correcto conocimiento de alguna “llave” o método para obtener los datos originales. En otras palabras el propósito de la encripción es mantener un mensaje en secreto aun cuando los datos cifrados se puedan obtener fácilmente.

La decripción es el proceso inverso a la encripción, es decir convertir los datos cifrados a una forma legible nuevamente.

Tanto el proceso de encripción como el de decripción requieren de información secreta que se conoce como llave. Para algunos mecanismos de encripción la llave es la misma para ambos procesos y en otros casos es posible que la llave sea diferente en ambos procesos.

La Criptología actual es más que el proceso de encripción-decripción, requiere de procesos como la autenticación y la certificación. La autenticación es un proceso mediante el cual se determina si un mensaje fue creado por una entidad. Generalmente se utilizan firmas digitales.

La certificación es el proceso mediante el cual se garantiza que el mensaje no ha sido manipulado y es auténtico.

Los cripto-sistemas más usados en la actualidad son los llamados:

-*Sistemas de llave Pública*: También conocido como llave asimétrica. En este caso cada usuario tiene un par de llaves una privada y una pública.
La llave pública se puede difundir sin ningún problema, mientras que la llave privada debe permanecer en secreto.
La encripción se realiza con la llave pública mientras que la llave privada sirve para hacer la desencripción.

EL criptosistema más popular para este caso es el “Rivest, Shamir, and Adleman” RSA.

-*Sistemas de llave Privada*: También conocidos como criptografía simétrica, tanto para la encripción como la decripción se utiliza la misma llave. El más usado de estos algoritmos es el “Data Encription Standard” (DES).

Para evitar los ataques, las Tarjetas Inteligentes utilizan el sistema Tecno-Hcmos, que consiste en guardar la información mediante cargas eléctricas en condensadores, que pueden albergarla hasta un periodo de diez años sin sufrir alteración alguna en las cargas eléctricas. Las Tarjetas Inteligentes también pueden llevar sistemas de autodestrucción con sensores que adviertan de una situación de peligro. Se envasan al vacío y cuando entra aire o se detecta la presencia de cualquier tipo de luz, el sistema se bloquea y se destruye la información.

A escala de software, también los sistemas criptográficos que defienden las claves de las tarjetas son susceptibles de agresiones sofisticadas. A pesar de que los algoritmos más utilizados (RSA, DES, Funciones HASH) han demostrado ser muy sólidos, podrían no serlo tanto las implementaciones físicas que se han realizado con ellos. Recientemente han aparecido los llamados ataques por criptoanálisis diferencial, que consisten básicamente en enfrentar dos tarjetas una nueva y otra que se ha sometido a una radiación local fuerte, de manera que quede alterada parte de la clave. Al comparar las salidas entre la buena y la mala se puede llegar a descifrar la clave por comparación. El remedio que han llegado a adoptar los fabricantes ante los mencionados ataques es relativamente sencillo: un sistema interno de detección de fallos que bloquea la salida de datos. Muchas de estas medidas de seguridad son secretas, y los fabricantes no acostumbran a hacerlas públicas.

IV. DESARROLLO DEL SISTEMA "AZUL y ORO"

IV.1 Análisis

Como se mencionó anteriormente, el objetivo principal de este trabajo es el ingresar a la Facultad de Ingeniería el concepto de Tarjeta Inteligente como medio de pago e identificación académica como aplicaciones base.

Para llevar acabo este objetivo es necesario diseñar e integrar un sistema mediante el cual se permite explotar la información contenida en las Tarjetas Inteligentes.

Este sistema deberá:

- Contener la infraestructura tecnológica centralizada necesaria para una correcta administración y operación de las credenciales. Esta infraestructura se enuncia a continuación de forma descriptiva más no limitativa:

1. Comunicaciones. Abarca todo lo concerniente a la forma de intercomunicar los equipos. (Medio de Enlace, Dispositivos de Control y Administración)
2. Site. Lugar físico en donde se encuentran los dispositivos de almacenamiento y de comunicación.
3. Terminales: Esta compuesta por el lector y la interfaz con la que interactúa la tarjeta, para una aplicación dada. El número de terminales dependerá de los requerimientos institucionales.
4. Distribución de Tarjetas: Es necesario contar con una entidad que se responsabilice de inventariar las credenciales, así como de también tener el control de la asignación y entrega de las mismas.

- Proporcionar integridad, confidencialidad y disponibilidad de la información en cada uno de los componentes que integran la solución (tarjetas, interfaces, terminales, etc.).
- Permitir la independencia de operabilidad para las aplicaciones que así lo requieran.
- Proveer una plataforma flexible para integrar cambios en cualquier momento sin mayores modificaciones a dicha aplicación.
- Brindar la posibilidad de realizar nuevas aplicaciones sobre la tarjeta, por mencionar algunos ejemplos:

  -Reloj Checador
  -Validación de Identificación mediante Datos Biomédicos
  -Control de Servicios Solicitados

De manera esquemática el sistema se representa en la *figura 4.1*:

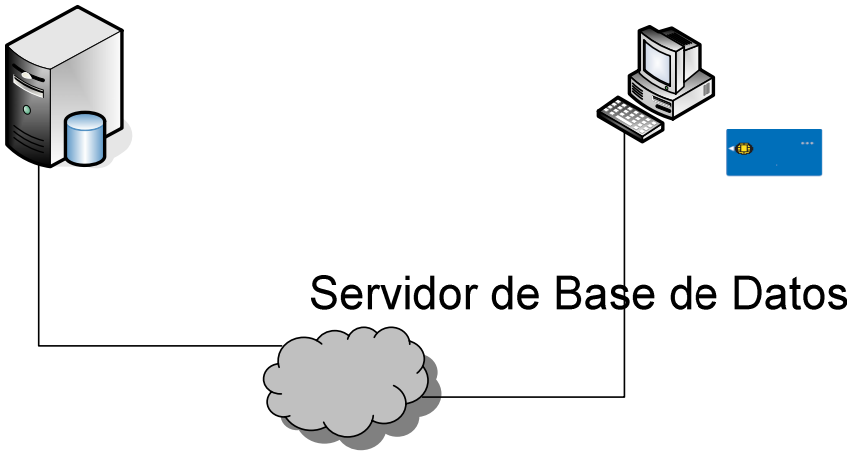


Figura 4.1 Sistema Azul y Oro

IV.2 Diseño

El sistema propuesto contempla la implementación de dos aplicaciones base: monedero PUMA e identiFI.

Monedero PUMA: Es un monedero electrónico que permitirá al estudiante realizar los pagos de servicios que requiera durante su permanencia en la Facultad de Ingeniería, y que contempla a su vez, el uso de una aplicación de lealtad con la cual se fomentaría el uso de este medio de pago.

Monedero PUMA realizará 2 tipos de Transacciones básicamente:

- COMPRA: Esta transacción consiste en debitar de la tarjeta un monto dado a cambio de la obtención de un servicio.

Red U

- RECARGA: Esta transacción consiste en aumentar el saldo de una tarjeta en función del monto en efectivo dado por el usuario al operador de la aplicación.

- ACTUALIZACIÓN DE PARÁMETROS: Esta transacción consiste en realizar la actualización de datos, tanto en la tarjeta como en la base de datos.

***identiFI*:** Es una aplicación en la cual se tienen los datos personales y académicos del alumno como lo es el nombre, plantel, carrera, materias en curso, etc.

Como se mencionó en el capítulo I para llevar a cabo una solución de este tipo es necesario desarrollar e integrar 3 entidades de manera global:

-TARJETA.

- Selección de Tarjeta
- Definición de Datos
- Mapeo del Chip
- Definición de Llaves
- Diseño de Impresión
- Personalización Gráfica y Eléctrica

-INTERFAZ

- Diseño de Interfaz
- Definición de Módulos
- Diagrama de Flujo
- Implementación

-SISTEMA CENTRAL

- Definición de Base de Datos

- Diagrama Entidad-Relación
- Medios de Comunicación
- Implementación

El sistema AZUL y ORO estará entonces conformado por una terminal (PC y lector de tarjeta) la cual se comunica con la base de datos central, y será capaz por un lado, de proporcionar un medio de pago confiable, del cual, se permita utilizar la información generada para llevar acabo análisis estadísticos en pro de mejorar los servicios; y por otro, disponer de la información académica de los alumnos.

El sistema en su totalidad será capaz de obtener cualquiera de los datos de la tarjeta para ser procesada por la aplicación Azul y Oro, o bien para ser almacenada en la base de datos, la *figura 4.2* muestra la base de datos prototipo diseñada para este sistema.

Para no minar la seguridad que proporcionan las tarjetas inteligentes es necesario mantener el control de la información en los diferentes puntos de acceso a ésta por lo cual es necesario plantear un esquema de seguridad para el control de usuarios tanto en la base de datos como en las diferentes interfaces que componen el sistema, estos esquemas se salen del alcance de este documento.

IV.2.1 Base de Datos

La base de datos contiene la información necesaria para la correcta administración de las tarjetas, así como también historiales que permiten evaluar el correcto funcionamiento de las aplicaciones. En base a esta información es posible desarrollar nuevas aplicaciones que den solución a nuevos problemas o requerimientos institucionales.
Es necesario hacer mención que no todas las aplicaciones (hablando de aplicaciones futuras) deberán necesariamente registrar una transacción contra el

sistema central, es decir dependerá de los requerimientos para los cuales haya sido construida dicha aplicación. Este concepto se conoce como transacciones fuera de línea, o bien se puede pensar en transacciones condicionadas, es decir, sólo se realiza una comunicación contra el sistema cuando se cumplen ciertos criterios establecidos.

La base de datos quedó definida de la siguiente manera, tal como lo muestra la *figura 4.2.1*

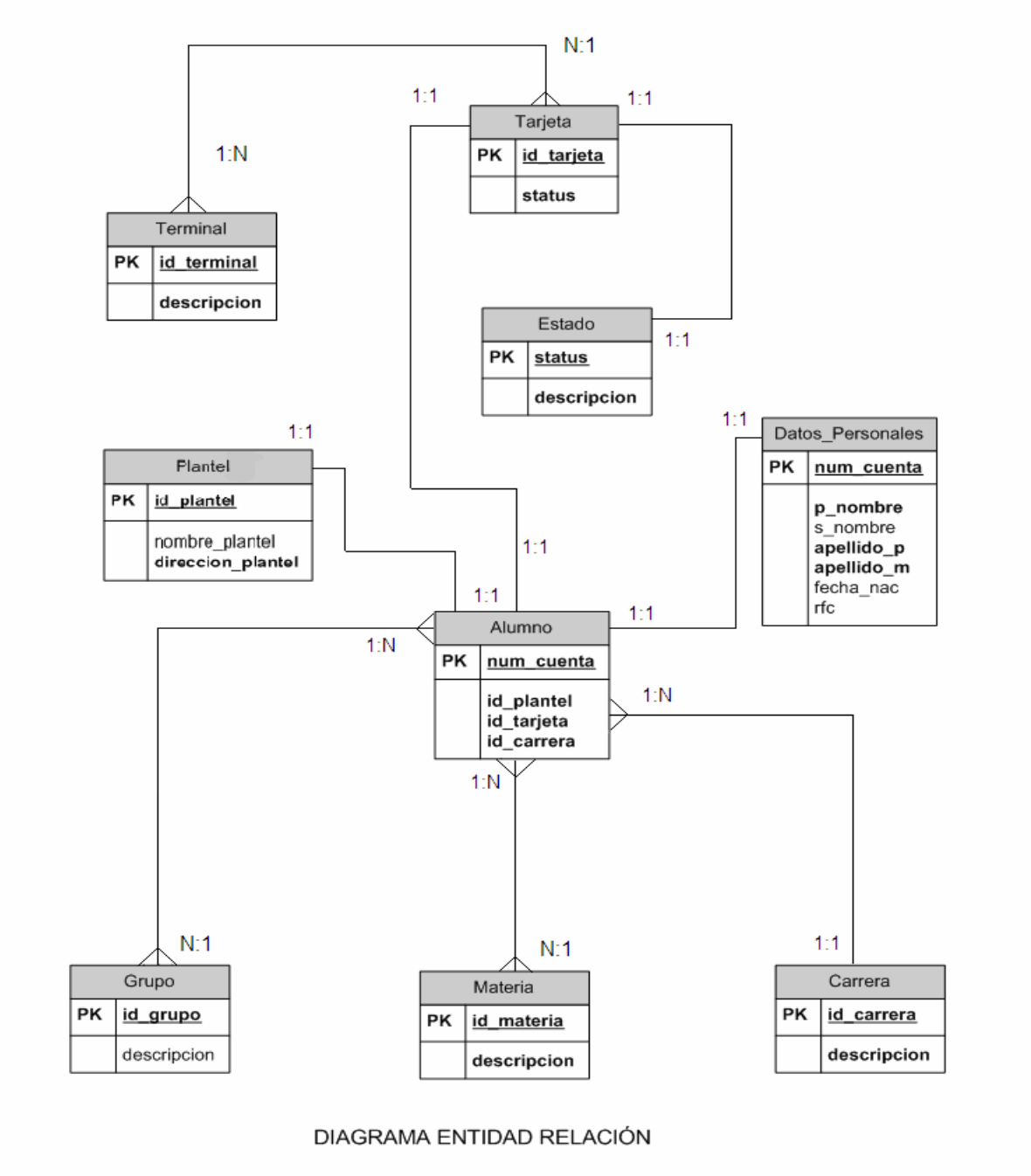


Figura 4.2.1 Base de Datos no normalizada, prototipo del sistema Azul y Oro

Normalizando la base de datos, finalmente queda definida de la siguiente manera, *figura 4.2.2*

