UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

USO DE TARJETAS INTELIGENTES PARA EL SISTEMA ESCOLAR Y LABORAL DE LA ENEP ARAGON

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

PRESENTA:

MOISES GONZALEZ GUTIERREZ

ASESOR:

M. en C. JUAN MANUEL LOPEZ CARRETO

2005

Dedicatoria

A Dios ....

Que me acompaño en todo el camino, sobre todo en los vados más oscuros proporcionándome todo los elementos necesarios para alcanzar mí meta.

A mis Padres ...

Que realizaron muchos sacrificios para que yo pudiera recibir una educación y una carrera.

A Gladis...

Que fue quien me impulso de principio a fin a realizar mi tesis.

A mis amigos y compañeros ...

Que me ayudaron con todos sus conocimientos cuando los necesite.

"Una cadena es tan fuerte como su eslabón más débil"

Sabiduría Popular

Objetivo General

Contemplando las bondades de la tecnología de las tarjetas inteligentes con esta tesis pretendo mostrar tanto a alumnos como a académicos de la ENEP Aragón las diversas áreas donde seria no solo viable sino también enormemente provechoso el uso de dicha tecnología en las múltiples áreas del ambiente tanto escolar como laboral, especialmente el manejo de características multiaplicativas de dicha tecnología.

ÍNDICE

Capítulo I. Estado del Arte.

Objetivo
Se establecerá una apertura a la problemática de la ENEP Aragón así como de los medios que se utilizarán para resolverla utilizando la TI.

I.1 Introducción.

I.1.1 Alcances.

Llevar el control de todos y cada uno de los elementos humanos que interactúan entre si dentro de una institución educativa, cualquiera que esta sea, nunca ha sido un trabajo sencillo.

Existen diversas áreas donde se puede apreciar esta complejidad. Cada una de ellas ofrece características muy particulares. Es por ello que es necesaria una solución que permita abarcar cada uno de estos aspectos.

El presente trabajo será orientado en exclusiva hacia las instalaciones de la ENEP Aragón, aunque por supuesto al ser las necesidades bastante similares al resto de la Universidad no sería muy complejo extenderlo al resto de la institución.

Se presentará un análisis completo que va desde las características físicas de la Tarjeta Inteligente o TI que se utilizará hasta los esquemas de flujo de datos. Además de ser posible y de contarse con los elementos necesarios, se realizará una presentación del funcionamiento de los diferentes los elementos que se utilizarían en un proyecto completamente funcional.

I.2 Definición del Problema.

I.2.1. Sistema actual de la ENEP Aragón.

Para poder ofrecer un panorama de las necesidades administrativas de la ENEP Aragón que la TI deberá ayudar a resolver, es preciso conocer cada una de éstas. Dichas necesidades serán clasificadas de acuerdo a los sujetos sobre los cuales giran los procesos dentro del centro de enseñanza esto es: Alumnos y Maestros.

Para cada uno de estos elementos, se describirán los diferentes escenarios en los cuales participan.

I.2.1.1. Pago de Servicios

El manejo del dinero dentro de la institución dentro de todos sus aspectos puede llegar a ser un proceso bastante complejo, peligroso y caro en cuestión de manejo y transporte del mismo.

A continuación se detallan algunos de estos aspectos y sus particulares situaciones negativas para cada uno de ellos:

- Tanto en la biblioteca como en otros lugares dentro de la ENEP donde se presta el servicio de las fotocopias el tiempo invertido en este proceso puede ser largo y extenuante debido a que:

    - En la mayoría de las ocasiones existe una gran cantidad de personas sobre todo en la biblioteca) las cuales muchas veces no lleva uno sino dos o más documentos a copiar.

    - Una vez que logramos llegar a la ventanilla de servicio y al hacer el pago correspondiente, resulta que nunca existe cambio, por lo que se tiene que conseguir de una forma o de otra provocando un retraso mayor.

- En el área de servicios escolares debido a que para algunos tramites es necesario realizar el pago correspondiente si este no ha sido efectuado, ya sea porque la caja ya ha cerrado, no cuenta con efectivo o porque la misma ventanilla esta a punto de concluir sus labores no será posible completarlos ese mismo dia, lo cual en algunos casos (como para exalumnos) es prácticamente imposible debido a sus demás ocupaciones.

- El pago para la expedición de papeles oficiales (tales como historiales académicos o tira de materias) que permiten realizar otros tramites tales como la inscripción a la biblioteca puede ser muy problemático por las misma razones que en el punto anterior, además de que en época de inscripciones no es uno o dos alumnos sino docenas.

- Uso de Servicios de Cómputo. Dentro de los laboratorios tanto para Internet (Fundación UNAM) como para otras aplicaciones (Centro de Cómputo) el cobro de todos sus servicios (y sobre toda su contabilidad) aunque eficaz no resulta eficiente.

I.2.1.2. Biblioteca

Dentro de las actividades de la biblioteca existen aspectos que a pesar de ser eficaces no son eficientes sobre todo en determinadas épocas y situaciones en los cuales los recursos no alcanzan a cubrir las demandas de los alumnos por lo que, estos llegan a tener una visión negativa e incluso deficiente de su escuela lo cual es dañino para toda la UNAM y no solo para la ENEP.

Uno de estos aspectos es tanto el préstamo como la devolución en los cuales aunque el sistema utilizado falla o "se cae" en muy raras ocasiones, este no puede ser utilizado si no se cuenta con el personal necesario lo cual en temporadas de exámenes con frecuencia llega a ser insuficiente lo que acarrea una cantidad de retrasos por no decir las frustraciones tanto por parte del alumnado como por el del personal.

- Por supuesto no son los únicos servicios que la biblioteca ofrece pero la mayoría de estos ya se encuentran incluidos dentro de la sección anterior ya que involucran manojo de dinero(copias, multas etc.)

I.2.1.3. Asistencia

En la actualidad el registro de asistencia de los maestros es realizado mediante la firma de los mismos en el momento de su entrada y de su salida en un cardes ubicado en la sala de maestros. Esta acción no es obligatoria ya que se realiza para la obtención de un bono por asistencia

Este proceso independientemente de ser un proceso extremadamente lento y obsoleto, es propenso a diversas irregularidades además de que no es posible llevar estadísticas confiables y eficientes de diversas situaciones tales como:

- La hora de entrada y salida de los maestros
- El grado de absentismo por áreas y carreras

Otra desventaja que acarrea llevar un control de este tipo es que al obligar a los maestros a realizar un registro en un lugar fijo y único se propicia la omisión de su registro ya sea por falta de tiempo o por indolencia.

I.3 Primer acercamiento a la Tarjeta Inteligente (TI)

Seguramente cada uno nosotros hemos tenido en nuestras manos una tarjeta con chip aunque sea de un tipo tan simple como la telefónica. Lo que probablemente no conocemos, es que este tipo de tecnología tiene un largo trecho recorrido, con un origen que se puede remontar hasta la década de los 70's en la que la microelectrónica empezaba a dar muestras de su enorme capacidad.

En dicha década se manejaban ya las populares tarjetas con banda magnética con el nombre y firma del usuario embosadas[i] en su superficie. Pero este tipo de medios adolece (y aun lo hace) de una debilidad fundamental que es que cualquier persona que tuviera al alcance un dispositivo de lectura y escritura de banda podía modificar (o como popularmente se le conoce en la actualidad "clonar") los datos de esta tarjeta, provocando el consiguiente fraude al sistema.

Para frenar este tipo de ilícitos se implantó la comunicación en línea con el banco, el cual verificaba el NIP (número de identificación personal) de la tarjeta al momento de hacer la transacción, pero este sistema involucraba altos costos de mantenimiento, además que como se ve en la actualidad esto no ha frenado en mucho los fraudes.

Por lo anterior, se inició la búsqueda de opciones que aportaran una mayor seguridad y que permitiera realizar transacciones fuera de línea la cual es la principal característica del las TI.

El inicio de esta solución fue la concesión de una patente en Alemania para Jurgen Dethloff y Helmut Grotrupp la cual definía la inserción de un microchip con capacidades aritméticas y lógicas (el primero de éstos fue hecho en Japón por Kunitaka Arimura en el año de 1970) dentro de una tarjeta de silicón[ii].

[1] Diseño que estampa sin tinta, dándole un efecto de bajo relieve.

El siguiente paso sucedió en Francia en 1974 por parte de Rolando Moreno a quien le fue concedida la primera patente de una tarjeta de Circuito Integrado o "IC" práctica.

Curiosamente, contra lo que uno se pudiera imaginar no fue el área bancaria la primera en la utilización real de estos primeros ejemplos de la TI (a pesar de que ya habían sido desarrollados los primeros microcontroladores seguros por parte de la compañía Motorola en 1979), sino una compañía telefónica en Francia en 1984[iii] las cuales no han cambiado mucho, excepto por su nivel de capacidad de almacenaje y seguridad

La principal razón fue que para poder brindar una seguridad adecuada hacia la información contenida en el chip de la tarjeta, se necesitaban algoritmos criptográficos los cuales alcanzaron un grado de madurez suficiente hacia la década de los 60's.

Estos algoritmos embonaron perfectamente en las características de las tarjetas de su época. Por supuesto conforme los procesadores de las tarjetas se hicieron más poderosos se utilizaron algoritmos más sofisticados y complejos.

Por esta razón en la actualidad para que una tarjeta sea considerada como inteligente es necesario que posea la capacidad de ejecutar algoritmos criptográficos (en una sección posterior se hablará sobre estos algoritmos) que permitan proteger su información. Estos fueron por primera vez usados por los bancos en Francia y posteriormente en Alemania.

Las primeras aplicaciones bancarias reales sucedieron en 1986 con la distribución de TI entre los clientes del Banco de Virginia y el Banco Nacional de Maryland[iv]

En la actualidad existen una amplia gama de diferentes variantes de Tarjetas con Chip las cuales van desde tarjetas de memoria, las cuales solo almacenan datos, por lo que no tienen la capacidad de procesamiento, pasando por tarjetas ecológicas (elaboradas mediante una combinación de PVC y PET (polietilenterftalato)), tarjetas Holográficas (utilizadas para promociones por ejemplo), tarjetas sin contacto (usadas en estacionamientos por ejemplo) hasta tarjetas multiaplicación. Buena parte de estas y otras variedades de tarjetas serán explicadas posteriormente.

En un apartado especial de este tipo de Tarjetas multiaplicativas se encuentran las tarjetas Java, las cuales pueden realizar cálculos independientes de los necesarios para la criptografía mediante el lenguaje de programación Java contando con la capacidad de que pueden ser "recicladas" en sus aplicaciones, además de que los sistemas y equipos en los cuales se apoya se reducen al mínimo además de que su capacidad puede alcanzar hasta un 1 MB[v] (ver figura 1).

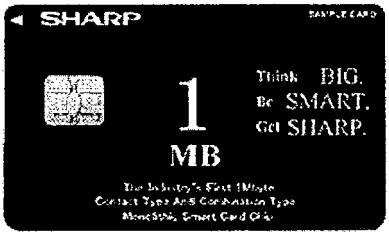


Figura 1.Tarjeta con capacidad de 1 MB

Por supuesto este tipo de tarjetas involucra contar con un alto presupuesto ya que algunos de los kits de desarrollo pueden llegar a costar hasta 400.00 dólares americanos[vi].

Para nuestro análisis se pretende que la TI sea un engrane dentro de una infraestructura soportada por un sistema de cómputo centralizado que en conjunto con los dispositivos conocidos como lectores (que son dispositivos que se encargarán de leer la información contenida en la tarjeta) y terminales (equipos que permiten además de leer realzar cálculos y verificaciones sobre los datos de la tarjeta) pueda supervisar diferentes aspectos desde el registro de asistencia de los recursos humanos, hasta el control del dinero que circula dentro de la ENEP Aragón.

La tarjeta que se pretende utilizar es de una capacidad de memoria y procesamiento pequeña sobre todo porque la información almacenada es mínima y la mayor parte del proceso deberá ser llevado a cabo por los lectores, terminales y un sistema de cómputo.

I.4 Una mirada a los usos de la TI en la ENEP Aragón.

I.4.1. Pago de Servicios

A continuación se mencionará la manera en que pude usarse la TI, dando a conocer varias de sus capacidades en algunas de las situaciones cotidianas que se viven en la ENEP Aragón. Cabe mencionar que en el desarrollo de esta tesis se abarcarán todos y cada uno de los aspectos que se definieron al principio de este capítulo

El uso de "dinero[2]" que solo pueda ser usado dentro de la institución permitiría llevar un control mucho mas estricto en cualquier aspecto en el que este factor se vea involucrado y para muestra se tomará los mismos problemas que se describieron en el punto que describe la situación actual de la ENEP Aragón.

- Para el uso de los servicios de fotocopiado el uso de dinero dentro de un chip evitaría el manejo en efectivo y reduciría significativamente tanto el tiempo de espera al obtener el servicio para el usuario como por parte de los que esperan por él. Un beneficio a largo plazo (si se decide en invertir

[2] En sentido estricto lo que se planea usar dentro de la institución no es dinero sino una representación de este.

en tecnología adicional, la cual puede ser en fotocopiadoras que los mismos alumnos puedan usar por medio de su tarjeta) que proporcionaría este proceso, es que nunca mas necesitaríamos de la utilización de trozos de papel para definir qué y cuántas copias ya que nosotros mismos podríamos proporcionarnos el servicio.

- Para los servicios de trámites escolares en lugar de ir y esperar a que la caja se encuentre disponible y posteriormente regresar a la ventanilla a utilizarlo, el dinero necesario para este se encontraría disponible en cualquier momento.

Una ventaja en extremo importante que involucra a todos los puntos anteriores, es que todos tanto los cobros como los pagos por todos los servicios (los anteriores solo son una muestra; existen muchos mas los cuales se describirán en el capítulo 4) podrán ser monitoreados en forma expedita.

El manejo del dinero para cada uno de los casos anteriores por lo menos en un nivel inicial se realizaría a través de una política compensatoria que permitirá saber exactamente de que manera y cuándo se gasto el dinero recabado. El cómo se maneje este tipo de política así como se llevará a cabo la recarga del dinero en las tarjetas se verá en el capitulo 4

I.4.2. Biblioteca

Dentro de la biblioteca, la cual, aunque presta su servicio de una manera eficaz, este puede ser mejorado de las siguientes maneras:

- Utilizando la TI como un registro de todo el material que en determinado momento el alumno tiene en préstamo sin necesidad de utilizar el sistema propio de la biblioteca

- Permitiendo a los usuarios registrar sus propios préstamos y devoluciones en ocasiones en que tanto el personal como el sistema se encuentren saturados, como puede ser en época de exámenes.

I.4.3. Asistencia

El uso de la tecnología de la TI permitiría obviar las situaciones inconveniencias mediante la utilización de tarjetas.

La probabilidad de la falsificación es prácticamente inexistente ya se definirían uno o varios niveles de protección dentro de la tarjeta para impedir que el registro pueda ser manipulado.