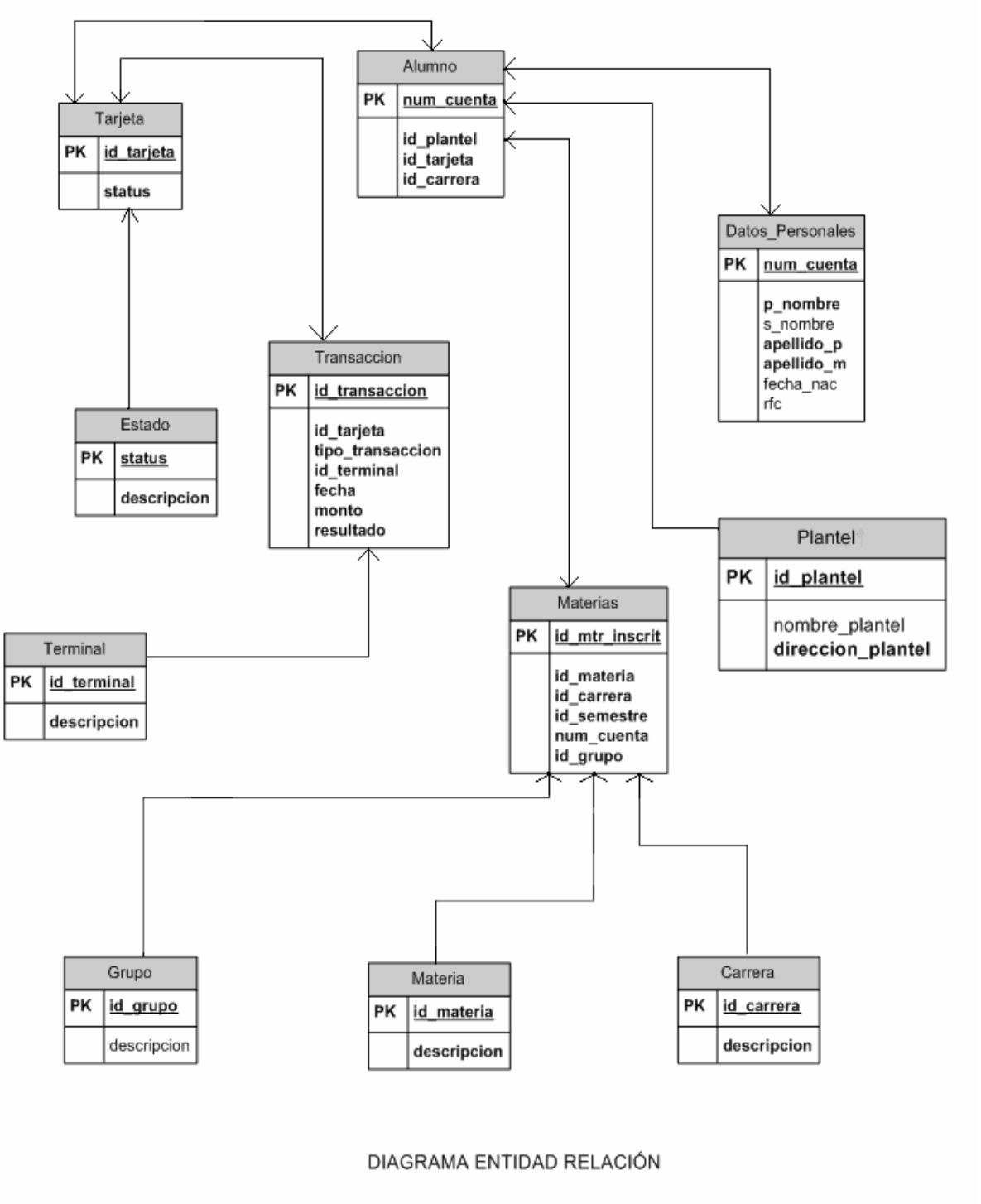


Figura 4.2.2 Base de Datos prototipo del sistema Azul y Oro, normalizada de primer nivel.

Diccionario de datos en la base de datos:

Nombre de la Tabla: Alumno		
Campo	Tipo	Descripción
num_cuenta	Varchar (9)	número de cuenta del alumno
Id_plantel	Char (2)	identificador del plantel donde esta inscrito el alumno
Id_tarjeta	Char (10)	identificador del número de tarjeta asociada al alumno
Id_carrera	Char (4)	identificador de la carrera donde se encuentra inscrito el alumno

Nombre de la Tabla: Tarjeta		
Campo	Tipo	Descripción
Id_tarjeta	Char (10)	identificador del número de tarjeta asociada al alumno
status	Char (6)	estado último de la tarjeta, pueden existir 5 posibles estados

Nombre de la Tabla: Transaccion		
Campo	Tipo	Descripción
Id_transaccion	Varchar (10)	identificador de la transacción realizada, es decir, se asigna un folio de transacción.
tipo_transaccion	Char (10)	se refiere a si la transacción es compra o recarga
Id_tarjeta	Char (10)	identificador del número de tarjeta asociada al alumno
Id_terminal	Char (10)	identificador de la terminal en donde fue realizada la transacción
fecha	datetime	Fecha con formato YYYY/MM/DD HH:MM:SS de la transacción realizada

monto	Char (10)	Monto de la cantidad debitada o abonada
resultado	Char (10)	Resultado satisfactorio o fallido de la transacción

Nombre de la Tabla: Estado		
Campo	Tipo	Descripción
status	Char (6)	estado último de la tarjeta, pueden existir 7 posibles estados
descripcion	Char (20)	Se tienen 5 posibles estados: bloqueo, suspensión, robada, ok, dañada.

Nombre de la Tabla: Terminal		
Campo	Tipo	Descripción
Id_terminal	Char (10)	identificador de la terminal en donde fue realizada la transacción
descripcion	Varchar (40)	Ubicación de la terminal, lugar donde se encuentra la Terminal

Nombre de la Tabla: Datos Personales		
Campo	Tipo	Descripción
Num_cuenta	Char (9)	número de cuenta del alumno
P_nombre	Char(10)	Primer nombre del alumno
S_nombre	Char(10)	Segundo nombre del alumno
Apellido_p	Char (20)	Apellido paterno del alumno
Apellido_m	Char (20)	Apellido materno del alumno
Fecha_nac	Varchar(10)	Fecha de nacimiento del alumno, formato: YYYY/MM/DD
rfc	Varchar(10)	RFC del alumno

Nombre de la Tabla: Materias		
Campo	Tipo	Descripción
Id_mtr_inscrit	Varchar (10)	identificador de la materia inscrita
num_cuenta	Varchar (9)	número de cuenta del alumno
Id_materia	Char (4)	identificador de la materia inscrita del alumno
Id_carrera	Char (4)	identificador de la carrera donde se encuentra inscrito el alumno
Id_semestre	Char (4)	identificador de la semestre inscrito del alumno
Id_grupo	Char (4)	identificador del grupo en la materia inscrita del alumno

Nombre de la Tabla: Materia		
Campo	Tipo	Descripción
Id_materia	Char (4)	identificador de la materia inscrita del alumno
descripcion	Varchar (20)	Nombre de la materia

Nombre de la Tabla: Carrera		
Campo	Tipo	Descripción
Id_carrera	Char (4)	identificador de la carrera donde se encuentra inscrito el alumno
descripcion	Varchar (20)	Nombre de la carrera

Nombre de la Tabla: Plantel		
Campo	Tipo	Descripción
Id_plantel	Char (4)	identificador del plantel donde se encuentra inscrito el alumno
Nombre_plantel	Varchar (20)	Nombre del plantel
direccion	Varchar (40)	Ubicación de plantel

Nombre de la Tabla: Grupo		
Campo	Tipo	Descripción
Id_grupo	Char (10)	identificador del grupo en la materia inscrita del alumno
descripcion	Varchar (40)	Nombre del grupo

IV.2.2 Tarjeta

La tarjeta utilizada para este proyecto tiene las siguientes características:

-Chip con 8Kb de memoria

-Tarjeta PVC

Dimensiones:

-tarjeta tipo id-1.

-ancho: 85.60 mm +- 0.76 mm (3.370 in +-0.03 in).

-alto: 53.98 mm +- 0.76 mm (2.125 in +-0.03 in).

-espesor: 0.76 mm +- 0.08 mm (0.030 in +- 0.003 in).

-esquinas redondeadas de un radio de 3.18 mm +- 0.30mm (0.125 in +- 0.012 in)

Definición de Datos:

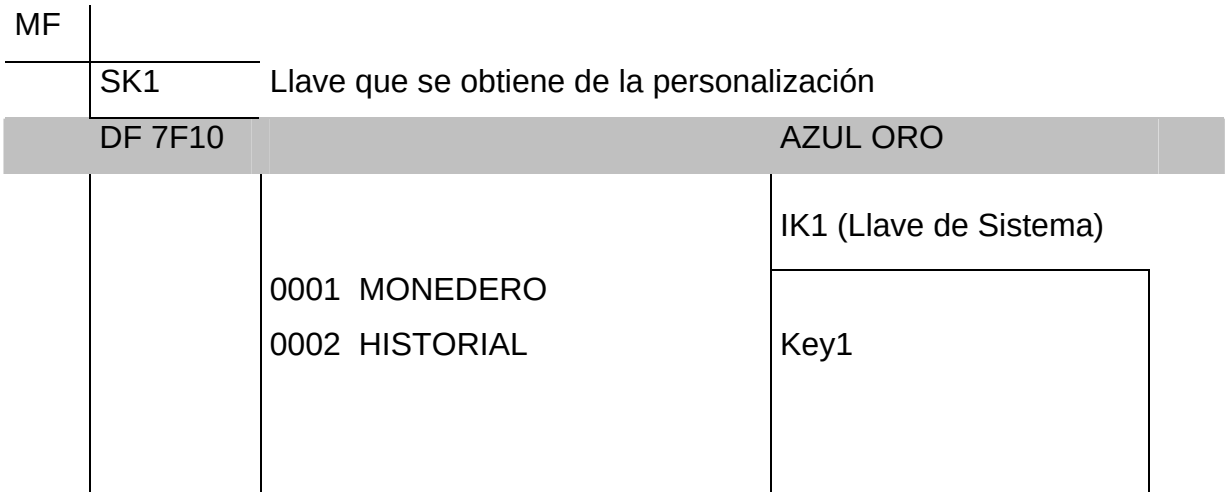
La información contenida en la Tarjeta Inteligente esta conformada por datos que deben ser almacenados de una manera estructurada para su correcta interpretación, es por eso que al definir los datos se tienen que contemplar aspectos tales como: optimización de recursos, longitudes, tipo de codificación, permisos de acceso, etc. Cabe mencionar que se tiene que almacenar toda la información que se requiere para el correcto funcionamiento de la aplicación. En la *tabla 4.1* se encuentran la definición de los datos de la tarjeta.

CAMPO	LONGITUD	SINTAXIS
NOMBRE	60 BYTES	A ∈ [0 ; 128 ASCII CODE]
NÚMERO DE CUENTA	5 Bytes	“NNNNNNNNN” N ∈ [0 ; 9] Eje(1) 095196626 CORRESPONDENCIA HEX(nc) 303935313936363236
PLANTEL	1 BYTE	“NN” NN ∈ [00 ; 99]
CARRERA	2 BYTES	“NNNN” NNNN ∈ [0000 ; 9999]
MATERIAS	28 BYTES	“NNNNNGG” N ∈ [00000000 ; 9999999] GG ∈ [00 ; 99] DONDE GG INDICA EL GRUPO DONDE ESTA INSCRITO
SEMESTRE INSCRITO	3 BYTES	YYYYSS 200602 YYYY ∈ [0000 ; 9999] SS [00 ; 99]
AÑO DE INGRESO	3 BYTES	YYYYSS 200602 YYYY ∈ [0000 ; 9999] SS [00 ; 99]
FECHA DE ÚLTIMA ACTUALIZACIÓN	4 BYTES	
BANDERAS DE CONTROL	3 BYTES	NNNNNN N ∈ [000000;999999]

MÁXIMO EN MONEDERO	3 BYTES	HHHHHH H ∈[0 ; F] ESTAS UNIDADES ESTAN DADAS EN CENTAVOS
SALDO	2 BYTES	NNNN
NIP	2 BYTES	NNNN N ∈ [0000:9999]
PUNTOS PARA LEALTAD	3 BYTES	HHHHHH H ∈ [O - F]
FECHA DE EXPIRACIÓN	3 BYTES	BCD
INTENTOS DE NIP	1 BYTE	BCD
LABORATORIOS	28 BYTES	NNNNNGG” N ∈ [00000000 ; 9999999] GG ∈ [00 ; 99] DONDE GG INDICA EL GRUPO DONDE ESTA INSCRITO

Tabla 4.1 Definición de los datos en la Tarjeta Inteligente

La estructura de la tarjeta se representa en la *tabla 4.2*



MAPPING

		Size (bytes)
MF		
DF azul y oro		38
	ISF	8
	IK 1 VALE (Llave de sistema)	24
	KEY 1 VALE	24
	Subtotal Llaves Aplicación	72
	Archivo de Trabajo EF1 0001 MONDERO Derechos de Acceso: Read = Libre, W/U = Key1	18
	Archivo de Trabajo EF2 0002 HISTORIAL Derechos de Acceso: Read = Libre, W/U = Key1	130
	Subtotal EF's	148
Total :	220	

Tabla 4.2 Estructura de la Tarjeta

En el chip de la Tarjeta Inteligente se encuentra definida la siguiente información:

-*Nombre*: 60 BYTES (20,20,20) ASCII
-*Número de cuenta* 5 BYTES (Identificador de la tarjeta) BCD-Plantel: 1 BYTE BCD
-*Carrera*: 2 BYTES BCD
-*Materias*: 28 Bytes (7 Campos de 4 Bytes) BCD en el 4 byte se encuentra el grupo

-*Semestre Inscrito*: 3 BYTES BCD

-*Año de Ingreso*: 3 BYTES BCD

-*Fecha de última actualización:* 4 BYTES BCD

-*Banderas de control:* 3 BYTES

-*Máximo en Monedero:* 3 BYTES HEXA

-*Saldo:* 2 BYTES HEXA

-*NIP*: 2 BYTES

-*Puntos para lealtad*: 3 BYTES HEXA

-*Fecha de Expiración:3 BYTES BCD*

- *Intentos de NIP*: 1 BYTE BCD

-*L*aboratorios: 28 BYTES (7 campos de 4 bytes) BCD en el 4 byte se encuentra el grupo

Esta anterior información queda representada en un mapeo tal como se muestra en la *tabla 4.3*

	BYTE 1	BYTE 2	BYTE 3	BYTE 4
0	NOMBRE	NOMBRE	NOMBRE	NOMBRE
1	NOMBRE	NOMBRE	NOMBRE	NOMBRE
2	NOMBRE	NOMBRE	NOMBRE	NOMBRE
3	NOMBRE	NOMBRE	NOMBRE	NOMBRE
4	NOMBRE	NOMBRE	NOMBRE	NOMBRE
5	APELLIDO	APELLIDO	APELLIDO	APELLIDO
6	APELLIDO	APELLIDO	APELLIDO	APELLIDO
7	APELLIDO	APELLIDO	APELLIDO	APELLIDO
8	APELLIDO	APELLIDO	APELLIDO	APELLIDO
9	APELLIDO	APELLIDO	APELLIDO	APELLIDO
10	APELLIDOM	APELLIDOM	APELLIDOM	APELLIDOM
11	APELLIDOM	APELLIDOM	APELLIDOM	APELLIDOM
12	APELLIDOM	APELLIDOM	APELLIDOM	APELLIDOM
13	APELLIDOM	APELLIDOM	APELLIDOM	APELLIDOM
14	APELLIDOM	APELLIDOM	APELLIDOM	APELLIDOM
15	NÚMERO DE	NÚMERO DE	NÚMERO DE	NÚMERO DE

	CUENTA	CUENTA	CUENTA	CUENTA
16	NUMERODECUENTA	PLANTEL	CARRERA	CARRERA
17	MATERIAS	MATERIAS	MATERIAS	GRUPO01
18	MATERIAS	MATERIAS	MATERIAS	GRUPO02
19	MATERIAS	MATERIAS	MATERIAS	GRUPO03
20	MATERIAS	MATERIAS	MATERIAS	GRUPO04
21	MATERIAS	MATERIAS	MATERIAS	GRUPO05
22	MATERIAS	MATERIAS	MATERIAS	GRUPO06
23	MATERIAS	MATERIAS	MATERIAS	GRUPO07
24	SEMESTRE	SEMESTRE	SEMESTRE	AÑO INGRESO
25	AÑO INGRESO	AÑO INGRESO	FECHA ÚLTIMA ACTUALIZACIÓN	FECHA ÚLTIMA ACTUALIZACIÓN
26	FECHA ÚLTIMA ACTUALIZACIÓN	FECHA ÚLTIMA ACTUALIZACIÓN	BANDERAS	BANDERAS
27	BANDERAS	MÁXIMO EN MONEDERO	MÁXIMO EN MONEDERO	MÁXIMO EN MONEDERO
28	SALDO	SALDO	NIP	NIP
29	PUNTOS PARA LEALTAD	PUNTOS PARA LEALTAD	PUNTOS PARA LEALTAD	FECHA DE EXPIRACIÓN
30	FECHA DE EXPIRACIÓN	FECHA DE EXPIRACIÓN	INTENTOS DE NIP	RFU
31	LAB01	LAB01	LAB01	LABGPO01
32	LAB02	LAB02	LAB02	LABGPO02
33	LAB03	LAB03	LAB03	LABGPO03
34	LAB04	LAB04	LAB04	LABGPO04
35	LAB05	LAB05	LAB05	LABGPO05
36	LAB06	LAB06	LAB06	LABGPO06
37	LAB07	LAB07	LAB07	LABGPO07

Tabla 4.3 Mapeo en bytes

IV.2.3 Diccionario de datos de la aplicación

Usuario Cliente: Persona que interactúa con la aplicación que se haya generado, en el caso de la aplicación monedero PUMA, aceptará la transacción recarga o compra a realizar.

Usuario Cardholder. Este usuario es el propietario de la tarjeta, en él recaerá la responsabilidad del uso de la tarjeta.

Administrador del Sistema. Este usuario tendrá privilegios de administrador y tendrá acceso a la base de datos para realizar cambios, modificar aplicaciones en la tarjeta o generar nuevas aplicaciones.

Oficial de Seguridad. Este elemento va a tener la información de la tarjeta en cuanto a las diferentes llaves que se manejen en la misma.

Recarga. Proceso de acreditar el balance de la tarjeta.

Terminal. Dispositivo o conjunto de dispositivos en donde se inserta la tarjeta para su acceso.

Monedero PUMA. Monedero Electrónico para uso interno de la Facultad de Ingeniería.

IdentiFI. Aplicación contenida en el sistema AZUL y ORO, que contiene los datos del alumnado de la Facultad de Ingeniería.

APELLIDOM: Apellido materno del Usuario Cardholder

ATR (Answer to Reset). Primera respuesta de la tarjeta al ser energizada.

IV.2.4 Interfaz

La *figura 4.3* muestra el Proceso Recarga-Usuario.