Así mismo se podría proporcionar un registro formal sobre el absentismo el cual seria perfectamente confiable así como verificable en cualquier momento (esto dependerá de cuantas veces al día se realizara la descargara la información de las terminales y/o lectores).

Finalmente para evitar la tentación de no hacer su registro de entrada por cualquier motivo se podrían establecer lectores en lugares estratégicos tales como estacionamientos y cubículos de la escuela.

Capítulo II. Evolución y Uso de Tarjetas.

Objetivo
Se ofrecerá al lector una mirada breve pero concisa al mundo de las Tarjetas Inteligentes en diferentes niveles para que pueda llegar a comprender como será posible la adopción de esta tecnología a los problemas por resolver

II.1 Tarjetas Inteligentes de Contacto

II.1.1. Antecedentes

Una vez que en el capítulo anterior se obtuvo una perspectiva de cual y como fue el origen de las TI, ahora se procederá a echar un vistazo a como están compuestas.

II.1.1.1. Historia

El nivel de integración (número de transistores que contiene un circuito y/o chip) de un chip en una TI de contacto en la actualidad es de aproximadamente de 4000[vii] billones[3]de transistores.

Esta enormidad de elementos dentro de tan limitado espacio no se consiguió de la noche a la mañana sino que requirió de un largo proceso que inició con la invención del primer transistor.

Este fue el primer paso en la carrera de la miniaturización, ya que se creo para cubrir las deficiencias de las válvulas de vació o como comúnmente se les conoce bulbos alrededor en el año de 1948 en los laboratorios Bell[viii], para las primeras computadoras.

Este primer transistor sentó las bases de la construcción del primer circuito integrado o chip en una base de silicio, que a su vez permitió la reducción del precio y de los porcentajes de error.

El siguiente paso se realizó con la invención del primer CI(Circuito Integrado) en el año de 1959 (tenía seis transistores[ix]) y mas adelante el primer circuito integrado plano por Robert Noice de Fairchild Semiconductors y Jack Kilby en Texas Instruments.

La invención del circuito integrado reveló el potencial para extender el costo y los beneficios de operación de los transistores a todos los circuitos producidos en masa. La invención del circuito integrado permitió que docenas de transistores se pusieran en el mismo chip. Este empaquetamiento permitió construir computadoras más pequeñas, rápidas y baratas que sus predecesores con transistores

El proceso de ir reduciendo cada vez más dío lugar a diferentes tecnologías a principios de los 60's tales como[x] :

---

[3] Se debe tener en cuenta que a diferencia de los hispanos parlantes un billón para los anglo parlantes no es un millón de millones sino mil millones. Ver. http://www.manuelmateos.com/criptosemas_del_ingles.htm ó http://www.ompersonal.com.ar/omexpress/numerosymedidas/numeroscardinalesyordinales.htm

- RTL (Lógica Transistor Resistor)
- DTL (Lógica Transistor Diodo)
- TTL (Lógica Transistor Transistor)
- ECL (Lógica Complementada Emisor).

En 1965, Gordon E. Moore (fundador de Fairchild, y patentador del primer circuito integrado) cuantificó el crecimiento sorprendente de las nuevas tecnologías de semiconductores. Dijo que los fabricantes habían duplicado la densidad de los componentes por circuito integrado a intervalos regulares (un año), y que seguirían haciéndolo mientras el ojo humano pudiera ver[xi].

A finales de los 70's se inician las tecnologías de lógica digital dispositivos en escala SSI (50 a 500 transistores) A diferencia de los CI elaborados mediante esta tecnología en el cual el máximo de compuertas[4] lógicas era de 10 ó 12, la integración MSI hizo integrar bloques más complejos como contadores y multiplexores.

Con la integración de LSI se hizo posible la realización de circuitos a medida como los controladores para las pantallas de video con el inconveniente de que su costo era muy elevado por lo que solo se dirigían a aplicaciones con alto volúmen de ventas[xii].

En la integración a gran escala (LSI, acrónimo de Large-Scale Integration) se combinan desde 500 a 50000 de transistores, además de resistencias y otros elementos, en un cuadrado de silicio que mide aproximadamente 1,3 cm de lado.

Esta tecnología en un principio no se sabía si podría ser para una utilidad general dentro de algún mercado más amplio.

II.1.1.2. Microprocesadores

En 1969 una compañía Japonesa fabricante de calculadoras realizó un encargo a una nueva compañía especializada en la fabricación de memorias conocida como Intel la realización de un circuito de control para un nuevo modelo de calculadora.

El primer diseño resultó tan complejo que el ingeniero Ted Hoof, pensó que las computadoras de la época tenían una complejidad similar pero a través de un diseño más simple, por lo que rediseñó completamente el sistema basándose en la estructura de las mismas:

- Un chip que integraría una CPU (Unidad Central de Procesamiento) sencilla que ejecutaría un programa de control
- Una pastilla ROM (Memoria de Solo Lectura) la cual almacenaría el programa de control
- Una RAM (Memoria de Solo Lectura) para almacenamiento de datos
- Un registro de para entra y salida

Esto dio como resultado un diseño conformado por cuatro chips o CI el cual con sólo cambiar le programa almacenado podía utilizarse para trabajos muy diferentes.

[4] Bloques de Circuitería que producen que producen las señales de salida lógica o lógica 0

Desde que se contrató a Intel para la realización del diseño, los costos para la realización de este diseño se habían elevado notablemente debido al tiempo(varios meses), por lo que Busicom, la compañía japonesa, solicitó una reducción en el precio a lo que Intel accedió a cambio de los derechos de los conjuntos de circuitos.

Finalmente Intel produjo el primer microprocesador comercial conocido como 4004 en sus catálogos en 1971.

Posteriormente, con el desarrollo de la integración en gran escala surgió el primer desarrollo de la primer TI el 21 de Marzo de 1979 surgida de los esfuerzos conjuntos realizados por las compañías Honeywell, CII, Bull, y Motorola. Esta primer tarjeta incluía una memoria 2716 y un procesador de 8 bits 3870 (ver detalle del circuito en la figura 2.0), lo que permitió que fuera más flexible[xiii].

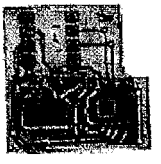


Figura 2.0 Fotografía del circuito de la primera de TI

II.1.1.3. Memorias

Como se describió anteriormente, para que un microprocesador funcione son necesarios CI donde almacenar y procesar la información que se va a manejar, mejor conocidos como memorias y por supuesto para las TI no podría ser la excepción aunque para estas existen diferencias significativas (en la mayoría de las tarjetas) de cómo se realiza dicha manipulación a través de las memorias. Estas divergencias se explicarán más adelante con mayor detalle. A continuación se describirán las características principales de las memorias que se utilizan dentro de las TI.

- **Memorias RAM**

Su nombre completo es "Ramdom Acces Memory" o Memoria de Acceso Aleatorio, esto es, se puede acceder a cualquier byte de la memoria sin pasar por los bytes precedentes. Este tipo de memoria en una TI es donde los datos son almacenados durante una sesión.

El acceso es posible en un número ilimitado de veces y no existe ninguna restricción (como ocurre en otras memorias) .Necesita un suministro constante de energía. Cuando esta es interrumpida el contenido de esta se pierde.

- **Memoria ROM**

Las ROM (Memorias de Sólo Lectura) son memorias que salen grabadas de fábrica con la programación especificada por el cliente.

En una memoria de solo lectura su contenido es absolutamente inalterable, desde el instante en que el fabricante graba las instrucciones, por lo tanto la escritura de este tipo de memorias ocurre una sola vez y queda grabado su contenido aunque se le retire la energía[xiv].

El otro subgrupo de memorias de sólo lectura está conformado por las memorias reprogramables. A su vez, entre ellas existen diferencias en su modo de borrado y reprogramación.

- **EPROM**

El subgrupo de las EPROM (ROM Borrable y Programable) se destaca en que, constructivamente sus componentes tienen una ventana que se halla directamente sobre la matriz del chip.

Cuando se hace necesaria una regrabación del chip, se somete al mismo a una radiación de luz ultravioleta muy intensa, con lo que se borra el contenido almacenado y se torna disponible para una nueva grabación.

- **EEPROM**

El otro subgrupo es el de las EEPROM ó E²PROM(PROM Eléctricamente Borrada), cuyo método de borrado y grabación consiste en la aplicación, de una manera determinada, de pulsos de tensión.

Son básicamente de sólo lectura; pero pueden ser usadas como de escritura "lenta"(Alrededor de 10 ms) para el almacenamiento prolongado de nuevos datos.

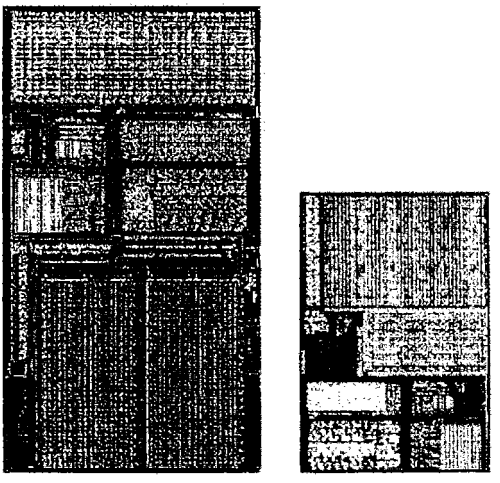
II.1.2. Elementos que conforman a la TI[xv]

Después de las secciones anteriores, en las que se hizo un breve resumen de las tecnologías que participan dentro de una TI, a continuación se orientaran estos conocimientos a las semejanzas y diferencias de ellos con los que se encuentran en la TI.

II.1.2.1. Microprocesadores

Los microprocesadores de la TI no son componentes estándar, por lo que no es posible adquirirlos en forma independiente. Por el contrario son CI especialmente desarrollados y no son implementados en otras aplicaciones. La razón para esto es el costo de su manufactura debido a que muchos de los elementos que están integrados en los microprocesadores estándar no son útiles para los propósitos de las TI..

Dado que estas características especiales ocupan dentro de la placa de silicio, el chip es despojado de ellas reduciéndolo aproximadamente un 10 %, es decir que de un procesador de 21.7 mm con una técnica de 1 μm se obtiene uno de 10mm con una técnica de 8 μm. como se pude apreciar en la figura 2.1.



[xvi]

Figura 2.1. Comparación entre un chip estándar y uno modificado para TI

Aunque los costos no son reducidos en forma significativa, el peso y volúmen que se ahorran justifican la modificación del chip

- **FUNCIONALIDAD:** A diferencia de un circuito estándar el microprocesador de una TI debe de estar perfectamente adecuado a su entorno, ya que debe contener una multitud de circuitos además del propio micro, entre los cuales se encuentran memorias, dispositivos entrada/salida (E/S) y alimentación de 5 V.
- **SEGURIDAD:** El chip al estar muchas veces dirigido hacia áreas sensibles en cuanto a los datos que contiene (como es el caso del dinero), este debe ser capaz de tener integrada y habilitada la seguridad desde su misma creación, como un proceso inevitable.
- **DISPONIBILIDAD:** Las políticas de seguridad de la mayoría de los fabricantes de tarjetas hacen prácticamente imposible que estos dispositivos lleguen al mercado abierto. Esto así mismo provoca que la ingeniería inversa sea extremadamente difícil para un competidor.

Algo que se debe considerar sobre estos dispositivos que aunque existen especificaciones exclusivas para ellos, los mismos han sido probados exhaustivamente. Al utilizar estos procesadores ya probados es lógico que la tecnología de estos no se encuentre al mismo nivel de los micros más avanzados.

Como un ejemplo de ello es que un número de 200 000 transistores contenidos en un chip actual para TI (el cual se considera elevado para este propósito)no se compare con los contenidos en el procesador Pentium el cual contiene aproximadamente 3.1 millones de transistores.

II.1.2.2. Coprocesadores

Como un apartado especial dentro de los procesadores para las TI, existen unidades llamadas coprocesadores los cuales permiten a una tarjeta realizar cálculos mediante algoritmos criptográficos más avanzados, así como autentificaciones más veloces. A los procesadores que incluyen este componentes se les da el nombre de Criptoprocesadores.

La desventaja que tiene esto es que su costo se eleva significativamente. Por ello este tipo de TI se utilizan principalmente en aplicaciones bancarias entre otras, que requieren de una seguridad más elevada.

II.1.2.3. Memorias

Dentro de los diferentes tipos de memorias que se utilizan dentro de una TI, la memoria ROM es de las más grandes incluso de la EEPROM, esto es debido que almacena el sistema operativo que administra todos los recursos, aunque en algunas tarjetas con una sola aplicación algunos elementos del sistema operativo se encuentran también en la EEPROM así como también algunas variables de aplicación.

Para darnos una idea del tamaño (y por supuesto el esfuerzo para construirlas dentro de un rectángulo de 25 x 15 mm) en la figura 2.2 se muestran las diferentes dimensiones de las memorias de una TI

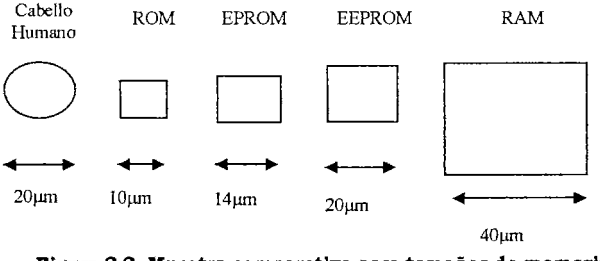


Figura 2.2. Muestra comparativa para tamaños de memorias xvii

- **MEMORIA ROM**

Como se mencionó anteriormente en la memoria ROM se almacena el sistema operativo de la tarjeta además de otros datos como son pruebas y funciones de diagnostico.

- **MEMORIA EPROM**

Este tipo de dispositivo se llegó a utilizar en las primeras TI que se produjeron ya que era la única clase de memoria existente que podía retener información sin que fuera alimentada constantemente por un voltaje. Su desventaja era que dado que sólo podían ser borradas por medio de Luz Ultravioleta estas no podían ser modificadas nuevamente, por lo que su uso no fue muy extendido.

- **MEMORIA EEPROM**

Esta memoria es usada en las TI para aquellos datos que debe poder ser grabados, borrados o modificados. Funcionalmente (aunque no estructuralmente) una EEPROM corresponde al disco duro de una computadora. Para minimizar los errores de escritura dentro de una memoria de este tipo existen software de detección de errores integrado como parte de la circuiteria. Este tipo de implantaciones en la memoria es común ya que aunque requiere de un espacio dentro del circuito (aumentando el tamaño del mismo), esto se compensa con un mayor tiempo de vida para el chip.

- **MEMORIA RAM**

Los tipos de RAM usadas en las TI son SRAM o memoria estática, con esto se quiere decir que su contenido no necesita ser refrescado tan frecuentemente como con otras (Memoria Dinámica DRAM).