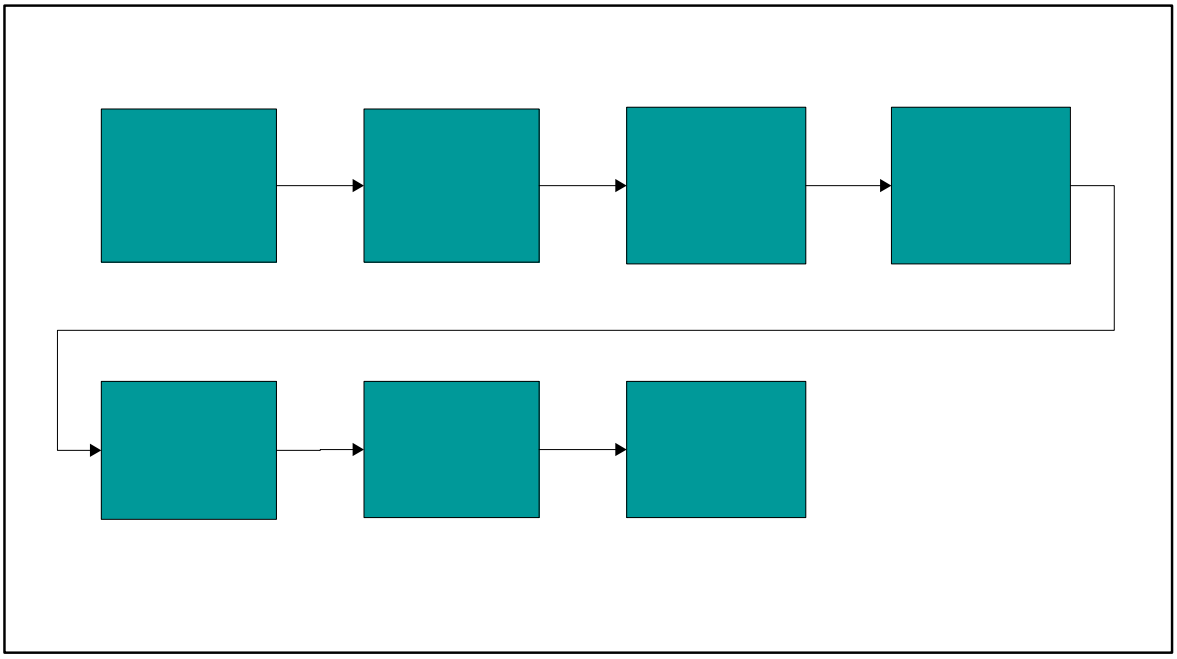
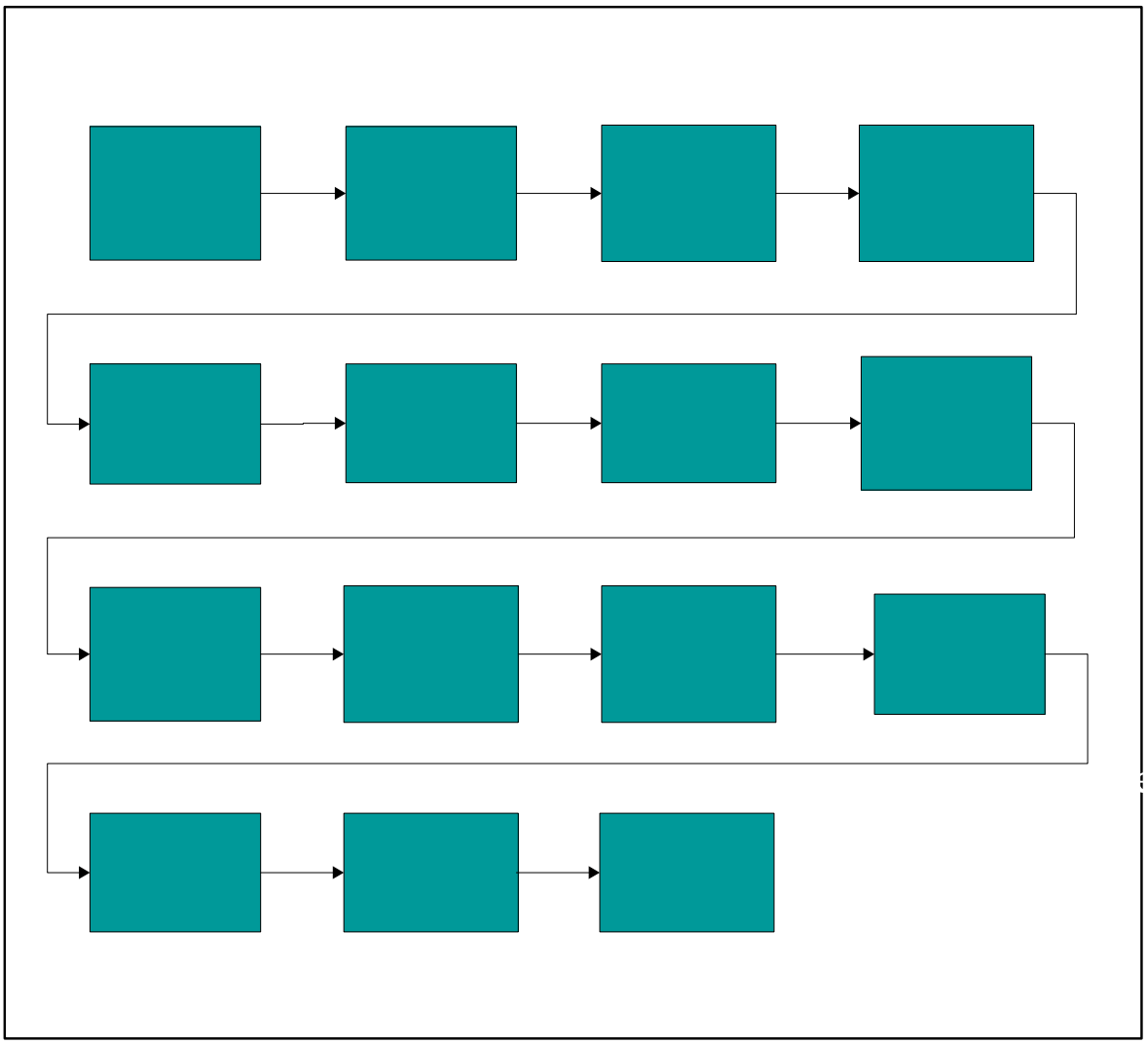
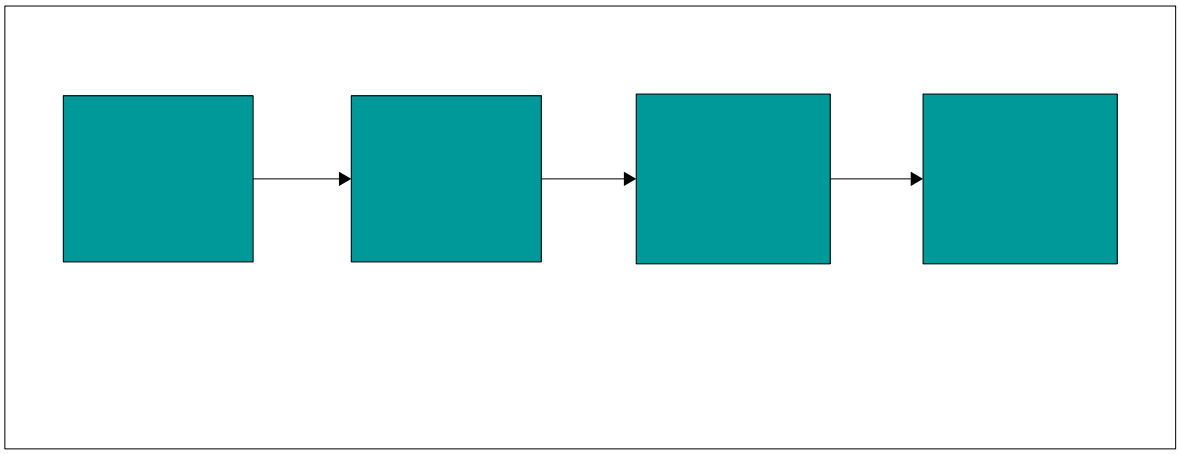


Figura 4.3 Proceso

La *figura 4.4* muestra el Diseño de Interfaz Recarga



La *figura 4.5* muestra el Proceso de Generación de Tarjetas



La *figura 4.6* muestra el Diseño de Interfaz Genera Tarjeta

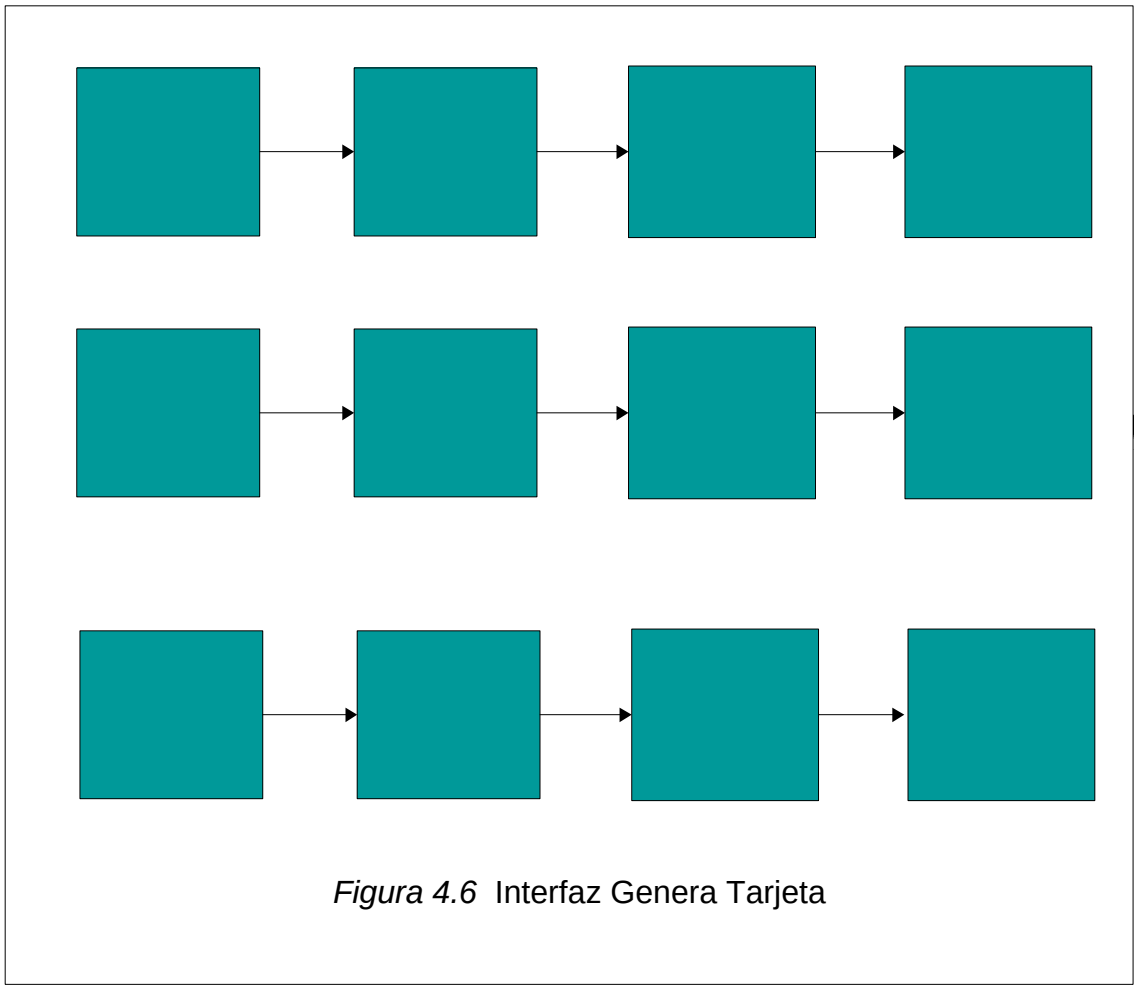


Figura 4.6 Interfaz Genera Tarjeta

4.5 . Pr
de

La *figura 4.7* muestra el Diseño Recarga DB-Cliente

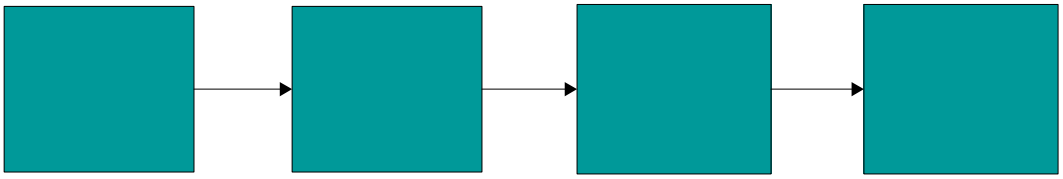


Figura 4.7 Recarga en Base de Datos-Cliente

En cada estado se tiene que verificar la respuesta de la tarjeta. Esta respuesta esta definida en el ISO 7816.

Durante el transcurso de las operaciones pueden ocurrir errores asociados a la tarjeta como pueden ser de escritura, falla en el voltaje, remoción anticipada pero también existen otro tipo de errores ajenos a la interfaz con la tarjeta como puede ser de comunicaciones, almacenamiento de datos, etc. Es por ello que es necesario tener el control, clasificarlos, informar al usuario y guardar en el sistema la información generada.

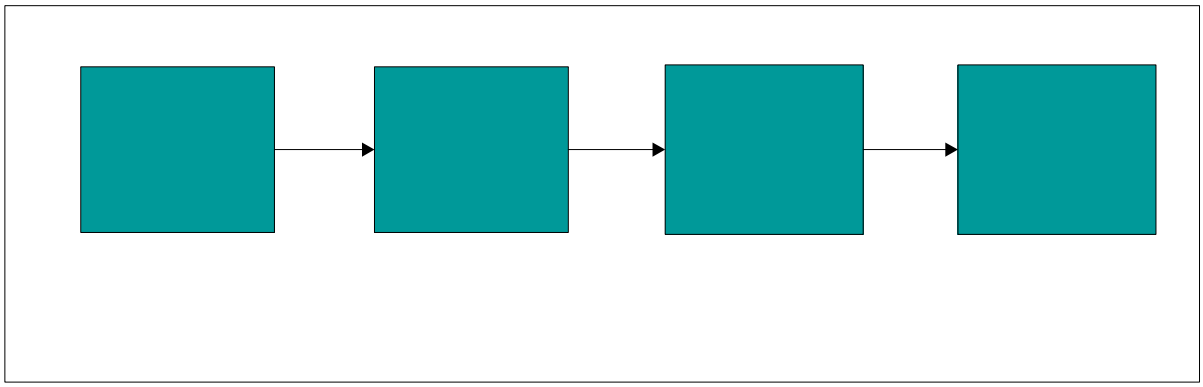
Figura 5.7 Rec
Datos-

De acuerdo a los conceptos de Ingeniería de Software podríamos comprender la recarga como un SERVICIO y por ende debe cumplir con los siguientes requisitos:

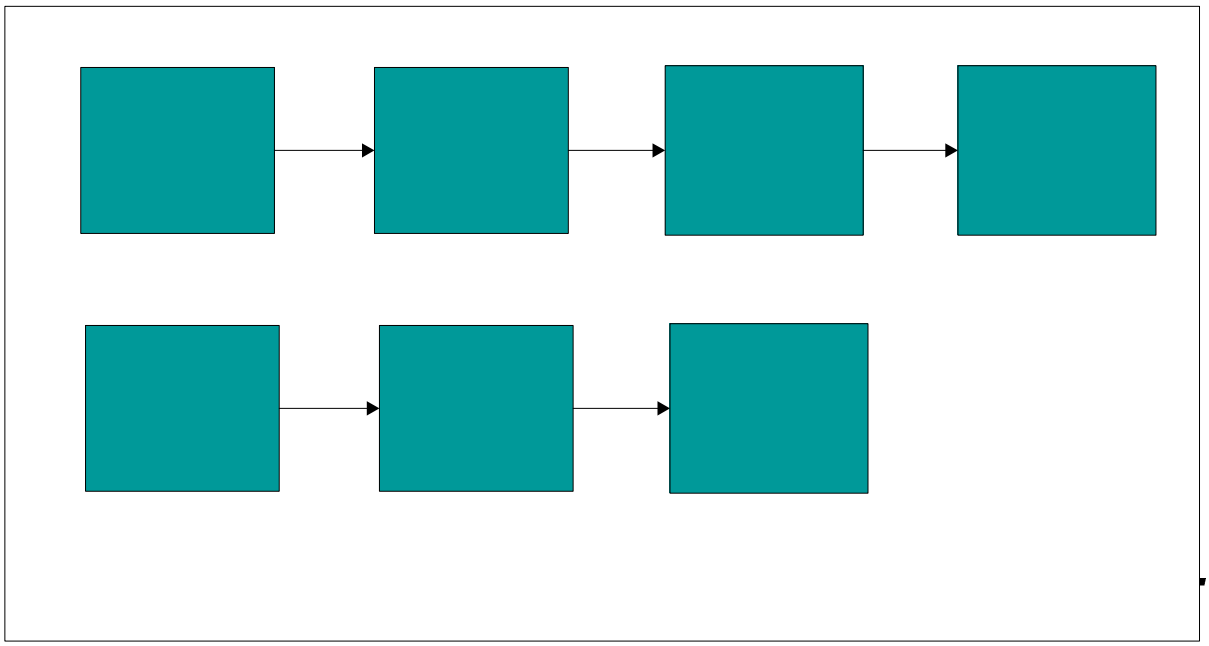
Ser seguro, lo que equivale a un uso correcto y con autorización
Ser válido, qué tareas o reglas se pueden aplicar
Manejar excepciones, informando al cliente
Contar con un catálogo de servicios que constituye un repositorio de servicios.

Diseño de Compra

La *figura 4.8* muestra el Proceso de Compra (TarjetaHabiente-Usuario Cliente).



La *figura 4.9* muestra el Diseño de Interfaz Compra (Usuario Cliente-Tarjeta).



.8 Pro

Es importante resaltar que se manejan dos conceptos importantes en la forma de transaccionar:

1. EN LÍNEA: La terminal realiza una comunicación hacia el sistema central Para verificar estados o actualizar parámetros.(recarga)

2. FUERA DE LÍNEA: La terminal no requiere de hacer una transacción al sistema ya que los datos no requieren de una comparación o actualización. (compra)

En un ambiente de producción, el tipo de transacción es definido por las reglas de negocio que imperen para un producto en particular.

IV.3 Construcción

Diagramas de Flujo

A continuación se muestran los diagramas de flujo de los dos procesos más importantes que realiza la Tarjeta Inteligente; el flujo de datos del proceso de Recarga-Cliente, el cual se encarga de realizar la parte de recarga en la tarjeta por un usuario; y el flujo de datos del proceso Compra-Cliente, este proceso es el que se encarga de validar cada compra realizada por el usuario, así como de validar la integridad de la cantidad a debitar y de revisar las banderas de control antes de pasar la transacción.

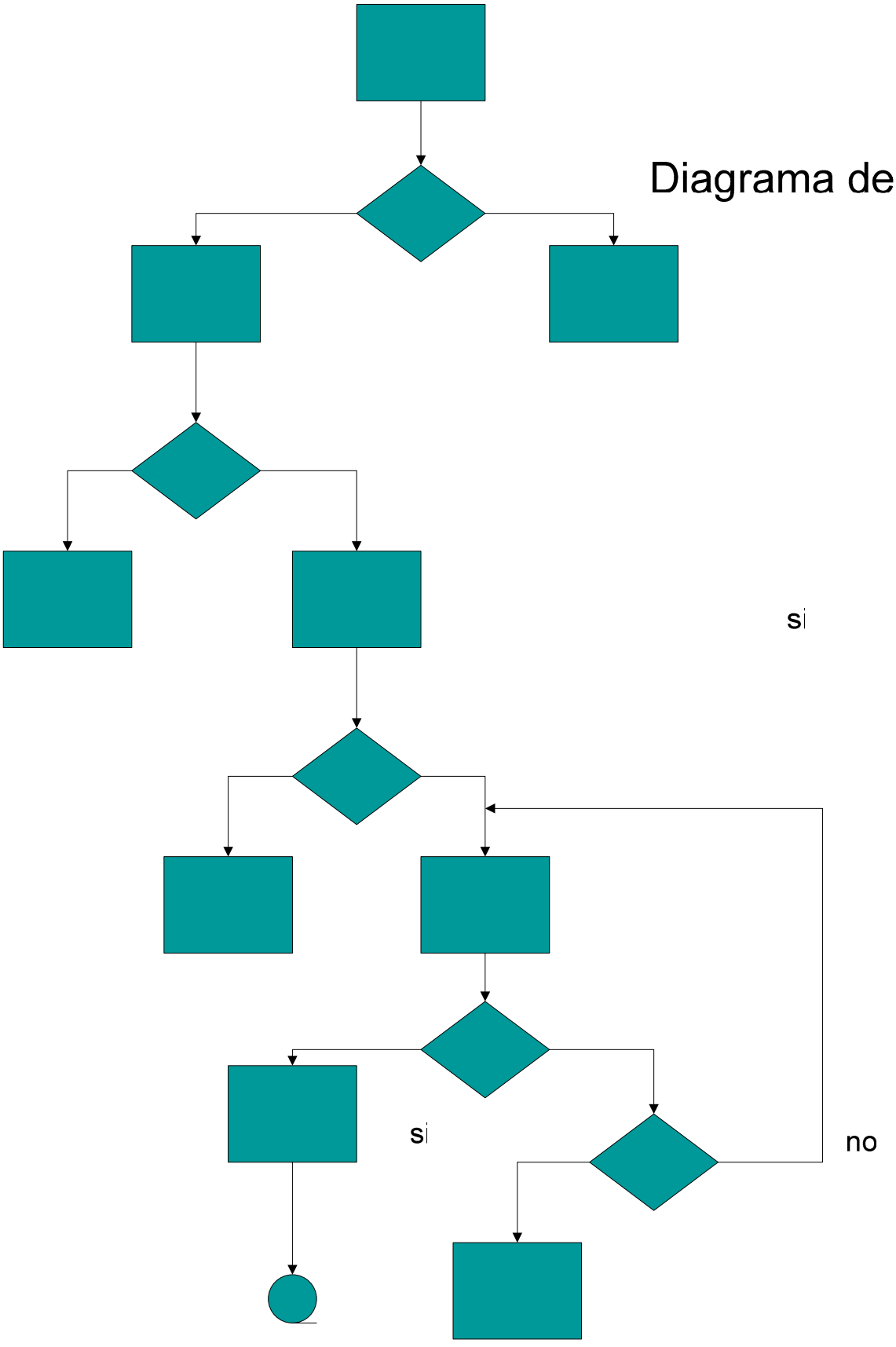
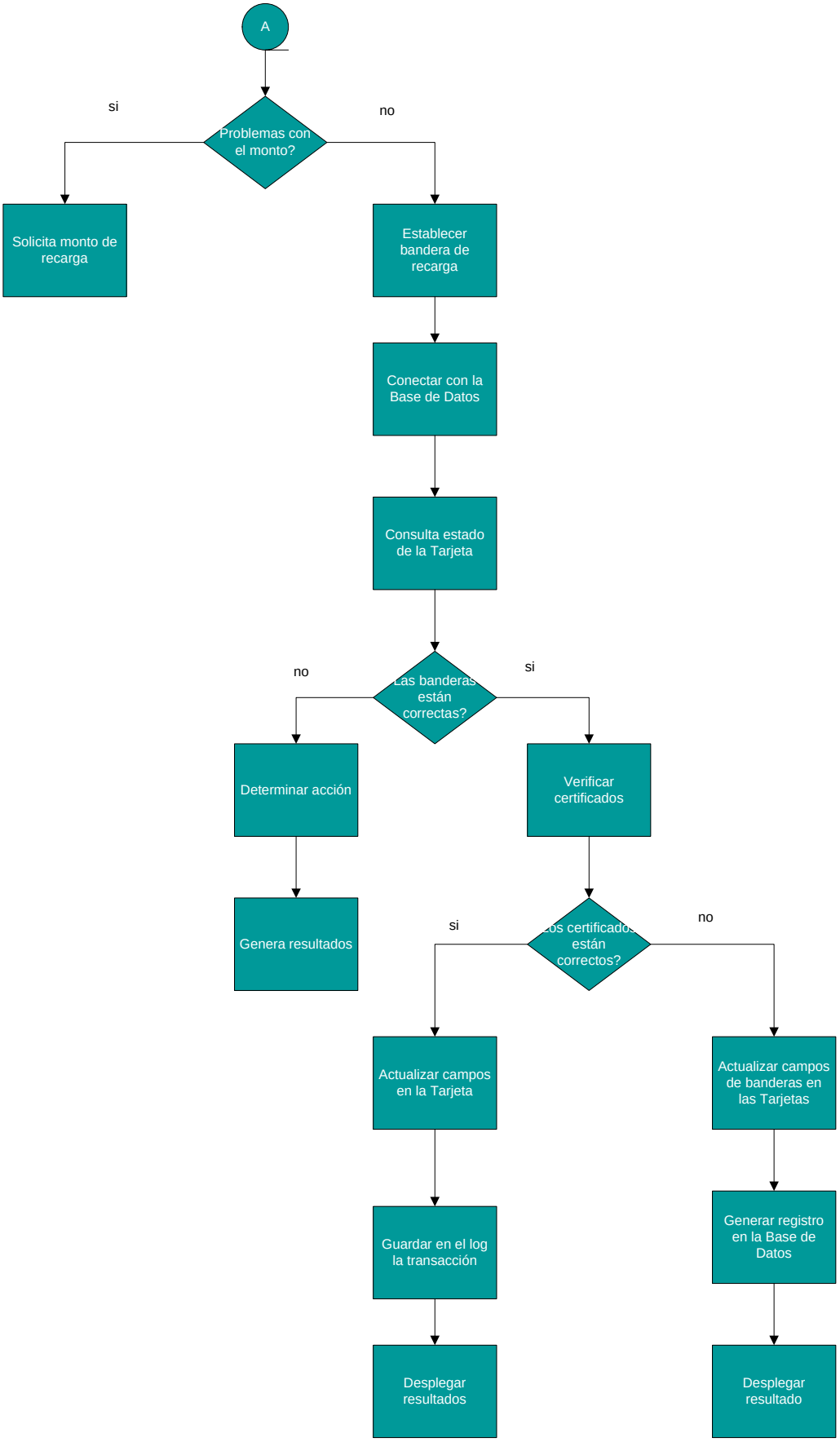


Diagrama de Fluj
si
si
no


A
Problemas con el monto?
si
no
Solicita monto de recarga
Establecer bandera de recarga
Conectar con la Base de Datos
Consulta estado de la Tarjeta
Las banderas están correctas?
no
si
Determinar acción
Verificar certificados
Genera resultados
Los certificados están correctos?
si
no
Actualizar campos en la Tarjeta
Actualizar campos de banderas en las Tarjetas
Guardar en el log la transacción
Generar registro en la Base de Datos
Desplegar resultados
Desplegar resultado