En la figura 2.3 y 2.4 se pude observar los diferentes componentes que anteriormente se han descrito:

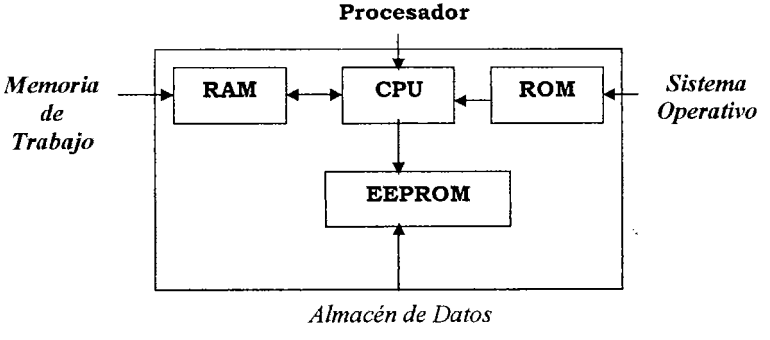


Figura 2.3. Diagrama esquemático de memorias

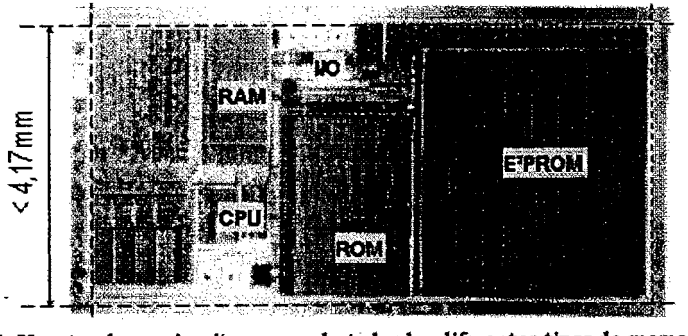


Figura 2.4. Muestra de un circuito ocupando todas los diferentes tipos de memoria

II.1.3. Estándares ISO para tarjetas

Para empezar, cabe preguntar que significa ISO, bueno pues es Organización para la Estandarización Internacional y como su nombre indica es una agrupación que define la forma de fabricación y funcionamiento de amplia gama de artículos y procesos alrededor del mundo.

Por supuesto el mundo de la TI no podía ser la excepción, al ser un dispositivo tan complejo y de tan amplio alcance. Y muestra se tiene a Francia en el que su uso es tan común como aquí la moneda fraccionaria.

Antes de seguir explicando las características de las ISO, es necesario mencionar por son importantes estos estándares para las TI.

- Permite la interoperabilidad entre tarjetas de diferentes emisores[5].
- El emisor puede elegir entre diferentes proveedores[6].
- Un proveedor puede suministrar a diferentes emisores

En esta sección se hará una breve mención acerca de algunos de estos estándares.

Las normas ISO controlan y especifican cada uno de los aspectos de la tarjeta desde la posición del chip hasta los comandos del sistema operativo que se ponga pasando por todos los dispositivos que interactúan con ella.

Como se definió en el capítulo anterior las TI no surgieron repentinamente sino que se derivaron desde otros tipos de los cuales tomaron sus ventajas y corrigieron sus errores. Los estándares también evolucionaron desde estas primeras tarjetas. Los primeros con el nombre de 7810 al 7813 (conocidos como con el nombre de series) los cuales definen las propiedades físicas agrupadas en el formato ID-1.Estos incluyen las tarjetas embosadas y con banda magnética.

Para que la TI (que para las normas ISO se conocen como tarjetas de circuito integrado o ICC) tuviera compatibilidad con los tipos de tarjetas previas, tuvo que darse una integración dentro de los estándares previos. La desventaja de esto fue que debido a los intensos procesos mecánicos a que es sometida la tarjeta, un alto nivel de resistencia es requerido en su fabricación.

Entre algunos de los diversos y arduos requerimientos que una tarjeta se encuentran:

- Resistente a Rayos X y Rayos UV.
- Resistente a altos voltajes, campos electromagnéticos y electricidad estática
- El circuito integrado no debe dañar la banda magnética.

La evolución desde las primeras tarjetas hasta las TI dentro de las normas ISO se muestra a continuación con algunas de ellas:

[5] Se llama así al que promueve la tarjeta.
[6] Se llama así al que fabrica la tarjeta.

II.1.3.1. Propiedades Físicas

Como se definió anteriormente, la TI esta dentro del formato ID-1 (existen también ID-2 y ID-3) perteneciente al estándar 7810 el cual define las características física de la tarjeta tales como flexibilidad, resistencia a la temperatura y dimensiones. En la figura 2.5 se puede apreciar algunas de sus características:

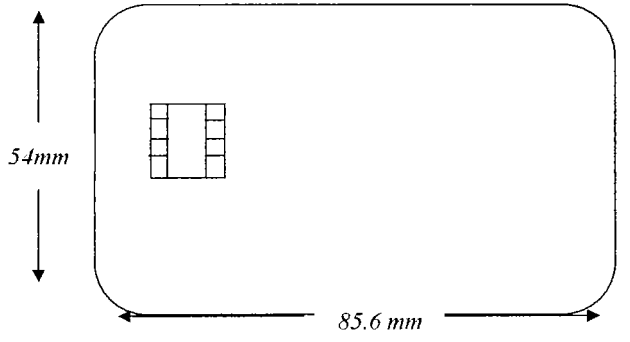


Figura 25.Diagrama grafico de dimensiones ISO

II.1.3.2. Tarjetas Embosadas

El tipo de embose y su lugar en la tarjeta se define en la norma 7811.Algunas de sus características se puede apreciar en la figura 2.6

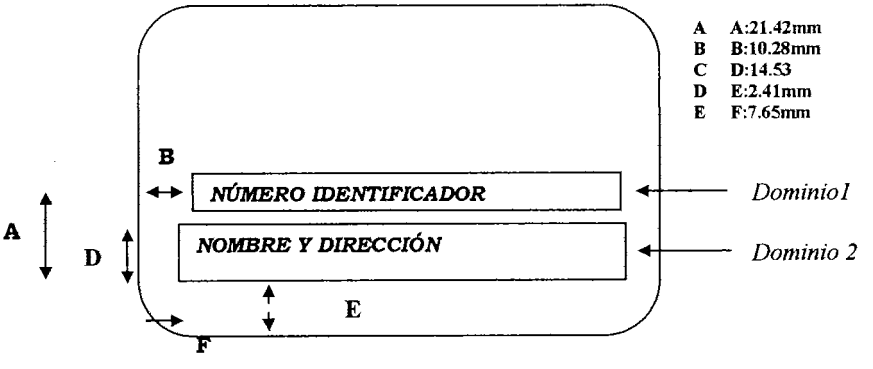


Figura 2.6. Dimensiones para tarjetas embosadas

Con una vista superficial, la transferencia de información mediante esta técnica hacia la tarjeta puede parecer primitiva pero no hay que olvidar que permitió la difusión de las tarjetas plásticas hacia el mundo entero.

II.1.3.3. ISO en Tarjetas Inteligentes.

Las tarjetas inteligentes son el miembro mas joven de la familia de tarjetas de identificación. La norma ISO en la que las TI están basadas es la 7816.Sus principales elementos de esta se mencionan a continuación:

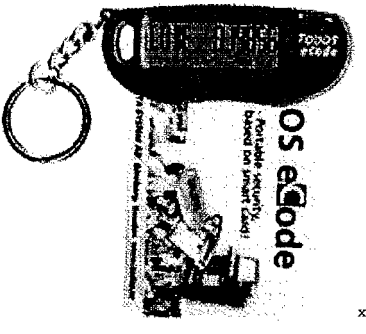
- ISO 7816-1: Características Físicas.
- ISO 7816-2: Dimensiones y ubicaciones de los contactos.
- ISO 7816-3: Señales Electrónicas y Protocolo de Transmisión
- ISO 7816-4: Respuestas y Comandos Ínter industrias.
- ISO 7816-5: Sistema de Numeración y Procedimiento de registro.
- ISO 7816-6: Elementos de datos Ínter industrias.
- ISO 7816-7: Comandos Ínter industrias y Consultas Estructuradas para una Tarjeta
- ISO 7816-8: Comandos Ínter industria Relacionados con Seguridad.
- ISO 7816-10:Señales electrónicas

II.1.4. Lectores

Toda la versatilidad de las TI seria inútil sin los dispositivos con los cuales interactúa con el usuario. Dentro de estos se encuentran los lectores y terminales. A continuación se describirán las características más importantes sobre los lectores. En la sección posterior se verán los aspectos de las terminales.

II.1.4.1. Descripción

Estos dispositivos también conocidos como CAD (Dispositivo de Aceptación de Chip) son en principio nada mas que una interfaz, es decir funciona como un enlace electromecánico entre el sistema operativo de la tarjeta y la computadora, aunque existen algunas excepciones como son los lectores portátiles los cuales funcionan con una pila y que permiten verificar algunos de los datos de la tarjeta(estos datos varían de tarjeta en tarjeta).Una muestra de ello se pude apreciar en la figura 2.7



xviii

Figura 2.7.Lector de Tarjetas

Existen diversas formas de clasificar los lectores, pero la mas utilizada es mediante la forma en que se comunican.

- **Lectores conectados a una PC**: Estos dispositivos como su nombre lo indica se utilizan para operaciones a través de un computador. Su conexión se realiza mediante cualquiera de los siguientes medios:

  - **Puerto Serie*(RS232)*:** Este tipo de lectores es el más común debido a su relativo bajo costo pero su inconveniente se centra en que su comunicación que al ser por puerto serial su trasmisión llega a ser muy lenta debido a que un byte es enviado hasta que el ultimo es recibido esto lo hace una comunicación muy lenta.

  - **PCMCIA (Personal Computer Memory Card International Association):** Este tipo de lectores se encuentra específicamente diseñado para computadoras portátiles. Una ventaja sobresaliente de este tipo de lectores es que permite la inserción de tarjetas y empezar a usarlas sin necesidad de reiniciar la máquina.

  - **Puerto USB:** Este tipo de lectores es de los más recientes, rápidos y caros ya que debido a que su tipo de conexión permite la transferencia de datos más eficiente.

- **Lectores conectados a un equipo específico**: Son lectores creados sobre diseño que actúan sobre otros dispositivos tales como máquinas expendedoras, parquímetros, controles de acceso etc.

- **Lectores Portátiles**: Son equipos que no necesitan de otro elemento para trabajar ya que son autosuficientes en elementos tales como memoria y baterías(Ver figura 2.7).

- **Teclado de PC** con lector integrado. Aunque estos no son tan abundantes hoy en día, se piensa que en un futuro serán objetos comunes en las casas ya que una aplicación práctica de ellos seria la autorización para el acceso de sitios Web.

Los lectores al tener una estructura relativamente sencilla tanto en su parte eléctrica como mecánica los hace unos dispositivos muy versátiles y significativamente económicos.

A pesar de ello sus características de seguridad dejan mucho que desear ya que al permitir el ingreso de datos confidenciales (tales como passwords) por medios no seguros (tales como los teclados de las computadoras) estos pueden ser interceptados y comprometidos. Esto se lograría colocado un elemento ya sea de software o hardware que permitiera leer cada una de las palabras que nosotros ingresáramos por dicho miedo, es decir toda la seguridad de la tarjeta estaría comprometida no importando si se tratase de la tarjeta mas cara con el procesador más rápido del mercado.

A pesar de esto existen algunos tipos de lectores que ofrecen cierta protección aunque algunos de estos dispositivos llegan tener un costo bastante alto en comparación con los lectores no seguros los cuales pueden adquirirse por unos pocos dólares.

A continuación se muestran algunos lectores segurizados:

II.1.4.2. Lectores Segurizados

CZAM-PC: Este tipo de lector contiene integrado un teclado propio como se puede ver en la figura 2.8[xix]. Gracias a esta característica el ingreso de cualquier elemento confidencial (tales como NIPS o Números de Cuenta) se encuentra a salvo ya que no pueden ser interceptados, por supuesto esta seguridad tiene su costo que es de aproximadamente de USD $ 60.00.[xx]

Este dispositivo es especialmente útil en transacciones en Internet. Este tipo de operaciones funcionan realizando una comprobación a través del NIP ingresado que es comparado con el que esta almacenado en forma segura en la tarjeta. Ver figura 2.8

Figura 2.8.CZAM-PC

Una desventaja de este equipo no evita la suplantación de identidad, es decir que si una persona logra tener acceso a la tarjeta y al NIP (ya sea por robo o por consentimiento propio) la seguridad queda comprometida nuevamente. A pesar de ello es que existen lectores asociados a la TI que permiten con toda seguridad comprobar que la persona que se encuentre realizando determinado operación sea realmente quien dice ser como se verá con el siguiente dispositivo:

II.1.4.3. Lectores Biométricos

Aunque el uso de estos dispositivos puede llegar a sonar una exageración casi rayando en la paranoia, no es este el caso. Estos dispositivos permiten la rápida y efectiva identificación de personas sin sacrificio de seguridad aunque con un precio algo alto (aproximadamente USD $1000[xxi]) aunque no tanto si se considera su casi invulnerabilidad.

- **LECTORES DE HUELLA DIGITAL:** Este tipo de lectores son los más conocidos dentro de los dispositivos biométricos. Aunque existen algunos de estos que no utilizan una interfase que permitan a la TI

interactuar con este, no se hablará de ellos en esta sección debido a que el lector para este proyecto solo es un dispositivo asociado y no el foco principal sobre el que deberá estar basada todo el sistema.

Existen diversas variedades de estos desde los utilizados para acceso a áreas restringidas como pueden ser bancos o laboratorios hasta elementos muy simples que se pueden usar para Internet.

Un ejemplo de este tipo de lectores se puede apreciar en la figura 2.9

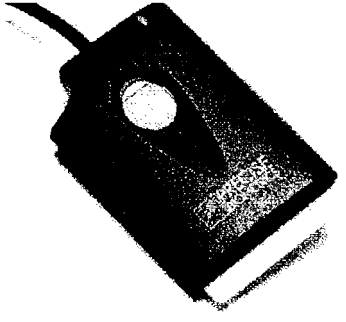


Figura 2.9. Lector de TI mediante Huella Digital [xxii]

Estos lectores poseen diversas características dependiendo de qué tantos servicios requiramos; desde solo verificar y registrar la asistencia hasta reportes personalizados sobre las operaciones incluyendo el tiempo desperdiciado y mucho más.

El tipo de conexión que utiliza esta clase de equipos va desde comunicación serial y paralelo hasta USB. Para el ejemplo de la figura 2.9 es necesario el uso de un host u dispositivo que procese la huella, para realizar el proceso de identificación aunque, existen aquellos que no lo necesitan.

No importando cuantos servicios ofrezca cada lector; el proceso para la validación del usuario es en esencia muy sencilla. La huella se encuentra almacenada en la tarjeta en forma segura (cifrada), al momento de introducirla al lector y colocar nuestra huella sobre este se realiza una comparación entre ellas admitiendo o rechazando al usuario.

Entre las principales ventajas de estos dispositivos están:

- Sensores Independientes.
- La verificación biométrica se realiza dentro del chip.
- Los datos no dejan el chip.
- La tarjeta misma cambia el estatus de seguridad. Esto significa que se auto bloquea.