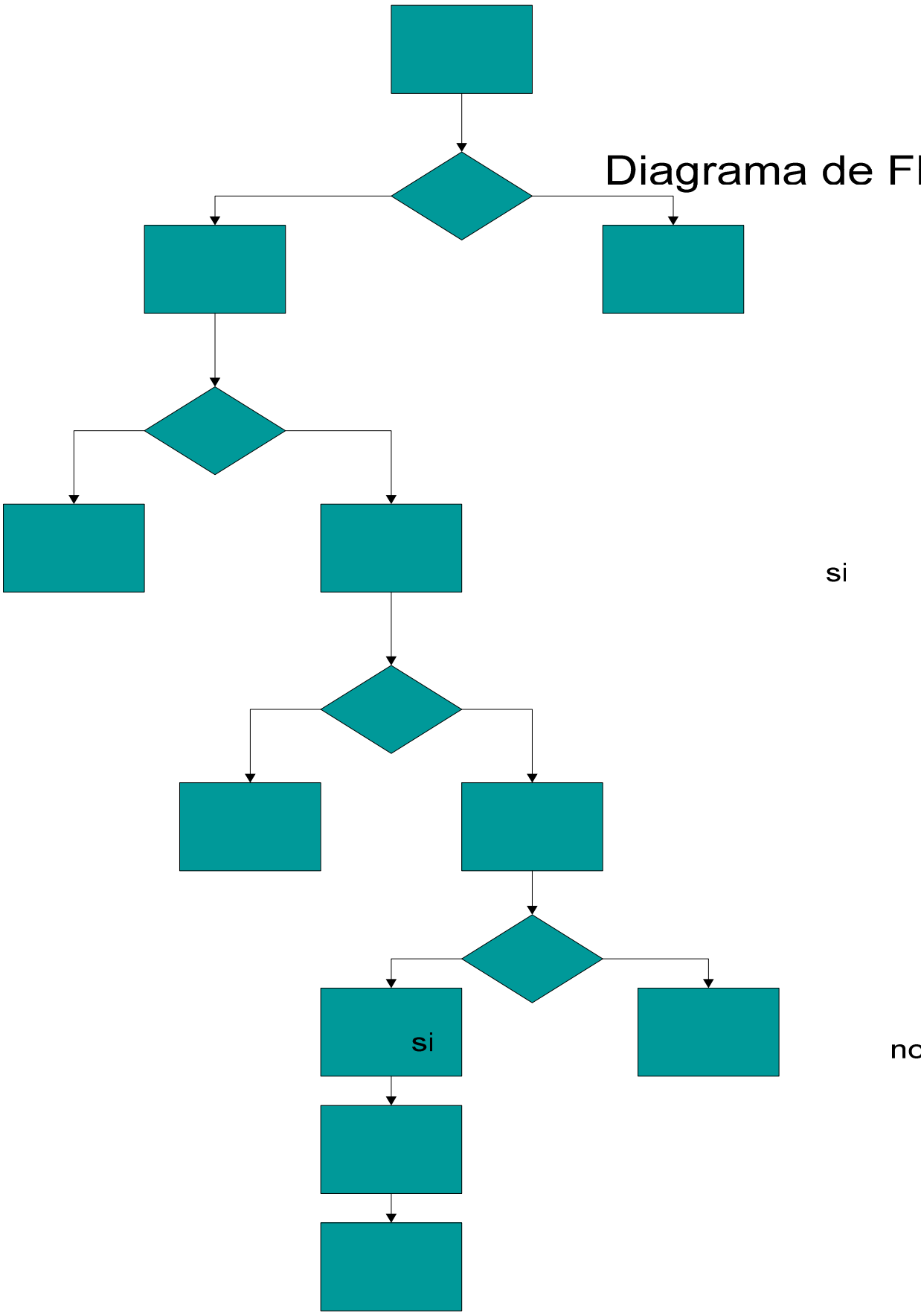
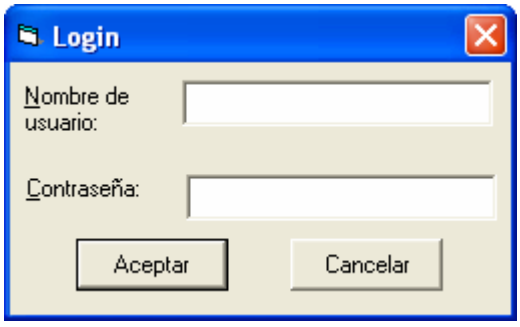


Diagrama de Fl
si
si
no

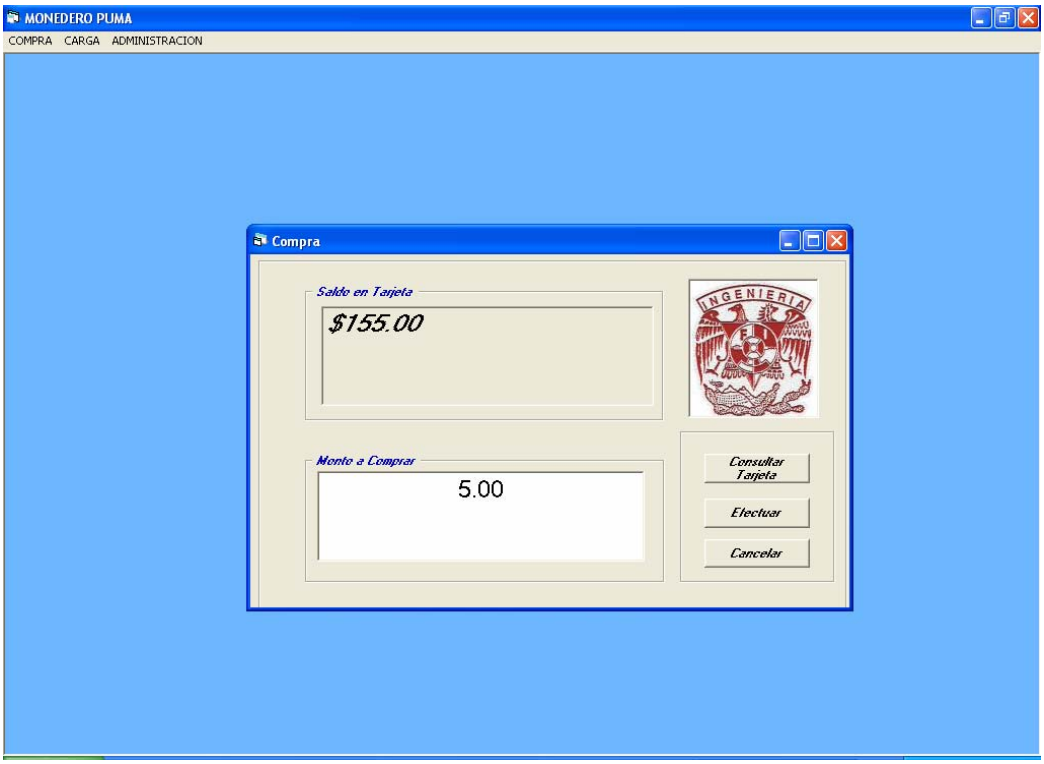
IV.4 Presentación

Entrada al sistema:

Las funciones que permite realizar la interfaz dependen del usuario que se registre y los permisos que hayan sido asignados a éste.



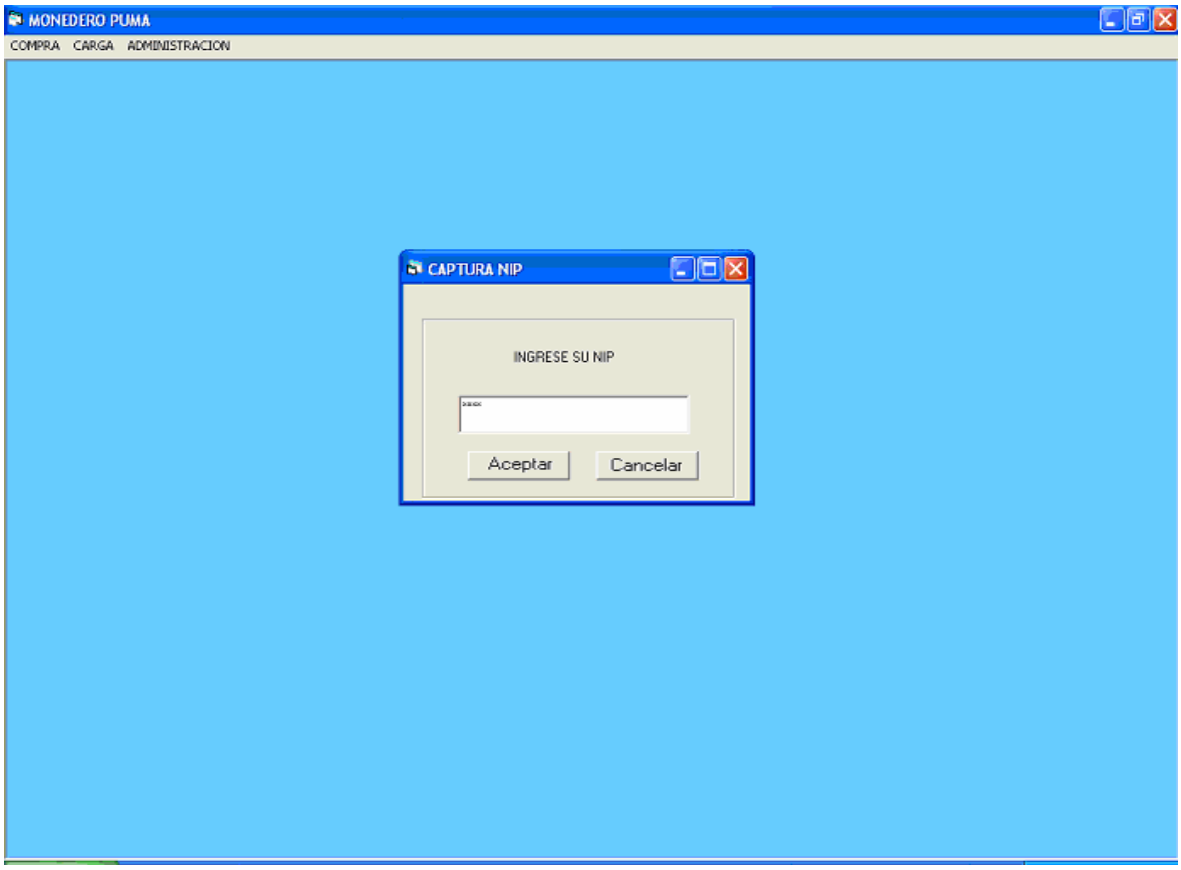
Proceso de Compra:



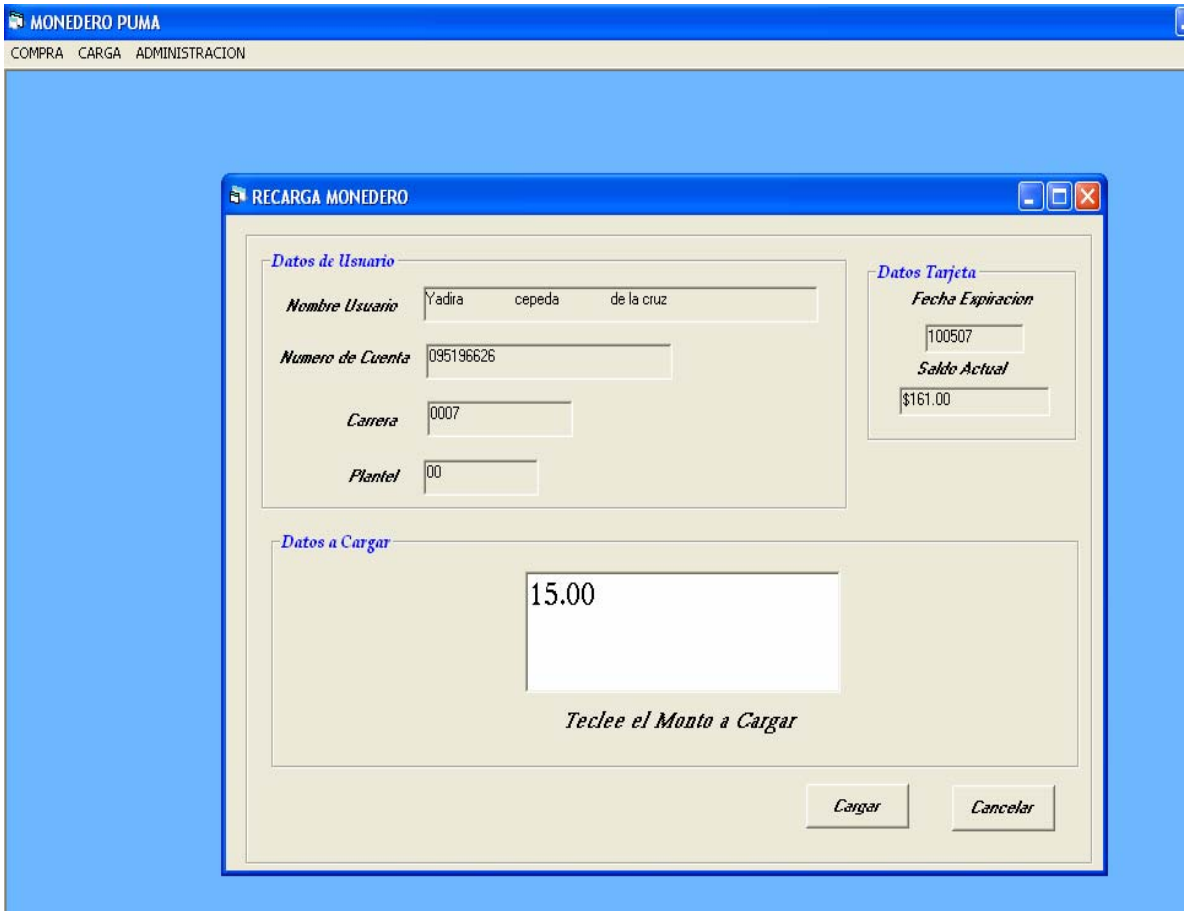
- Se consulta el saldo en la tarjeta y éste es desplegado
- Se ingresa el monto de la compra
- La tarjeta es debitada

Proceso de Recarga:

- El usuario Cardholder debe ingresar el NIP de su tarjeta
- Se realizan todas las validaciones



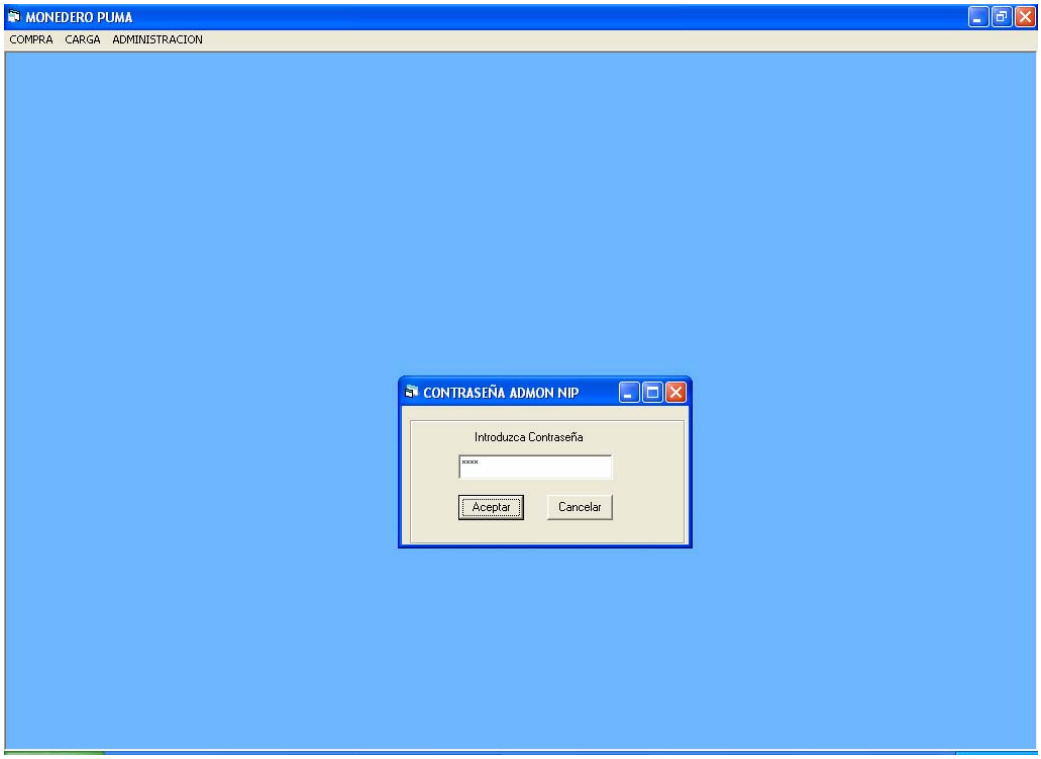
- Si es correcto se permite ingresar la carga
- Se despliegan los datos que se tienen en la tarjeta
- Se solicita ingresar el monto
- La tarjeta es acreditada con el monto



Proceso de Administración:

Para mantener el control de los permisos en la aplicación es necesario tener dos rubros en el proceso de administración:

- Administración de NIP



- Administración de Tarjetas

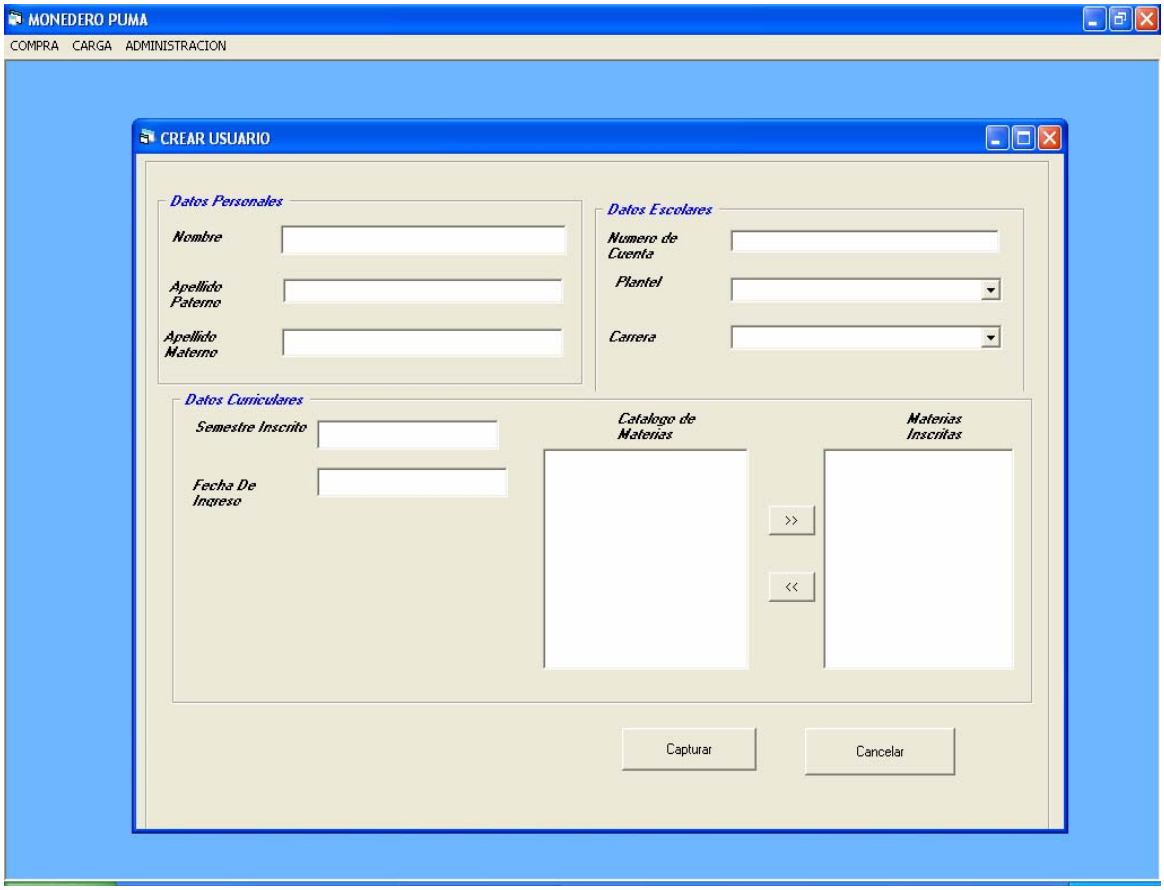
1. Creación de Usuarios: Se da de alta en la base de datos un cardholder con los datos que se definieron en la captura de datos.

2. Creación de Tarjetas: Una vez que se tienen los datos en la base de datos se hace la customización de la tarjeta

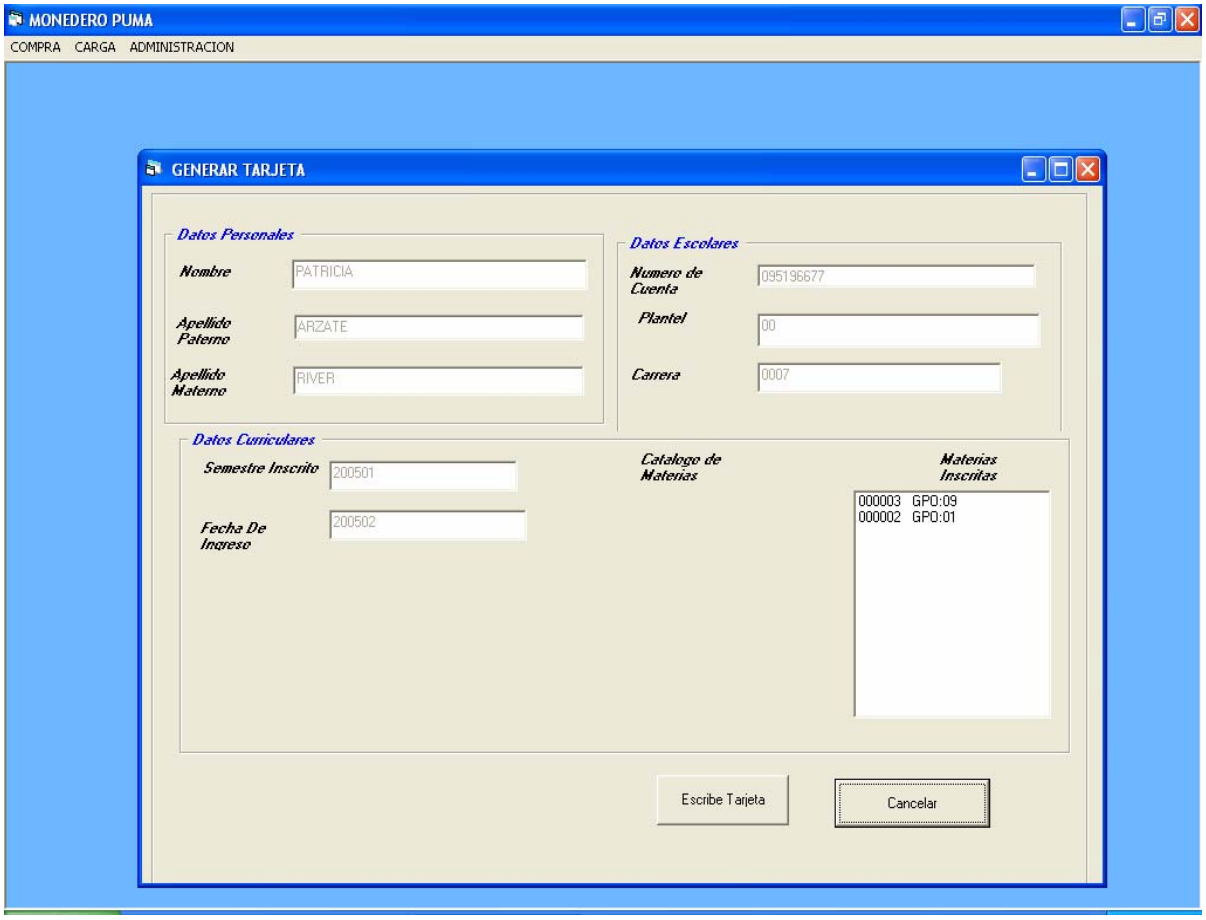
Es necesario mantener este control debido a los permisos asignados

Creación de Usuario:

Se capturan los datos que pertenecen a la aplicación identiFI para posteriormente ser cargados a la base de datos.