II.1.4.4. Características físicas de lectores

Por supuesto los lectores también tienen que cumplir con las normas ISO, aunque estas como se dijo anteriormente deben ser utilizadas a escala mundial; también existe una excepción llamada Estándar Nacional Francés o AFNOR el cual coloca el chip de la tarjeta en otra posición. Debido a esto algunos lectores deben ser construidos y equipados con dos cabezas lectoras, auque este estándar se encuentra en un periodo de transición por lo que no se piensa que dure mucho esta característica en los lectores.

Cuando una TI es insertada en un lector que este conectada a otro dispositivo(a este también se le conoce como host), ya sea una PC o uno especialmente diseñado para este, se conecta vía un conductor energizándolo, entonces la tarjeta debe ser detectada a través de un micro switch o una celda fotoeléctrica.

Todo este proceso entre la tarjeta y el lector se realiza a través de los contactos de la tarjeta que es la laminilla que se observa a simple vista de la tarjeta, como se observa en le diagrama 2.11[7]

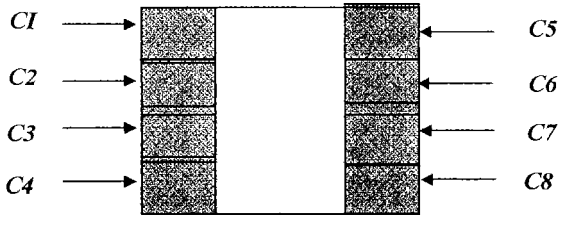


Figura 2.11. Diagrama de contactos de TI

Cada uno de estos contactos se encuentran establecidos por el estándar ISO 7816-2 como se describe en la tabla 2.12

CONTACTO	DESCRIPCIÓN	FUNCIÓN
CI	Vcc	Alimentación
C2	RST	Reset
C3	CLK	Frecuencia
C4	RFU	Reservadas para futuras acciones
C5	GND	Tierra
C6	Vpp	Voltaje Externo de Programación
C7	I/O	Entrada/Salida para comunicación
C8	RFU	Reservado para uso futuro

Figura 212. Estándares ISO para contactos de una TI

[7] Este esquema es sólo un ejemplo de un tipo de tarjeta. El esquema puede variar de fabricante a fabricante

II.1.5. Terminales

A diferencia de los lectores, las terminales para TI son mas sofisticadas en cuanto a su funcionamiento e interacción con la tarjeta ya que están conformados por lo que contiene una computadora aunque con sus características reducidas.

La principal diferencia entre los lectores y las terminales es que a los primeros se les considera como dispositivos "tontos" ya que no pueden hacer nada por si mismos sino que dependen de un host. En cambio las terminales al poder incorporarles instrucciones programadas, son capaces de procesar las tarjetas con solo introducirlas y realizar múltiples transacciones por lo que también se le conocen como POS o puntos de venta.

Esta descripción de POS no significa que solo se dediquen al comercio, por venta se pude entender cualquier operación a que realice sobre la tarjeta tal como puede ser una operación con vales o una validación criptográfica.

Las POS pueden funcionar en uno o en ambos de los siguientes modos:

- **En línea**: Esto significara que el dispositivo se encontrará completamente dependiente de un sistema que administre y autorice cada uno de sus procesos. Un ejemplo práctico que aunque no usa un chip inteligente si actúa sobre uno, es un cajero automático.
- **Fuera de Línea**: La terminal no necesita de un proceso que la supervise, es decir con sólo introducir la tarjeta la misma terminal es capaz de realizar las peticiones pertinentes.
- **Híbridas:** Pueden realizar ambas actividades aunque no al mismo tiempo dependiendo de la forma en que hayan sido programadas.

A diferencia de las tarjetas que poseen una estructura muy similar, las terminales varían de acuerdo a las necesidades para las que se usen. Una distinción se encuentra por ejemplo entre terminales móviles y estacionarias.

- Las estacionarias se alimentan de una fuente de energía fija y dedicada en exclusiva para esta como puede ser un eliminador o una pila.

- En cambio las móviles aprovechan la energía que les proporciona el dispositivo al cual estén conectadas, como puede ser una terminal que se encuentre a bordo de un sistema de transporte. Todas las terminales para TI poseen su propia pantalla para mostrar la evolución de las diferentes transacciones, así como un mini teclado para poder interactuar con ella.

Algo que si comparten todas las terminales existentes es la existencia de un microprocesador el cual dependiendo de su capacidad será mas o menos rápida y con mas o menos funciones.

El tiempo de vida de una terminal varia bastante ya que estas deberán soportar condiciones de humedad y temperatura cambiantes.

II.2 Tarjetas Inteligentes sin Contacto o "Contact Less".

II.2.1. Un poco de historia.

De los pocos elementos que una tarjeta inteligente de contacto tiene en su contra es que para que realice sus funciones es que necesita estar insertada ya sea en un lector o terminal. Esta acción provoca bajo algunos escenarios (como es el transporte público) retrasos que pueden ser inaceptables para determinada actividad en la cual su uso de la velocidad es esencial.

Para estas situaciones se ha desarrollado una rama de las TI que no necesitan de estar fisicamente unidas a algún dispositivo para poder funcionar, es decir las Tarjetas Sin Contacto o más comúnmente llamadas "Contact Less"(CL).

Aunque comparten ciertos aspectos con Tarjetas Inteligentes de Contacto (TIC) su funcionamiento varia sobre todo en su forma de comunicación la cual se realiza por medio de radiofrecuencia y en cómo fueron creadas.

La tecnología en que se basan las CL se remonta a esfuerzos por parte de los ingleses (en la Segunda Guerra Mundial para identificar sus aviones que regresaban de los bombardeos) el cual se realizaba por medio de identificación por radiofrecuencia o RFID, pero no fue sino hasta 1977 que se hizo publica y disponible para el público. El primer uso de esta tecnología en el plano civil fue la localización de ganado colocándole etiquetas con RFID.

Fue a principios de 1980 que la tecnología de radiofrecuencia (RF) comenzó a reducirse y éste fue usado para identificación de empleados insertándolos en sus tarjetas de identificación.

A lo largo de los años se aplicó de muy diversas maneras para el rastreo desde el salmón hasta camiones de carga, pero no fue sino hasta 1986 cuando se usó para tarjetas con microprocesador o MCU.

La primera CL que se creó funcionaba a 300 kHz una frecuencia muy baja considerando las actuales tarjetas que suelen usar una frecuencia de 13.56 Mhz, aunque existen en la actualidad tarjetas que funcionan a 125kHz que son las que se usan para controles de acceso. Esta tecnología de TI fue la base para el desarrollo para los estándares ISO de las CL.

La siguiente generación de las CL fue una híbrido (o dual) de dos chips, uno sin contacto y uno con contacto que posteriormente fueron integrados en uno solo. En estas primeras versiones el procesador necesitaba una alimentación de energía a través de los contactos. A diferencia de esto, la memoria usaba de 5 a 10 veces menos y se alimentaba por medio de la señal de radiofrecuencia.

Al no tener una alimentación adecuada este tipo de tarjetas no ofrecía el mismo nivel de seguridad que las tarjetas de solo contacto.

Conforme los avances en las tecnologías permitieron al procesador recibir energía a través de la señal de radiofrecuencia las CL permitieron el uso de las mismas prestaciones que las de contacto.

En la figura 2.14 se puede apreciar la evolución de las tecnologías de Cl en comparación con sus usos:

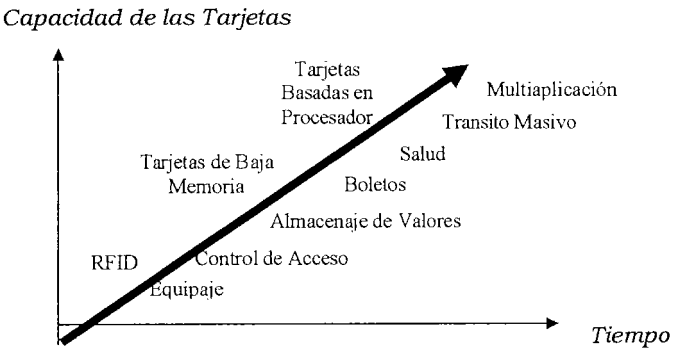


Figura 2.14. Avances de las Tarjetas Inteligentes sin Contacto

II.2.2. Características físicas y Capacidades de las CL

La estructura interna y funcionamiento de una CL aunque en algunos puntos similares a las de contacto (como pude ser el uso de un microprocesador y memoria) expone ciertas particularidades que deben ser vistas más minuciosamente.

Dependiendo del tipo de tarjeta la distancia a la que el chip puede trabajar es de 80 cm. e incluso en muchos casos no necesita siquiera ser sacada de la billetera. Y puede realizar diversas operaciones al mismo tiempo.

Existen diversas tecnologías para el uso de CL como son:

- **125 Khz**

Es una tecnología para usos de sólo lectura (sobre la tarjeta) y es usada por muchos de los sistemas de control de acceso existentes. Sus características permiten la transmisión de un número único para ser trasmitido en forma segura para ser utilizado por un sistema externo. Este sistema determina los derechos y privilegios asociados al portador de esa tarjeta. Entre otros usos esta el de control de animales.

- **ISO 14443 Y ISO 15693**

Este tipo de tarjetas al seguir estos estándares les permite el uso del nombre de Tarjetas Inteligentes de Lectura / Escritura y que permiten el almacenamiento de diferentes tipos de datos.

Las tarjetas que siguen estos estándares permiten determinar el apropiado nivel de acceso, todo esto a través del mismo procesador. Estos tipos de tarjetas adicionales incluyen factores de identificación como pueden ser elementos biométricos y NIPS's y otras tecnologías incluyendo a aquellas de contacto satisfaciendo los requerimientos de aquellas situaciones en las que la combinación de diferentes técnicas sean necesarias[xxiii].

El estándar ISO 14443 especifica la comunicación (transmisión, anticolisión y selección) en tarjetas cuyo alcance máximo es de 10 o mas y el ISO 15693 se usa tanto para tarjetas en la que su distancia de uso es de 50cm a un poco más de un 1 m y es posible usarla con solo pasar caminado junto al lector[xxiv].
Además de la utilización de los dos estándares previamente definidos, existe otro que es el ISO 7816.

Este estándar define muchas características físicas incluyendo el tamaño de la tarjeta, su fortaleza mecánica y sus propiedades eléctricas dentro de las tarjetas MIIFARE las cuales fueron creadas por Philips (entre otras como Atmel, ST, entre otras) y ocupan cerca del 91% del mercado[xxv]. Entre sus usos principales se encuentra el control de acceso, transporte y rastreo de equipaje[xxvi].

Este tipo de tarjetas usa una frecuencia de 13.56 Mhz.

La transmisión y recepción de información se realiza por medio de una antena que va embebida dentro del mismo plástico, esta pude tener de 3 a 5 vueltas de alambre o una tinta conductora conectada al chip ya sea de memoria con microprocesador, esta estructura se pude observar en la figura 2.15

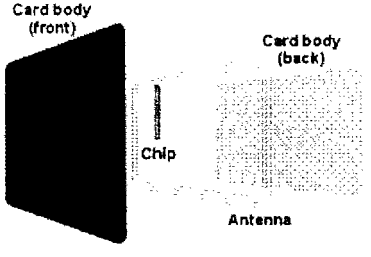


Figura 2.15. Estructura Interna de una Tarjeta sin Contacto

II.2.3. Tipos de Tarjetas CL

Existen tres tipos de tarjetas sin contacto

II.2.3.1. Memoria

Las tarjetas CL de memoria usan el chip para almacenar información de autentificación. En su forma más segura estas tarjetas pueden contener un número serial único e incluye la habilidad de asegurar permanentemente secciones de memoria o permitir escribir por medio de una palabra clave. Además de esto no existe ninguna otra prestación en cuanto

a seguridad tales como encriptación de datos el cual debe ser realizado por medio de mecanismos externos a la tarjeta.

II.2.3.2. Wired Logic

Contienen un circuito especifico que es usado para autentificar por si mismas que los lectores y/o terminales con los que interactúa sean validos, además que permite encriptar comunicaciones

II.2.3.3. Microcontrolador (MCU)

Este tipo de tarjetas permiten implementar autentificación y encriptación de datos. Pero no solo eso sino que también permiten ejecutar sus propias funciones para la seguridad como son características biométricas y firma digitales. Además permiten el uso de diversos sistemas operativos[xxvii].

Este tipo de tarjetas se subdividen además en:

- **HÍBRIDA**

Este tipo de tarjetas contiene dos chips cada una con su respectiva interfase. Cada uno de estos no permite la comunicación entre ellos por lo que es necesario el uso de lectores de ambos tipos y ser utilizados en forma independiente.

A pesar de esto algunas aplicaciones en que se requiere el uso de las ventajas de mundo de contacto y sin contacto es bastante útil además de que su precio es un poco más accesible en comparación con aquellas en las que es posible compartir información entre tecnologías con y sin contacto.

- **COMBI**

También conocida como dual, este tipo de tarjeta posee una interfase (aunque existen algunos tipos que poseen su propia interfase) compartida. Gracias a esto es posible que ambos chips puedan comunicarse entre si[xxviii]. Su estructura se puede observar en la figura 2.17

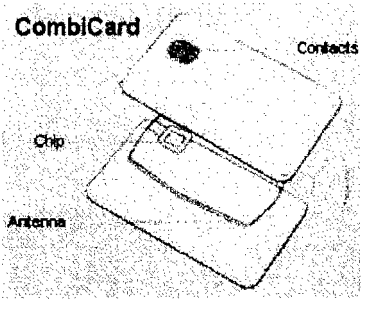


Figura 2.16. Estructura de una Tarjeta Combi

Esto es especialmente útil para el caso de monederos electrónicos, rastreo de equipaje y boleto electrónico como lo hizo la aerolínea alemana Lufthansa.

De los posibles inconvenientes son que le precio es significativamente mayor a una tarjeta Híbrida.

II.2.4. Lectores y Terminales para CL

A continuación se describirán algunas de las características de los dispositivos utilizados para interactuar con las tarjetas sin contacto

II.2.4.1. Lectores

Al igual que los lectores para tarjetas de contacto los lectores se utilizan para realizar la interfaz entre un host y la tarjeta. A pesar de ello existen ciertos tipos que poseen cierta autonomía para realizar algunas operaciones por si mismos pero la característica de toma de decisiones se enfoca hacia terminales.

A semejanza de los lectores para tarjetas de contacto, en las CL también existen diversos tipos de lectores dependiendo de nuestras necesidades los cuales deben seguir los protocolos 14443 y 15693.Un ejemplo de estos son:

- **Lectores de Control de Acceso:** Como su nombre lo indica restringen y/o registran el acceso a determinados lugares entre los cuales se encuentran los llamados lectores biométricos

- **Lectores de Interfase:** Este tipo de lectores se utiliza para la conexión directamente a un procesador

Dentro de los tipos de conexiones que se usan para interactuar con estos lectores se encuentran

  - **RS232**
  - **Paralelo**

II.2.4.2. Terminales

A diferencia de las tarjetas de contacto no existe una gran variedad de terminales ya que su costo lo hace prohibitivo, además de que su uso se encuentra orientado a aplicaciones muy especificas en los que requiera de validaciones muy estrictas pero de una manera portátil. Un ejemplo de estas se encuentra en la figura 2.18[xxix]

Figura 2.17. Terminal Lectora de Tarjetas sin Contacto

II.2.5. Sistemas Operativos de Tarjetas (S.O)

Aunque un S.O de una tarjeta pueda parecer alejado a la percepción habitual de un sistema operativo (S.O) de una computadora, en realidad no lo es tanto ya que después de todo este no es mas que un conjunto de instrucciones que permiten la interacción de diversos componentes lo cual aplica tanto para una PC como para una tarjeta.

Una condición agregada a esto es que la estructura de un S.O dependerá en forma critica del fabricante de la tarjeta ya que algunos de ellos aplican una versión pragmática en donde lo principal es que el S.O cumpla con el trabajo. En cambio existen otros apegados a una estricta metodología.

II.2.5.1. Historia

Los primeros programas para un sistema operativo de TI, que se comenzaron a desarrollar alrededor de 1980, no eran en absoluto parecidos a los actuales sino que más bien un conjunto de instrucciones almacenadas en una memoria ROM y con un propósito especifico es decir que eran elaborados con sólo un objetivo el cual podía ser desde decrementar un número para alguna agrupación bancaria hasta autentificar un NIP de una empresa gubernamental, pero no más que eso es decir que no podían ser modificadas.

El desarrollo de los S.O como tales puede ser ilustrado con la red celular en Alemania. La tarjeta usada por la compañía C-Networks en 1987 que a pesar de ser creada en específico para este uso al igual que sus antecesoras, permitía el uso de comandos y protocolos de transmisión específicos así como una estructura de archivos hecha a la medida[xxx].

El siguiente paso fue una transición de S.O específicos aquellos de propósito general y un ejemplo de ello fueron los llamados primeros GSM[xxxi8], cuya estructura era significativamente mas abierta. Este tipo de estructura permitía el agregado de aplicaciones propiamente dichos.

No fue sino hasta 1996 la compañía Schlumberger introdujo la primera tarjeta que aceptaba correr programas mediante algunos lenguajes de alto nivel tales como Java

II.2.5.2. Características Básicas de S.O

- **De Contacto**

En contraste a los sistemas operativos convencionales para los de las TI no es posible utilizar un medio de almacenamiento externo además de que no posee una interfaz para el usuario. La prioridad es la ejecución segura de un programa y la protección a los datos existentes.

Debido a las restricciones de memoria existentes la cantidad de código que puede ser almacenado dentro de una tarjeta es muy limitada. Por ejemplo los módulos principales

[8] Global System for Mobile Communications

son almacenados en la memoria ROM. Debido a esto es que ninguna otra modificación puede hacerse al S.O después de su fabricación, o por lo menos es muy difícil ya que sólo el mismo fabricante podría hacerlo a un costo muy alto y con un tiempo de dilación de 10 a 12 semanas.

Todo esto provoca que el tiempo invertido en pruebas y control de calidad sea mucho más elevado que el programa en si, además que de que debe extremadamente estable y robusto, es decir que caídas del sistema deben de encontrarse severamente controladas.

A pesar de esto, existen por supuesto errores que solo se podrán observar en su fase de implementación como sucede en cualquier sistema.

Un diseño estrictamente modular contribuye en forma crucial a la detección y corrección de errores durante la fase de implementación. Una ventaja importante de esta modularidad es el hecho que si el sistema cae generalmente la seguridad no queda comprometida ya que el daño se limita solamente a su localidad.

El procedimiento usual en el diseño es llamado modulo-interfase. En este las tareas de sistema y aplicaciones son descompuestas en funciones tanto como sea posible y estas encapsuladas en módulos, los cuales pueden ser asignadas a una persona para su programación (el cual por cierto se realiza en código ensamblador) lo cual minimiza en gran medida el código a realizar y probar.

Un aspecto importante de la arquitectura de estos sistemas es que no existe la opción de ejecuciones multiproceso debido a las limitaciones del hardware y conceptos asociados a la seguridad. Una desventaja inherente a esto es que no permite el uso de funciones que puedan supervisar diversos aspectos de la operación.

En resumen los S.O de las tarjetas inteligentes de contacto cumplen con las siguientes tareas:

- Trasmisión de Datos desde y hacia la tarjeta
- Control de la ejecución de Comandos
- Administración de los datos
- Administración y ejecución de los protocolos criptográficos

Para los S.O también existen normas ISO que regulan la forma en que los comandos que se envían hacia la tarjeta y este es 7816 el cual indica que la estructura de cada comando (al cual se le conoce como APDU o Aplication Protocol Data Unit) y posee una estructura básica la cual utiliza dos diferentes tipos de parámetros.

Los primeros son los llamados parámetros obligatorios que se usan no importando la acción a realizar o comando utilizado y que son:

- **CLA o Clase de Instrucción**: Identifica una categoría de comando
- **COD o Código de Instrucción**: Especifica la instrucción para el comando

- **PI P2 o Parámetros 1 y 2**: Usado para proveer información extra a la instrucción

Además se encuentran los llamados parámetros opcionales. Este tipo de parámetros se utilizara o no dependiendo de la instrucción

- **LC**. Especifica la longitud del campo de datos
- **Campo de Datos:** Contiene datos que son enviados a la tarjeta para ejecutar la instrucción
- **LE**: Especifica el número de bytes esperados

- **Sin Contacto**

A diferencia de las tarjetas de contacto para las CL no existe un estándar para la estructura de los comandos que se le envían a la tarjeta por lo que cada fabricante realiza su propia definición.

Ente los S.O mas conocidos dentro del mercado se encuentran los de Starcos Air, Multos y CyberFlex. Todos ellos pueden manejar tanto la parte de contacto y la de sin contacto para el caso de tarjetas duales.

II.2.6. Estructura para Tarjetas de y Sin Contacto.

Independientemente a los diferentes mecanismos que operan para la autentificación e identificación en las TI, la función principal de estas es el almacenaje de información.

II.2.6.1. Tarjetas de Contacto

La forma en que esta es almacenada es muy similar a las estructuras de árbol a las que estamos acostumbrados con carpetas y archivo con la diferencia de que aquí no existe una interacción entre hombre y máquina sino sólo entre máquinas. Los nombres de los archivos son identificados por números hexadecimales.

Cuando un archivo es borrado (una característica que la mayoría de los S.O de las TI no posee salvo las más avanzadas) esto no significa que su lugar pueda ser ocupado por otro. Todos los archivos son usualmente creados durante la fabricación o en la personalización por lo que las modificaciones van encaminadas hacia el contenido del archivo

Los S.O actuales poseen la característica que toda la información referente a sus archivos se encuentra almacenada dentro del mismo archivo. La forma en que están constituidos se divide en dos partes. La primera conocida como cabecera contiene los datos acerca de la estructura y condiciones de acceso y el cuerpo el cual es asociado mediante un puntero, contiene los datos en si mismos. Ver figura 2.18

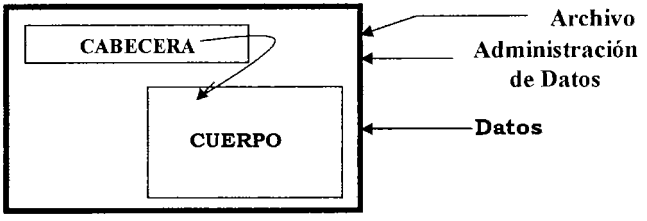


Figura 2.18.Estructura de un archivo en una TI

Como una mejora las cabeceras y los cuerpos de los archivos se almacena en lugares diferentes de la memoria. De esta forma si algún error ocurriera al escribir los datos este no podría afectar alas condiciones de acceso del mismo.

- **Tipos de Archivos**

La estructura del sistema de archivos así como cada parte de la tarjeta se basa en un estándar ISO, que en este caso es el ISO 7816-4 y como ya se comentó anteriormente sigue una estructura de árbol, que esta constituido por:

- ***Archivo Maestro (MF)***

Se trata del directorio raíz al cual se ingresa inmediatamente en le momento de energizar la tarjeta. Este contiene toda la estructura (o estructuras) que se planeen colocar en la tarjeta.

- ***Archivos Dedicados (DF)***

Estos directorios se usan para separar y clasificar las diferentes aplicaciones dentro de una tarjeta y a sus diferentes archivos. En teoría pueden anidarse el numero de DF que se desee pero en la practica el limite de la memoria restringe su numero

- ***Archivos Elementales (EF)***

Este es el nivel final de la estructura. Estos se utilizan para el almacenamiento de diferentes tipos de datos. También pueden usarse tantos como la memoria lo permita. Agregados a estos últimos se definen archivos que sirven para el control de las aplicaciones tanto a nivel seguridad (manejo de llaves criptográficas) como en el ámbito administrativo. Estos archivos se encuentran especialmente resguardados por el sistema operativo. En la figura 2.20 se puede apreciar las posibles estructuras en una TI.

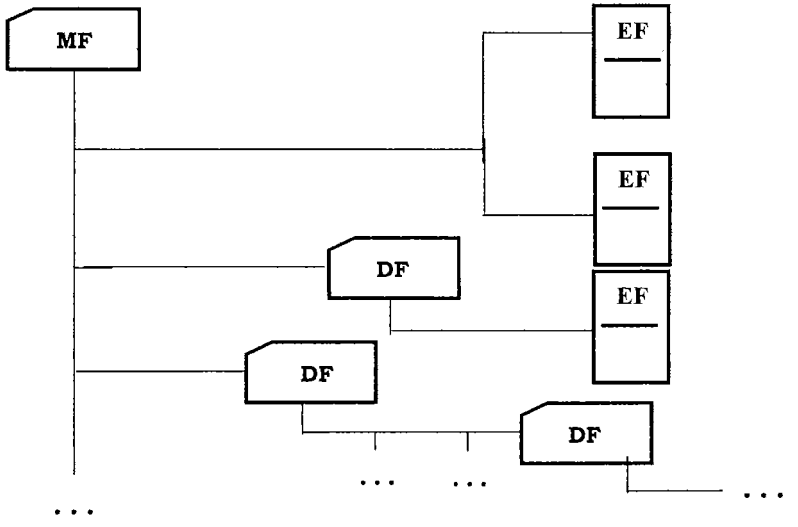


Figura 2.19. Distribución Lógica de los archivos dentro de una TI

Para los EF existen diversos atributos para definir las propiedades del archivo. Entre algunos de estos existen los permiten colocarlos como de solo lectura otros que almacenan valores como llaves criptográficas que no pueden ser leídos una vez definido el valor de estas, otro que pueden ser usados sólo a través de una NIP etc. Sin embargo, esto depende del sistema operativo que contenga la tarjeta.

II.2.6.2. Tarjetas Sin Contacto

A diferencia de las tarjetas de contacto dentro de las tarjetas sin contacto no existe un estándar definido para el almacenamiento de información.

A pesar de esto y en consecuencia por la competitividad dentro del mercado, si existe un estándar llamado MIFARE el cual fue creado por la compañía Philips para la operación de tarjetas CL. Este estándar se usa para áreas tan diversas como controles de acceso y pago electrónico.

Otras características que involucran este estándar son

- Es una tecnología comprobada alrededor del mundo en diferentes situaciones que van desde control de acceso hasta el uso en sistemas de transporte masivo
- Siguen los estándares ISO, pero sobre todo que usa el 14443-A que tiene las de ventajas:
  - Una mayor velocidad de respuesta
  - Una mayor inmunidad contra el ruido

- Más simple de implementar[xxxii]
- Su uso abarca cerca del 91% del mercado[xxxiii].

El estándar que se desarrollo para MIFARE, el cual a su vez respeta el ISO 14443, es usado por diferentes fabricantes

Las tarjetas MIFARE se encuentra compuesta por 16 sectores, de los cuales el primero se utiliza comúnmente para almacenar el directorio el cual se conoce como Directorio de Aplicaciones MIFARE (MAD), y los restantes 15 pueden ser utilizados para aplicaciones de monedero o para almacenamiento en general.

Así mismo cada sector posee una llave A y B mediante los cuales se otorgan privilegios de acceso. Este par de llaves pueden ser definidas como de lectura y lectura /escritura o como decremento y decremento / incremento. Un ejemplo de este ultimo podría ser en un torniquete de acceso que mediante la llave A se deduzca de un sector determinado y mediante la llave B se incremente en otro al llegar a una taquilla.

Las llaves MIFARE son esencialmente contraseñas numéricas usadas para controlar el acceso de los sectores.

La estructura MIFARE además posee un número aleatorio único de 32 bits el cual es granado en forma inalterable por el fabricante. Este es llamado Numero Serial de Tarjeta (CSN) o Identificador Universal (UID) y puede ser leído por cualquier lector sin poner en riesgo ninguna llave almacenada.

Pasando a un nivel más profundo cada sector se divide a su vez en cuatro bloques numerados del 0 al 3.

- En el bloque 0 del sector 0 se encuentra él ID de 32 bits y no puede ser modificado. En los restantes bloques cero si se pueden almacenar datos.
- En los bloques del cero al 2 (sin contar el primer sector) se usa para almacenar datos.
- En el bloque 3 (o cabecera de sector) contiene las llaves y condiciones de acceso para todos los bloques incluyéndose a si mismo y sólo hay un par de llaves por sector.

Dentro de las condiciones de acceso estas pueden ser únicas para cada bloque(0-3).

Estas condiciones son expresadas por un numero binario de 3 bits (000-111) con lo cual se permite hasta 8 diferentes posibles formas de configurar los bloques.

Las condiciones de acceso almacenadas en la cabecera de sector pueden ser permitir o impedir que los datos sean leídos o escritos usando una o ambas llaves.

Ahora dentro de los bloques los valores que se pueden almacenar en estos se componen de:

- 4 Bytes de Información de Dirección.

- 4 Bytes de Valores de Datos.
- 4 Bytes para el complemento de los valores de datos
- 4 Bytes para los valores de datos repetidos.

Los valores de datos son almacenados tres veces en un bloque para permitir detecciones de errores y capacidad de corrección

II.2.7. Descripción comparativa

El uso de la TI marca la vanguardia en cuanto a servicios y prestaciones para la seguridad y velocidad de ciertos procesos como se ha venido describiendo en este y el capítulo anterior. A partir de esto se podrá observar mas claramente el porque el uso de las TI es la tecnología mas adecuado para el proyecto que nos ocupa.

Ahora bien dentro del mercado actual existen tecnologías que han sido igualmente usadas por mucho tiempo y con resultados comprobables y que se utilizan para el manejo de procesos en una forma eficiente.

En la tabla 2.21 se mencionan algunas de estas tecnologías junto con sus limitantes en comparación con las Tarjetas Inteligentes.