Creación de Tarjeta:



IV.5 Pruebas

La matriz de pruebas de la *tabla 4,* muestra el conjunto de las posibles entradas al sistema y la manera en como el sistema respondió a las mismas.

Tabla 4. Matriz de Pruebas

NÚMERO DE PRUEBA	PROCESO	DESCRIPCIÓN	RESULTADO	OBSERVACIONES
1	PROCESO DE PERSONALIZACIÓN	Tarjeta válida sin personalizar aplicar proceso de personalización	OK	Personaliza tarjeta
2	PROCESO DE PERSONALIZACIÓN	Tarjeta diferente a la requerida por la aplicación	OK	Se detiene el proceso
3	PROCESO DE PERSONALIZACIÓN	Lector Apagado	OK	No permite el acceso
4	PROCESO DE PERSONALIZACIÓN	Tarjeta No insertada	OK	No permite el acceso
5	PROCESO DE PERSONALIZACIÓN	No existe el registro Insertado	OK	No permite el acceso
6	CREAR USUARIO	Validación de todos los campos a llenar	OK	Recuerda el nombre del campo que no ha sido capturado
7	CREAR USUARIO	No existe conexión a la base de datos	OK	Envía error de Conexión de Base de Datos
8	CREAR USUARIO	Datos Incompletos	OK	Muestra error solicitando se llenen los campos
9	GENERACIÓN DE TARJETA	Datos Correctos, Tarjeta y Lector	OK	La personalización es exitosa

		correctos		
10	GENERACIÓN DE TARJETA	Tarjeta No insertada	OK	Muestra error de lectura en la tarjeta
11	COMPRA	Prueba OK	OK	La tarjeta es debitada
12	COMPRA	Monto mayor al saldo de la tarjeta	OK	No se permite el débito
13	COMPRA	Certificados Erróneos	Ok	Falla en el débito
14	COMPRA	Falla en lector	OK	No permite el acceso
15	COMPRA	Falla en tarjeta	OK	No se el acceso
16	COMPRA	Tarjeta con banderas	OK	No se permite el débito
17	RECARGA	Prueba OK	OK	La tarjeta es acreditada en el saldo
18	RECARGA	Bloqueo NIP	OK	No permite la recarga
19	RECARGA	Tarjeta con banderas	OK	No se permite la recarga
20	RECARGA	NIP introducido incorrecto	OK	Se incrementa el número de Intentos y no se permite recarga
21	RECARGA	El monto a recargar excede el máximo en monedero	OK	No se permite la recarga
22	RECARGA	No hay comunicación con el sistema	OK	No se permite la recarga
23	RECARGA	Certificados Erróneos	OK	No se permite la recarga

La fase de pruebas consiste, como se mencionó anteriormente, en determinar el comportamiento del sistema bajo los posibles escenarios que se pueden presentar, los cuales no precisamente llevan a una transacción satisfactoria, pero de cualquier manera el sistema logra mantenerse estable en la resolución de dichos factores en general.

V. CONCLUSIONES

V.1 Del Sistema Azul y Oro

En este trabajo se presentaron dos aplicaciones en tarjetas Inteligentes las cuales aportarían a la Facultad de Ingeniería un beneficio que compete a los aspectos económicos y administrativos, ya que la implementación de un monedero electrónico, llevaría a la Facultad de Ingeniería a un esquema de prepago, el cual ha sido utilizado en diferentes tipo de comercios y generan ganancias considerables por el solo hecho de contar con un flotante.

Por otro lado permite una mejor implantación de recursos y administración de los mismos, pues en base a la información generada se pueden obtener estadísticas que nos indiquen un determinado comportamiento y realizar una acción en pro del mejoramiento de los servicios.

Como se mencionó en los capítulos anteriores se pueden implementar más aplicaciones, tales como: un reloj checador para el personal docente; control de acceso a estacionamientos y edificios, así como a las salas de cómputo; validación de personal para exámenes por autentificación de huella dactilar; asistencia del alumnado, y todo bajo la misma implementación, lo que lleva a economizar el entregable al usuario (la Tarjeta Inteligente) y por otro lado a

que se dispone de la información generada por las aplicaciones y con la garantía de que la ocurrencia de un fraude es básicamente imposible.
Por otro lado se garantiza la vida útil de las tarjetas por lo menos 5 años en condiciones normales de uso.
Cabe mencionar que como se mostró en el cuerpo del trabajo se requiere de una infraestructura de comunicaciones y almacenamiento que de soporte al control de las tarjetas, así como de las aplicaciones implementadas en las mismas.

V.2 Del manejo de llaves.

La misión principal del manejo de llaves es mantener a éstas de manera confidencial. Si esto se puede garantizar entonces una sola llave sería suficiente para todos los procesos que se lleven a cabo en el ciclo de vida de la tarjeta, pero como esto no se puede garantizar en la práctica, es necesario utilizar diferentes llaves y diferentes procedimientos como son: la derivación, diversificación, versiones, llaves dinámicas, etc. Es necesario tener en cuenta que el uso excesivo de estos procedimientos genera retrasos en las transacciones y por otro lado se consume espacio en memoria (esto depende de la longitud de las llaves), por lo cual será necesario hacer un análisis del tipo de transacción, periodicidad de uso, confidencialidad de la información, etc.

V.3 De las Tarjetas Inteligentes.

Las Tarjetas Inteligentes son microcomputadoras (contienen microprocesador, memoria, Bus da datos I/O) en las que se puede crear aplicaciones de diversos tipos, en donde la información se puede almacenar de forma segura bajo diferentes esquemas.
La información esta estructurada de manera jerárquica lo que permite administrar los datos y aplicaciones bajo distintos tipos de acceso a esta misma.

Tanto el sistema operativo como la estructura física del chip han sido estandarizados lo cual permite una diversificación en el uso de dispositivos para accesarlas.

A continuación se presenta el prototipo en cuanto al diseño que se pensó para la aplicación de IdentiFI. La *figura 5.1* muestra el anverso de la credencial y la *figura 5.2* muestra el reverso de la credencial.

Figura 5.1 Anverso de IdentiFI

Figura 5.2 Reverso de IdentiFI.

V.4 Aplicaciones a Futuro

Aquellos campos que se dejaron para uso futuro.

Dentro de los datos contenidos en la tarjeta se propone que se agregue la siguiente información:

-Foto

-Historial

-Firma

-Huellas Digitales.

El porque no implementar en este momento estas aplicaciones se debió en primer lugar a que no contamos con los recursos necesarios (hardware, software) que nos permitan capturar digitalmente las fotos, las firmas, las huellas, para la implementación. En segundo lugar se debe a que la tesis tiene por objetivo mostrar a la Facultad lo qué es la Tarjeta Inteligente en base a las aplicaciones de monedero electrónico e identificación pues nosotros consideramos que son aplicaciones viables que permitirán familiarizar a la comunidad ingenieril con esta nueva tecnología. Sin embargo de ninguna manera queda limitado el sin fin de aplicaciones que pueden implementarse utilizando la Tarjeta Inteligente.

Caso de Negocio Universidad:

Reutilización de las tarjetas.

Las tarjetas serían anónimas, es decir, la información en el Impreso de la tarjeta no tendría ningún tipo de información personalizada. La ventaja de esta situación es la reutilización y venta de la tarjeta.

Es decir, la primera generación que adquiera la tarjeta la va a comprar y las generaciones posteriores pagarían por la tarjeta pero ésta sería reutilizable para la universidad.

La generación de un flotante en una cuenta de la Universidad.
Se introduciría el concepto de prepago en la Universidad, el prepago ha demostrado tener una buena aceptación en la sociedad.

Control de Ventas en las bibliotecas de las instalaciones de la UNAM.
Se podría extrapolar, pues los establecimientos que se encuentran en la Universidad podrían fungir como puntos de venta.

Aplicación de lealtad para fomentar el uso de la tarjeta.
Minar un amplio sector de explotación utilizando las tarjetas, generando nuevas aplicaciones (acceso, préstamos), respaldado por la seguridad que proporcionan las tarjetas.

Prestigio para la Universidad Nacional Autónoma de México y para la Facultad de Ingeniería al ser la primer Universidad Pública que incorpora este tipo de tecnología.

Caso de Negocio Exponsor:
Venta de tarjetas para cada alumno que pertenezca a la universidad.
Promoción de la tecnología CHIP.

GLOSARIO

BCD (decimal codificado en binario) es una forma directa asignada a un equivalente binario. Para este documento se utiliza (8,4,2,1)

BYTE: 8 bits agrupados.

CARDHOLDER: El usuario de la tarjeta, miembro.

CHALLENGE: Proceso de generación de número aleatorio para autenticación.

CONTACTLESS: Sin contacto

CUSTOMIZACIÓN: Adaptación de parámetros en la tarjeta.

DES: Data Encription Standar. Algoritmo simétrico para cifrado de datos

EMBEDED: Circuito embebido, incrustado.

ENCRIPCION: Proceso por el cual se codifican los datos en un mensaje.

GUILLOCHE: Patrón de líneas complejas formado entre varias curvas y de acuerdo a ciertos principios matemáticos.

LLAVE: Valor de tipo binario utilizado para cifrar datos.

LOG: historial de las transacciones del sistema

RSA: Algoritmo asimétrico para cifrado de datos sus iniciales hacen referencia al nombre de los creadores del popular Rivest, Shamir, and Adleman.

BIBLIOGRAFÍA:

Dreifus Henry y J. Thomas Monk, Smart cards: A guide to building and managing smart cards applications. Editorial John Wiley & sons, Inc.

W.Rankl, W.Effing, Smart Card Handbook. Editorial John Wiley & Sons, primera edición.

Pressman R., Ingeniería del Software, un Enfoque Práctico, tercera edición, Editorial Mc Graw-Hill, 1993.

Sommerville, Ingeniería del Software, 6ª edición, Addison-Wesley, 2002.

J.D. Ullman, Principles of Database Systems. Computer Science Press.

H.F. Korth, Fundamentos de Bases de Datos, 3ª edición, Mc Graw Hill

http://www.dcc.uchile.cl/~rbaeza/cursos/proyarq/hlopez/node4.html

http://www.rsasecurity.com/rsalabs/node.asp?id=2336

http://www.eumed.net/cursecon/ecoinet/seguridad/inteligentes.htm

http://www.segu-info.com.ar/proteccion/

BIBLIOGRAFÍA:

Dreifus Henry y J. Thomas Monk, Smart cards: A guide to building and managing smart cards applications. Editorial John Wiley & sons, Inc.

W.Rankl, W.Effing, Smart Card Handbook. Editorial John Wiley & Sons, primera edición.

Pressman R., Ingeniería del Software, un Enfoque Práctico, tercera edición, Editorial Mc Graw-Hill, 1993.

Sommerville, Ingeniería del Software, 6ª edición, Addison-Wesley, 2002.

J.D. Ullman, Principles of Database Systems. Computer Science Press.

H.F. Korth, Fundamentos de Bases de Datos, 3ª edición, Mc Graw Hill

http://www.dcc.uchile.cl/~rbaeza/cursos/proyarq/hlopez/node4.html

http://www.rsasecurity.com/rsalabs/node.asp?id=2336

http://www.eumed.net/cursecon/ecoinet/seguridad/inteligentes.htm

http://www.segu-info.com.ar/proteccion/