	Código de Barras	Banda Magnética	Tarjetas de Memoria	Tarjetas Inteligentes
Tecnología Madura	SI	SI	SI	SI
Costo	Relativamente Bajo	Caro, por la toda la infraestructura necesaria, aunque el costo en si de la tarjeta es muy bajo.	Bajo	Dependerá del alcance que se le pretenda dar.
Seguridad	De Bajo a Medio. Dependerá del control de las mismas	Bajo	De Medio a Alto	Alto a muy Alto
Capacidad de Almacenaje	De Bajo a Medio. Hasta 1028 bytes[xxxv].	Bajo. Aproximadamente 134 kbytes[xxxvi] de dependiendo del numero de tracks	Aproximadamente de 12bytes a 20kb	Puede llegar hasta a un 1 MB[9]
Capacidad de Procesamiento	No	No	No	Si
Capacidad de Modificación	No	No	Si	Si
Multiaplicación	N/A	No	No	Si

[9] Ver sección 1.3 del capítulo 1

Ejemplos de Aplicaciones	Identificación de productos, Control de Asistencia	Control de Acceso, Pago Electrónico	Tarjetas Telefónicas	Múltiples que van desde monedero electrónico hasta control de acceso y transporte, incluyendo aplicaciones creadas en forma especifica

Figura 2.20. Tabla Comparativa de tarjeta de Identificación

Capítulo III. Elementos de las Multiaplicaciones

Objetivo
Ya que el lector se encuentre instruido en las características elementales de las tarjetas y su usos, se introducirá al mismo dentro del área que será el elemento clave que administrará y controlara la información dentro de la tarjeta: La Multiaplicación. Así mismo se dará una breve hojeada a la contraparte de la tarjeta, aquella que servirá de interfaz entre el usuario y la tarjeta. Las Terminales que a diferencia de un simple lector son mucho mas complejas, es por ello que merecen una sección especial. Además de que se realizará un recorrido a través de la seguridad en las tarjetas

III.1 Descripción de una multiaplicación.

III.1.1. Descripción

Una definición simple de lo que es una multiaplicación es que se trata de una representación de un producto o servicio en una tarjeta. Dentro de esta definición se incluye que cada una de estas aplicaciones puede ser capaz de comunicarse o no con sus compañeras, esta comunicación dependerá de las necesidades del cliente.

III.1.1.1. Tipos de Multiaplicaciones.

Existen tantos tipos de aplicaciones como necesidades para ellas, pero dentro de los mas utilizados se encuentran

- **Banca y Finanzas.** Envuelve operaciones para crédito, debito y monederos electrónicos.
- **Transacciones en Red.** Incluye operaciones tales como teléfonos móviles, televisión de paga y acceso y autentificación en la red.
- **Transporte y Control de Acceso.**
- **Tarjetas de Gobierno.** Se incluye tarjetas de identificación, Tarjetas de Salud y Licencias de Manejo[xxxvii].
- **Lealtad:** Permite proporcionar a determinada institución o empresa que sus usuarios se beneficien a partir del uso de la tarjeta y al mismo tiempo al emisor lograr que los usuarios utilicen sus servicios en lugar de los de la competencia
- **Comunicaciones Móviles Digitales:** Los teléfonos móviles que utilizan las redes "Global System for Mobile Communication" (GSM) han de equiparse con una tarjeta inteligente para identificar al usuario.
  Esta tarjeta, denominada " Subscriber Identification Module " (SIM) puede ser una tarjeta de tamaño normalizado (norma ISO) o una versión para insertar que consta sólo del chip rodeado de unos pocos milímetros de plástico.

El SIM es unívoco para cada usuario individual y se puede transferir de un teléfono a otro, dándole la misma identidad y el mismo número de teléfono asignado al suscriptor.

- **Sector Financiero:** Zolotaya Korona es uno de los mayores sistemas de pago bancario con tarjeta inteligente, que ha operado en Rusia con 120 bancos, 200.000 tenedores de tarjetas y 100.000 transacciones semanales en el último año y medio. El sistema comprende 4.500 puntos: terminales de venta, cajeros automáticos, terminales de autoservicio y sucursales bancarias

- **Transportes:** La Unión de Autobuses de Seúl, que agrupa a 89 compañías de autobuses, es actualmente el mayor usuario mundial de tarjetas inteligentes sin contacto. En sus 8.700 autobuses se utilizan estas tarjetas y se han instalado unos 1.700 puntos de recarga. Para principios de enero de 1997 el número de tarjetas de autobuses emitidas en Seúl habrá llegado a 2,5 millones, con unos dos millones de transacciones diarias[xxxviii].

Algunos más se pueden observar en la figura 3.2

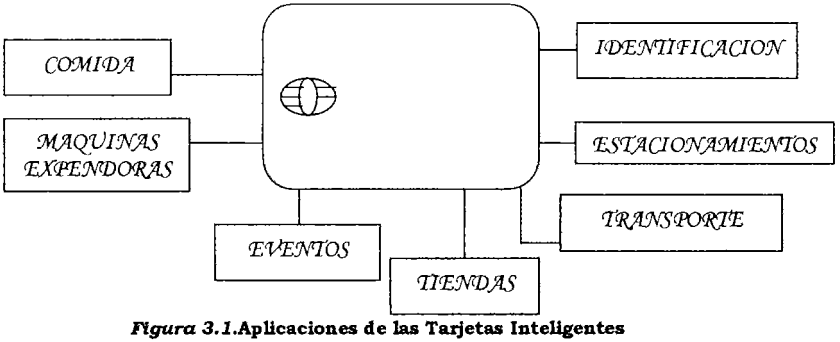


***Figura 3.1.*Aplicaciones de las Tarjetas Inteligentes**

III.2 Consideraciones de Seguridad y Criptografía en TI.

III.2.1. Introducción

Como se ha venido diciendo una de las principales ventajas de las TI comparada con otros dispositivos tales como banda magnética es la seguridad

III.2.1.1. Consideraciones de seguridad para sistemas con TI

La seguridad que se debe considerar sobre un sistema que utilice las TI no sólo depende de la tarjeta en si misma, (que si es un punto vital y sobre el cual se comentara más adelante) sino de todo lo que interactúa con ella e incluso aquellos elementos que se podrían determinar éticos que pueden afectar su uso no por efectos técnicos sino más bien operativos.

Por ejemplo uno de ellos es que la tarjeta deberá contener la mínima información posible, pero de forma tal que pueda formarse un rastro de las actividades del usuario de la tarjeta, claro que solo si la institución tiene la protestad de hacerlo como por ejemplo una institución bancaria en previsión de la resolución de algún asunto judicial.

Por supuesto que información sensitiva como la del caso anterior, deberá ser protegida para que sólo pueda ser accedida por las autoridades pertinentes. Es decir el usuario deberá ser enterado de cualquier operación que se realice con los datos almacenados y si estos son utilizados para cualquier manipulación externa ya sea por la misma institución o por alguna otra externa.

Es importante definir políticas tanto de lado del administrador para prevenir casos de abusos de poder como del usuario para detectar cualquier actividad inusual(como algún intento de fraude).

Englobado dentro de esta ultima cuestión se encuentra (como se ha visto en el capitulo 2) la TI comprende de una diversa variedad de protecciones que va desde la criptografía hasta el uso de huellas digitales y oculares en contraste con la banda magnética en la cual el único elemento cifrado es su numero de identificación.

Además de protección las TI dan la posibilidad de autentificación de la tarjeta y cuyos métodos se encuentran[xxxix]:

- ***Autentificación de usuario:*** La Persona que posee la tarjeta debe validar que es el propietario legitimo ya sea con un PIN o en casos más sofisticados con una huella digital.

- ***Autentificación de Transacción***: Confirmación de que una transacción es valida.

Otro asunto que es necesario considerar en los sistemas con TI es la seguridad del sistema en si mismo así como la de las bases de datos (en caso de las hubiera) que lo soportan.

Existen algunos de elementos que podrían fallar en un sistema como este, lo que lo convertiría en el elemento débil y por tanto el causante de una ruptura del mismo sobre todo donde los datos son enviados de una PC a otra, por esto se dice que la TI no es una panacea y es susceptible de ser comprometida si sus elementos tanto internos como externos no son correctamente configurados.

El reto es desarrollar técnicas rigurosas y arreglos administrativos que minimicen el riesgo de un uso no autorizado y de alguna revelación de alguna información personal o transaccional.

Existen algunas medidas prácticas para ayudar a incrementar la seguridad en un sistema de TI son:

- Diseñar arreglos apropiados de seguridad dentro de la tarjeta para separar aplicaciones en tarjetas multiaplicación definiendo diferentes

niveles de seguridad donde la información confidencial haya sido almacenada.

- Educar a la gente de operaciones en políticas de seguridad para prevenir un acceso no autorizado tanto de la información transaccional como la almacenada.
- Educar a los poseedores de las tarjetas acerca de los usos de las contraseñas(en caso de que las hubiera)

Los poseedores de las tarjetas deben tener el derecho de saber que información se mantiene en su tarjeta (por supuesto esto no incluye la información de seguridad de la misma tarjeta tal como llaves utilizadas para proteger la información). Esto se logra proveyendo de lugares específicos para que el usuario pueda consultarla.

Cabe preguntarse acerca la información referente a la seguridad (la posesión de los elementos que protegen la tarjeta). Pues bien es necesario llevar un control de todo el flujo de la información. Es conveniente que la obligación de proteger estos secretos no recaiga en una sola persona sino en varias esto para minimizar la tentación de abusos.

III.2.1.2. Elementos Lógicos de Seguridad

Dentro las TI, la criptografía es el principal frente que se tiene para proteger la valiosa información almacenada en ella, es por ello que se dará un breve vistazo a este concepto

III.2.1.3. Criptografía

El tema de criptografía es en extremo complejo al menos en el diseño de sus los algoritmos debido a que se utilizan matemáticas de muy alto nivel. Un elemento importante acerca de la criptografía utilizada en las TI es que aunque la criptografía no es el elemento más débil si podría convertirse en una falla si su implementación se realiza de manera incorrecta. Es decir la criptografía es necesaria para la seguridad pero no es suficiente[xi].

En la presente sección se describirán algunos elementos básicos de la misma lo cual nos permitirá comprender en sus elementos básicos como la información contenida en una TI es resguardada

- **Una breve introducción.**

El objetivo primordial de la criptografía, por un lado es mantener determinada información secreta la cual sólo deberá poder conocer el destinatario elegido, y por otro, asegurar su autenticidad.

Existen varios elementos que además del anterior ayudan a resolver la criptografía:

- **Integridad**. Se refiere a que la información no puede ser alterada al ser enviada, es decir que llegue tal como se envió. Dentro de las TI esto se aplicaría por ejemplo que al realizar una transferencia de fondos por determinada cantidad esta sea respetada por el monto que se definió.
- **Autenticidad**: Se refiere a que se pueda confirmar que el mensaje haya sido enviado por quien dice que lo envío ya sea un individuo o un

equipo. En las tarjetas estas pueden ser autentificadas por la terminal para verificar que sea una tarjeta valida y no un posible fraude.

III.2.1.4. Evolución de Algoritmos

Dentro de la criptografía existen dos tipos de vertientes

- **Criptografía de llave privada o Simétrica.**

En este tipo de criptografía existe sólo un tipo de llave con la cual son cifrados y descifrados los mensajes.

Aunque este tipo de algoritmo es el más rápido, ambas partes debe poseer la llave ya que si no es así el mensaje no podrá ser cifrado lo cual plantea el problema de transferencia de la llave ya que necesitaría realizarse en persona (involucrando perdida de tiempo) o por algún medio seguro (lo que implicaría un mayor costo) para transmitirla.

El proceso para este tipo de criptografía se observa en la figura 3.3

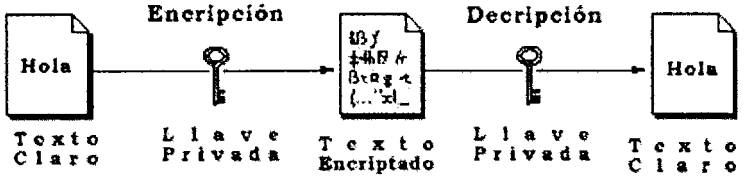


Figura 3.2. Mecanismo de Llave Simétrica

Como se observa en la figura 3.3 el proceso de cifrado necesita un texto claro(o texto plano como comúnmente se le conoce), el texto cifrado y la llave que se usa para pasar de uno a otro. Estos tres elementos se combinan mediante un algoritmo de cifrado.

Dentro de los más conocidos algoritmos simétricos se encuentran los siguientes:

- **IDEA**
- **DES**
- **TRIPLE DES**

Cada uno de ellos responde a diferentes necesidades dentro de la industria.

- **Criptografía de llave Publica o Asimétrica.**

Este tipo de criptografía apareció mas recientemente y consiste en que se disponen de dos llaves, una publica y una privada.

Ambas llaves se encuentran relacionadas pero la que se utiliza para encriptar es la publica y para descifrar es la privada. Ver figura 3.4

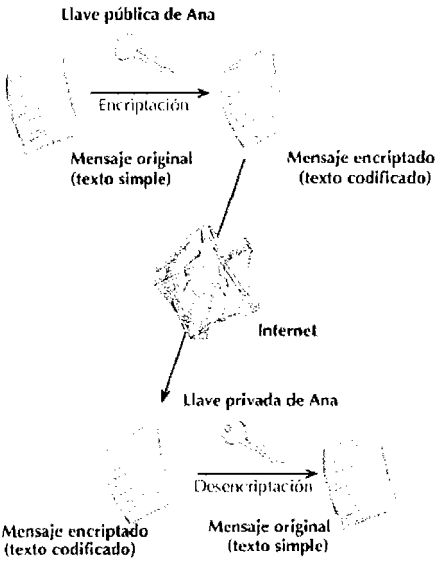


Figura 3.3 Proceso de Criptografía Asimétrica

Mediante este método no es necesario que la llave con la que se cifra deba viajar a través de un medio seguro (ya sea en persona o mediante una transmisión segura) ya que la llave publica utilizada para cifrar se encuentra disponible para todos.

La desventaja de este sistema es que utiliza mas recursos de procesamiento debido que utilizan matemáticas más complejas como son el manejo y factorización de números primos por lo que en este tipo de TI son mas caras.

El algoritmo mas usado dentro de las TI es el RSA, aunque existen algunos que también se utilizan dependiendo del fabricante como son:

- Montgomery (utilizado por los chips de Motorola)
- Waleffe and Quisquater (utilizado por los chips de Philips)
- Levy-dit-Vehel and Naccache (utilizado por Gemplus),
- Bucci y otras variantes de Barrett (usado por Amtec)
- Sedlak (utilizado por Siemens)[xli].

III.3. Administración de Llaves Criptográficas

III.3.1. Introducción

En un mundo ideal, las llaves que se utilizan dentro de un sistema de tarjeta inteligente para proteger su información siempre permanecerían a salvo del mundo exterior. Desgraciadamente esto no es posible en el mundo real. Es por ello que se recurre al proceso de incrementar él número de llaves

Por supuesto esta técnica no se aplicaría en todos los diseños con una TI, esto dependerá de la clase de sistema como por ejemplo no seria necesario en aquellos en los que la tarjeta permanece un corto periodo de tiempo.

III.3.1.1. Llaves Derivadas

Dado que diferencia de las terminales, las tarjetas se hallan totalmente expuestas a un ataque, es importante que la llave maestra utilizada para el cifrado no resida dentro de la tarjeta sino que en su lugar exista una derivación de esta.

La llave derivada es generada mediante un algoritmo criptográfico. Los datos de entrada son la propia llave maestra y una característica individual de la tarjeta tal como el número de tarjeta que es grabada en la misma durante su fabricación.

III.3.1.2. Llaves diversificadas

Para también minimizar las consecuencias de una llave comprometida se definen diversas llaves para cada función criptográfica.. Por ejemplo es posible distinguir una llave para mensajería segura, para cifrado o para autentificación, esto es cada operación tiene su propia llave maestra y a su vez su propia derivación.

III.3.1.3. Versiones de Llaves

Como regla no es suficiente dar a una TI durante su tiempo de vida una única llave. Considerando el caso en el que una llave maestra pueda ser comprometida por un intruso en forma externa esto podría causar la inmovilización del sistema completo, es por ello que en las últimas generaciones de sistemas de TI, estos son capaces de actualizar a nuevas generaciones de llaves.[xliii].

Capítulo IV. Utilización de lo Aprendido.

Objetivo
Una vez que se tiene una visión general de lo que es y lo que se puede hacer con una Tarjeta Inteligente el lector podrá comprender como cada una de las partes descritas en los capítulos anteriores se utilizarán para resolver la problemática en forma detallada

IV.1 Utilidades de la TI dentro de la ENEP Aragón.

IV.1.1. Introducción

Aunque a primera vista la TI inteligente podría usarse en multitud de aspectos, es importante considerar que los aspectos donde las diferentes prestaciones podrían ser útiles son aquellas donde la seguridad que ofrece dicha tecnología, no pueda ser reemplazadas por ninguna otra, es decir que la relación costo-beneficio sea conveniente.

El aspecto costo de esta relación podría parecernos que sería muy elevado debido a la variedad de elementos que participarían en un proyecto de este tipo, pero antes de concurrir hacia estas consideraciones se debe antes dar un vistazo mas a fondo.

Cada uno de los elementos que se han mencionado en los capítulos anteriores dependerán de la complejidad del proyecto que se pretenda alcanzar, ya que obviamente no es lo mismo establecer uno para 10, 100 o un 1, 000,000 de tarjetas.

Otro aspecto es que no debe ser visto en forma como un gasto sino mas bien como una inversión que va desde corto hasta largo plazo.

Nuevamente esto dependerá de qué tan extenso se requiera el proyecto, pero de acuerdo a este tenemos tres situaciones principales como son:

- El manejo del efectivo en todas las áreas donde se maneja este tiene un costo (el cual debe ser bastante elevado por cierto).
  Este puede ser significativamente reducido(sino es que eliminado) mediante el uso de diversas características de la TI y sus elementos asociados.

- Dentro de la biblioteca al retirar o entregar algún material el proceso para tal fin en ocasiones provoca el atraso de los alumnos ya que es necesario de un empleado para efectuarlo. Con la TI podría ser posible que incluso no sea necesario de demasiados empelados sino que el mismo alumnos realice su propio proceso de préstamo.

- El control de la asistencia de los maestros se realiza de una manera mediante la cual no es posible llevar registros y estadísticas confiables de la misma. Mediante la TI el registro se podría hacer de una manera automatizada y confiable.

Otros aspectos que se deben tener en cuenta son, que la TI no se debe ver orientada hacia un solo objetivo (o problema) en particular, sino que se debe existir la sinergia necesaria

entre cada uno de ellos ya que de otro modo se podría tener como resultado un desperdicio de sus capacidades.

Es por todo esto que los diferentes problemas (de los cuales se dio un avance en el capitulo 1), que a continuación se expondrán se encontrarán relacionados, aunque a primera vista no lo parezca.

Como se ha venido expresando en diversas ocasiones a lo largo de la presente tesis, este documento no pretende de ninguna manera definir en su totalidad cada aspecto de la solución a los problemas anteriormente enumerados, sino demostrar a través algunos prototipos, cómo sería posible poner en práctica un sistema mucho mas eficiente para cada una de las personas que estudian y/o trabajan en la ENEP Aragón en las diferentes áreas anteriormente expuestas.

A pesar de lo anterior, los modelos que se presentarán aunque en menor escala trabajarán en forma eficiente y si se integrarán en una escala mayor no deberían variar.

Ahora bien, antes de definir cualquier elemento tecnológico que deberá ser incluido dentro del sistema se debe analizar punto a punto los lugares donde este se implantaría ya que cada sección plantea requerimientos específicos que van desde la disponibilidad de la información hasta el tipo y cantidad de la misma (reportes y estadísticas).

Como para cualquier problema, lo primero para resolverlo es definir con precisión cada una de sus partes. Aunque en el capítulo 1 se vio una introducción a ellos a continuación se tendrá una concepción ampliada de ellos mostrando las oportunidades y beneficios de la TI dentro de la ENEP

IV.1.2. Pago de Servicios

En la actualidad el manejo de efectivo dentro de la ENEP Aragón se maneja a través de la caja que se encuentra en la institución. A través de esta se realizan la mayoría de los pagos de los servicios que presta la escuela con la excepción de algunos elementos como las fotocopias que son pagadas en el momento de solicitarlas en el mismo lugar ya sean en la biblioteca o en el centro de fotocopiado el cual se encuentra ubicado adyacente a los laboratorios.

Los pagos que la ENEP Aragón utiliza a través de la caja son:

- Idioma.
- Centro de Cómputo.
- Multas.
- Copias.
- Altas Bajas.
- Credencial.
- Reposición.
- Cursos.
- Administrativos (Constancias, Extraordinarios etc).
- Bonos(Internet)

Por supuesto que este sistema presenta algunas desventajas entre las cuales se encuentran:

- Si alguien necesita realizar un pago y la caja ya ha cerrado, este se tendrá que posponer para el día siguiente hábil aunque este sea urgente como es el caso del pago por algún documento oficial (tal como un comprobante de estudios).

- La caja debe contar en todo momento con cambio suficiente lo cual implica frecuentes viajes al banco lo cual origina gastos administrativos, además de la molestia para los usuarios en caso de no tenerlo.

IV.1.2.1. Tipo de Aplicación a utilizar y su forma de trabajo

El mecanismo que se plantea mediante el cual se realizarán las transacciones es un proceso de ***lealtad***.

Normalmente un proceso de este tipo se utiliza para que los clientes de determinado negocio sigan asistiendo a estos a cambio de recibir gratificaciones, descuentos o cualquier otra retribución a cambio de su preferencia.

Este tipo de estructura de comercio no es considerada propiamente como dinero electrónico ya que primordialmente para que esto se califique así, debe existir algún tipo de relación con alguna institución de crédito y/o bancaria, lo cual a su vez involucraría procesos y costos mas elevados de operación además de que elevaría significativamente el costo del proyecto lo cual no es necesario ni mucho menos conveniente en nuestra situación.

Ahora bien probablemente uno se preguntaría, si no existe un concepto como tal de dinero, entonces ¿cómo se maneja un proceso de lealtad?. La respuesta es por medio de puntos, los cuales en términos prácticos se puede como considerar "dinero" ya que para obtenerlos será necesario intercambiarlos por dinero físico.

Aunque es un concepto simple, el implementarlo y sobre todo mantenerlo no lo es tanto ya que es necesario contar con un firme **sistema de compensación o conciliación** la cual se deberá de encargar de controlar los cargos y abonos necesarios dentro de la contabilidad de cada uno de las situaciones en las que el dinero es utilizado dentro de la institución.

Por supuesto para todo esto es necesario (casi se podría decir imprescindible) contar con un buen sistema de cómputo el cual permitiría realizar estas transacciones en forma totalmente controlada, automática y monitoreada por parte del área de contabilidad de la escuela.

Un punto primordial que es importante recalcar es que para que esta clase de sistema funcione es necesario unificar los proceso de pago en todos las posibles situaciones donde se maneje dinero (por supuesto podría haber excepciones como el comedor el cual es concesionado a un particular y no se le podría forzar a adherirse al sistema).

Este punto se requiere encarecidamente debido a que si se intentara mezclar diferentes tipos de pago en primer lugar el sistema alcanzaría un nivel de complejidad mayor, el cual no es necesario para nuestros propósitos y en segundo lugar el control y todos los demás beneficios que proporcionaría la tarjeta inteligente se perderían o al menos se reducirían considerablemente.

Ahora bien para realizar esta unificación de la forma de pago todos los pagos que se realizan en la escuela (incluyendo los de copias tanto en la biblioteca como los del anexo) tendrían que ser procesados por una sola caja en la cual el encargado por medio de un dispositivo terminal (o un lector junto con una PC, de esto se hablará mas adelante) se encargaría de recibir el dinero procesándolo y bonificando esta en la tarjeta en puntos los cuales solo serían validos dentro de la institución.

Establecido ya este entorno, no importaría que fuera una cantidad mayor o fraccionaria ya que la tarjeta estaría adecuada para recibir la cantidad con pesos y centavos exactos por lo que la pesadilla de los alumnos de no poder pagar sus tramites debido a la falta de cambio terminaría así como el problema del manejo de la morralla para la caja.

Una vez que el alumno tuviera su dinero dentro de la tarjeta éste podría utilizarla en cualquier momento e incluso podría depositar una cantidad importante en ella para que no tuviera que pasar incluso en todo el semestre por la caja.

Los beneficios que se tendrían con este sistema de Tarjetas Inteligentes (al menos por ahora para esta área de pagos) son:

- Control exacto y centralizado del manejo del efectivo en caja.
- No mas retrasos y molestias en el pago de un servicio para los alumnos
- Generación de reportes y estadísticas en forma casi automática.

Este último punto se deberá considerar sobre la base en que tan frecuente se requeriría la información. Es decir ¿debería ser totalmente en línea por hora o diario? (puede haber otras circunstancias las cuales pueden ser flexibilizadas dependiendo a la programación del dispositivo).

Por supuesto que para el área de contabilidad la respuesta seria que la información se debería encontrar disponible en forma constante lo cual se puede realizar en efecto, pero su desventaja es que puede llegar a saturar la red y en determinado momento incluso derribarla en casos tales como inscripciones o altas y bajas en las que este tipo de procesos aumentan en forma significativa.

Una observación que es importante recalcar es que ni la tarjeta ni las terminales son las que proporcionan la capacidad de administrar los datos recabados de los usuarios sino que esta deberá ser enviada a un sistema de cómputo especialmente creado (el cual no se definirá en la presente tesis aunque si un ejemplo) que se encargara de recopilar, procesar y almacenar estos datos para producir esta información para que posteriormente pueda ser manipulada por parte del personal autorizado
Al referirnos en párrafos anteriores, sobre la frecuencia en que la autoridad pertinente requiera la información significa que esto dependerá que tan seguido enviemos la información hacia el servidor lo cual puede ser por cada transacción hecha, por hora o cuando se agote el espacio en la terminal.

En una parte de la explicación se dijo que podrían usarse terminales y/o lectores unidos a PC. En realidad la diferencia en cuanto a funcionalidad no es mucha ya que como se explicó en él capítulo 3 una terminal es en esencia un lector y una PC al mismo tiempo, por lo tanto en si las diferencias básicas serian los costos y el manejo del equipo.

En esta situación del manejo del equipo es importante señalar que como se puede ver todos los días en lugares donde se utilizan tarjetas de crédito y débito lo más práctico es el uso de terminales. La razón es que al tratarse de un modelo auto contenido es prácticamente imposible realizar modificaciones sobre las mismas, a diferencia de una PC la cual es en extremo manipulable tanto por software como por hardware.

Por esta razón se recomienda que para este proyecto se utilicen terminales (en algunos lugares por sus características especiales se utilizarán lectores) para inhibir cualquier intento de modificar su proceso.

Una vez que se ha definido el flujo del dinero al ingresar a la institución vía la caja, veremos el otro lado de la moneda es decir donde el dinero guardado en el chip se utilizará.

Al existir tantos procesos involucrados en el manejo de pagos, es obvio pensar que cada uno posee sus necesidades específicas.

En los siguientes apartados se detallara el proceso de cada una de las situaciones donde el pago por el mencionado servicio debe ser hecho de forma obligatoria en la caja de la escuela, además se harán sugerencias sobre la información que podría ser recaba por medio del sistema en forma de reportes y que se considera podría proporcionar una asistencia valiosa.

Cada uno de estos eventos se agruparán sobre la base del lugar donde se realizarán los tramites ya que dependiendo de esto se definirá qué clase de información podría ser útil.

Es importante tener en cuenta que la recopilación de información para los datos recabados por la aplicación lealtad (así como sus consecuentes reportes) dependerá que tantas veces se envíe la información desde las terminales ya que estas se encontrarán fuera de línea en cada proceso.

IV.1.2.2. Pagos por trámites en Ventanillas Escolares.

Esta área al ser de los puntos centrales dentro de la ENEP abarca una multitud de procesos de pago que deben de pasar a través de ella. Estos se subdividen en:

- Alumnos
    - Constancia de Créditos
    - Constancia de Estudios
    - Extraordinarios.
    - Credencial
- Exalumnos

- Constancias de 100% de Créditos.
- Certificados de Estudios
- Revisión de Estudios
- Compulsa de Documentos
- Registros y Ejercicio Profesional

Al contar con un sistema de cómputo propio dentro de la misma área, el cual se encarga de retribuir toda la información necesaria a los administradores, no será necesario(al menos por el momento) que la tarjeta ayude proporcionar alguna reporte sobre la variedad de transacciones que se ejecutan en dicha sección ya sea mediante reportes o estadísticas.

A pesar de esto el uso de la tarjeta inteligente beneficiaría en reducción de molestias y tiempo de procesos esto es debido a que en lugar de tener que ir a realizar un pago por alguno de estos servicios y después tener que retornar con la posibilidad de que ya no este abierto o que haya demasiada gente, en su lugar al pedir un tramite en ese mismo momento se podría solicitar descontándolo de nuestra tarjeta que por supuesto deberá haber sido recargada previamente.

IV.1.2.3. Gobierno

Dentro del área de gobierno existen diferentes instancias en las cuales el pago por sus servicios es obligatorio. A continuación se detallan algunas de estas:

- *Secretaria Académica*
  - **Registro de Tesis**: Existen algunos datos útiles que se pueden recabar por medio de la tarjeta (independientemente del costo mismo del servicio) entre ellos se encuentran la cantidad de tesis que se inician y que a la vez concluyen (por supuesto tendría que hacer una comparación con los registros de titulación).
  - **Servicio Social:** Es esta sección como su nombre lo indica se realiza todos aquellos tramites para poder liberar el servicio social del alumno. En esta sección de gobierno solo existe un pago que es por registro del servicio social. En este caso aunque igualmente se hace necesario una terminal, se presume que su tipo seria mucho más sencillo que el de otras áreas debido a que existirían mucho menos transacciones.

Independientemente de los datos a recabar de los puntos anteriores, existe la posibilidad de poder registrar y obtener información sobre:

- Cantidad exacta sobre los pagos de los registros de tesis.
- Nombres y Carreras de los que registran su servicio social

IV.1.2.4. Servicios de Cómputo

En la actualidad el uso de las computadoras es prácticamente indispensable dentro de la institución sin importar a que carrera nos enfoquemos.

Desde el simple uso de una hoja de cálculo o un procesador de textos hasta aplicaciones CAD y lenguajes de programación los servicios de cómputo son siempre requeridos.

Para cubrir todas estas necesidades existen dos instancias:

- **Fundación UNAM**

Dentro de esta área los servicios que se prestan se hacen a través de bonos de las siguientes características:

  - Por horas
  - Por 5 horas
  - Semestral(100 horas)

Además se proporciona el servicio de impresiones. Este también podría ser incluido dentro del esquema de uso de la aplicación lealtad de la tarjeta.

El cobro del tiempo utilizado e impresiones se realizaría mediante una terminal la cual sería utilizada por el administrador del centro de cómputo que al terminar el alumno el uso del equipo solo se tendría que verificar el tiempo utilizado y hacer el descuento correspondiente de la tarjeta.

El manejo de descuento podría realizarse de dos maneras

  - Como en la actualidad se manejaría un bono o vale dentro de la tarjeta de la cual se podrían descontar puntos. La desventaja con esta opción es que para poder definir la aplicación bono se requeriría espacio de tarjeta con lo cual se reducirían nuestras opciones en un futuro si quisiéramos agregar nuevas aplicaciones.

  - Con la segunda alternativa, se utilizaría la misma aplicación de lealtad que se usaría en todas partes con lo cual el espacio quedaría intacto para un futuro uso.

- **Centro de Cómputo**

Dentro de esta área el uso del equipo se encuentra mas orientado a determinadas carreras (aunque no vedadas a otras en el caso de los cursos).

En cuanto al uso de estas para los cursos se tendría una situación muy similar a la de la Fundación UNAM solo en lugar de llevar un registro de horas se tendría en la tarjeta el identificador del curso por medio del cual se podría tener el control por medio de los

torniquetes para su acceso al centro de cómputo utilizando el horario del mismo registrado en la tarjeta

Además para el uso de equipo por hora se llevaría también en la misma forma que el equipo de cómputo mediante un control de las mismas comprándolas y registrándolas previamente.

IV.1.2.5. Copias

El uso del servicio de fotocopiado puede llegar a ser (por experiencia propia) una verdadera hazaña de paciencia debido a:

- La limitada cantidad de gente que provee esta función la cual llega a variar dependiendo de la hora y día.
- La limitación (de nuevo) en cuanto al efectivo ya que si no se tiene el necesario y suficiente todo el tiempo de espera puede llegar a ser en vano.

Estas limitaciones se hacen especialmente graves en el área de la biblioteca la cual tiene en calidad de clientes cautivos a sus usuarios ya que si no se tiene la capacidad de préstamo de material no se tiene otra opción que sujetarse y soportar todas las situaciones anteriormente descritas. A diferencia de servicio de fotocopiado que se encuentra en el área adyacente de laboratorios, con en la cual es posible utilizar algún otro que se encuentre en el exterior de la escuela.

En esta situación la aplicación de lealtad proveería todo el cambio necesario ya que través de una terminal el monto sería descontado de la tarjeta en forma exacta sin tener la necesidad de tener los bolsillos llenos de monedas.

En cuanto al problema de la gente insuficiente, una posible solución aunque (por supuesto a mediano o a largo plazo) es permitir que los alumnos obtengan sus propias copias con una fotocopiadora que reciba directamente la tarjeta.

En referencia a la información que se podría recabar se encuentra:

- Un promedio de copias, pudiendo diferenciar en que sector se hicieron e incluso que carrera es la que más utiliza[10].
- La cantidad de dinero *exacta* que se recaba también por sector pudiendo incluso reconocer por operador[11].

IV.1.2.6. Multas de Biblioteca

Todos los usuarios de la biblioteca saben que es en definitiva frustrante no poder obtener material porque una multa esta registrada a nuestra cuenta y si a esto le añadimos que la caja tiene horarios que aunque supuestamente fijos estos pueden variar dependiendo de

[10] Es importante recalcar que esto se haría por medio del sistema y no se incluiría en la tarjeta
[11] Esta acción recaería en su mayor parte en la programación de las terminales.

la persona encargada (extendiéndose incluso de una semana a otra aumentando su costo de pago) esto nos puede llevar a un continuo dolor de cabeza (en especial sí se es inconstante en la entrega del material).

Ahora bien mediante la aplicación lealtad el pago de una multa puede hacerse directamente en la biblioteca (claro sí previamente cargamos puntos en la tarjeta) en forma expedita mediante terminales instaladas en la misma mesa de préstamo.

Al igual que en anteriores conceptos el sistema con la TI ofrecería información que en este caso podría ser:

- Cantidad de Pagos por Multas.
- Estadísticas y Promedios de Multas por carrera e incluso por alumno.

IV.1.2.7. Educación Continua

Como su nombre lo indica esta sección de la escuela consiste en extender la educación dentro de la institución y no solo para los alumnos sino para cualquier persona que desee avanzar en su preparación.

Aunque el alcance de la educación del área como tal dentro de la UNAM incluye enseñanzas tan dispares como diplomados para titulación, sistemas de universidad abierta y diplomados, dentro de la ENEP la oferta educativa se encuentra restringida a:

- Actualización y Capacitación
- Redacción y Ortografía
- Relaciones Humanas
- Didáctica General
- Formación de Instructores
- Evaluación de Proyectos
- Lenguas
- Ingles
- Francés
- Italiano
- Apoyo a la Titulación
- Arquitectura
- Comunicación y Periodismo
- Derecho
- Diseño Industrial
- Economía
- Ingeniería Civil
- Ingeniería en Computación
- Ingeniería Mecánica Eléctrica
- Pedagogía
- Planificación para el Desarrollo Agropecuario
- Relaciones Internacionales y..
- Sociología

- Cursos de Computo
- Procesadores de texto y edición de publicaciones
- Hojas de cálculo y paquetes financieros
- Manejadores de bases de datos
- Paquetes integrados para oficina
- Diseño asistido por computadora
- Lenguajes de Programación
- Administración en cómputo y redes
- Internet
- Regularización de Asignaturas
- Vinculación Universidad-Empresa[xliii]

Cada una de estas opciones representa información que puede ser recopilada por la TI así como en todos los anteriores pagos mediante la aplicación de lealtad.

IV.1.2.8. Idiomas

Finalmente el pago de los idiomas se haría utilizando la misma aplicación de lealtad la cual ofrecería las mismas ventajas de pagar al momento los idiomas sin esperar al horario de la caja junto con la información recopilada de los alumnos que permitiría proveer un mejor desempeño en esta área

Entre la información que se podría recuperar esta:

- Registro de las inscripciones
- Constancias

Dentro de estos dos ámbitos se podrían generar algunos reportes a partir de los datos de la tarjeta, con excepción claro de la gente externa la cual al ser una prestación exclusiva para los alumnos (por lo menos de la ENEP) no podría otorgárseles.

El reporte se derivaría pudiendo contar con información tal como:

- Número de cursos por alumno
- Duración promedio
- Grado de deserción
- Generación de Constancias en forma automática

Es importante aclarar que para poder contar con esta información no sería necesario agregar ningún dato nuevo a la tarjeta ya a que partir de sus datos generales se pueden obtener todas estas estadísticas.

IV.1.2.9 Flujo de la información y Administración de Lealtad

Ahora bien una vez que se tienen contemplados cada uno de los ámbitos donde el uso de la aplicación lealtad se podría utilizar, el siguiente paso es describir como la información de sus respectivas transacciones deberá fluir hacia el sistema que deberá controlar, administrar, monitorea, y registrar todos los puntos que en estos son gastados.

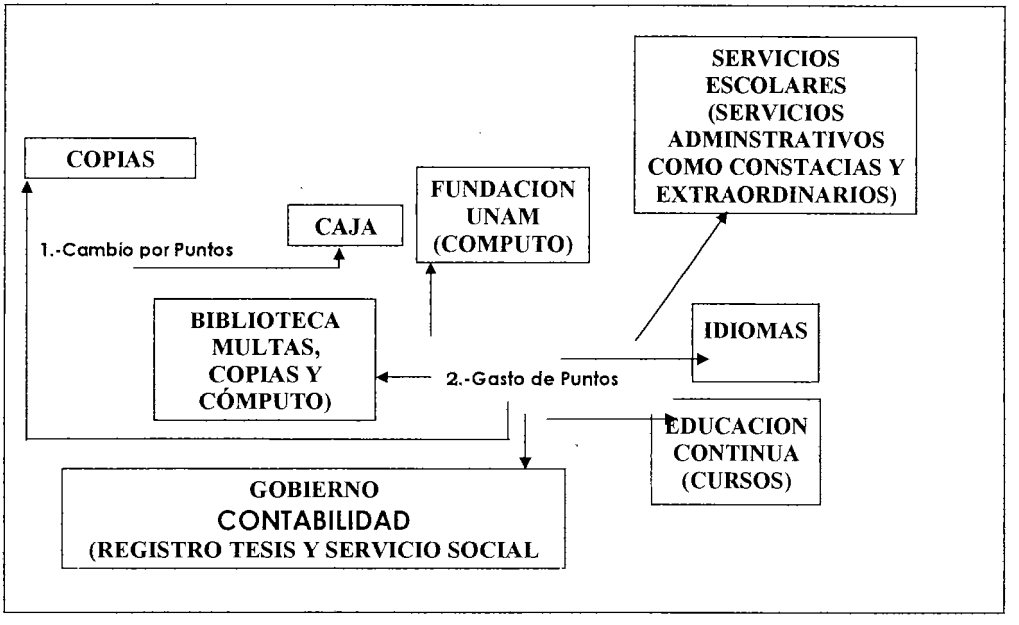


Fig. 4.1 Esquema de Flujo de Puntos en Lealtad

Como se puede apreciar en la figura 4.1 en primer lugar los alumnos deberán mediante su tarjeta agregar puntos a la misma cambiándolos en la caja.

Una vez hecho esto los alumnos podrán utilizarlos en cualquiera de los lugares autorizados y habilitados con terminales las cuales se encargaran de descontarlos y llevar un registro de cada una de las transacciones que se lleven a cabo junto con los datos del tarjeta habiente como su identificador (Numero de Cuenta o RFC) el monto de la transacción, fecha y hora y por supuesto el monto.

Cada determinado tiempo estas terminales descargaran o colectaran esta información ya sea en modo automático o manual y será enviada hacia un colector central el cual se encargaría de:

- Administrar:
    - Verificar el estado de las terminales.
    - En caso de ser colectas automáticas revisar que estas se hagan de manera adecuada.
    - Vigilar que no existan problemas con las bases de datos.
    - Poder llevar el control de las tarjetas sabiendo a quien pertenece para así poder llevar un control mas específico.
- Compensar:

- Verificar que los montos en efectivo que son recaudados en caja sean congruentes con los datos que registro la terminal. Claro que esto solo se podría hacer al hacer un corte de caja (al final del día).
- Controlar que los montos que se han registrado en caja coincidan con los gastos que se han hecho por usuario, es decir que si X persona cargo determinada cantidad esa persona esa misma persona no pueda gastar una cantidad mayor.

- Registrar:
  - Generación de reportes del que, como, cuando, cuanto y quien gasto que cosa.
  - Generación de reportes de colectas informando el comportamiento de las terminales.
  - Reportes del balanceo y como esta se comporta.

Las anteriores opciones pueden ampliarse dependiendo de las necesidades del departamento de contabilidad o de la dirección.

IV.1.2.10. Conclusión Lealtad

Como se puede ver existe una gran cantidad servicios que esta área proporciona, por lo que así mismo la TI y su sistema adjunto podría ayudar a organizar, entre ellos se encuentran:

- Administración efectiva de los pagos por los servicios
- Visualización de que servicios son los mas utilizados y por quien son utilizados (Estudiantes de la ENEP, Universitarios y Externos).

Para el caso de externos y Universitarios, dado que la tarjeta solo sería distribuida dentro del alumnado y personal docente el registro de esta información se tendría que hacer a través de las terminales.

Una vez que se ha detallado todas aquellas secciones donde el uso del dinero sería simplificado a través de la TI, ahora se procederá a describir algunas otras secciones donde el uso de la tarjeta como identificación y registro de actividades dentro de estas mejoraría tanto por parte de la sección en cuestión como para los alumnos

IV.1.3. Biblioteca

La actividad fundamental de nuestra y cualquier otra biblioteca es la de préstamo de libros. Esta actividad esta controlada (tanto las entradas como las salidas) por el personal de la institución, el cual en determinadas épocas no es suficiente como es el caso de exámenes finales

Aunque el sistema de cómputo de la biblioteca resulta bastante confiable, en algunas ocasiones el servicio que proporciona no cumple con las expectativas debido a la gran cantidad de personas que en determinado momento ocupan sus servicios.

La secuencia actual de pasos que se realizan para el préstamo y devolución de material se puede apreciar en el diagrama 4.2

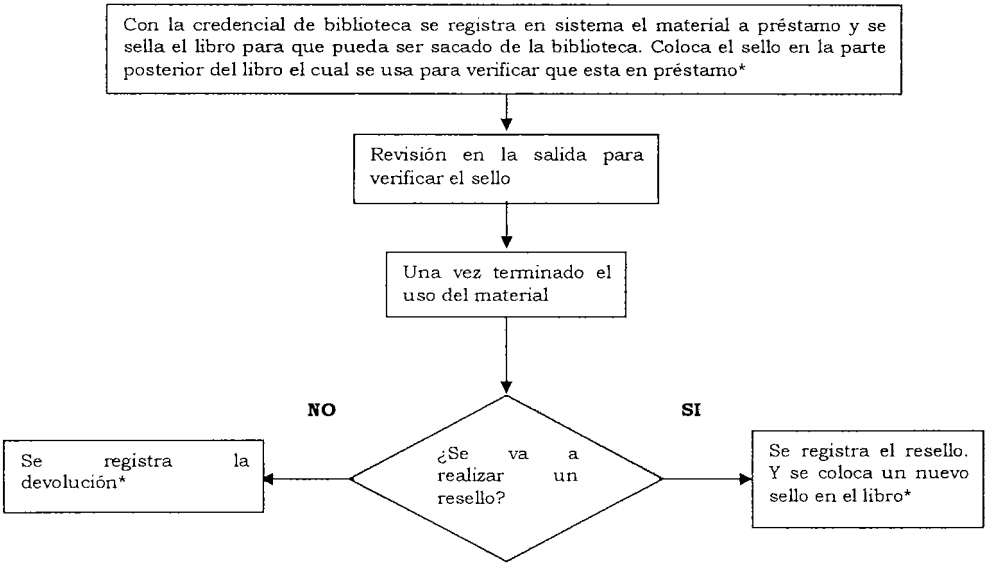


Fig. 4.2 Ciclo para Préstamo y Devolución de Material en la Actualidad

*. El tiempo utilizado en este paso dependerá de la cantidad de personas con el mismo tramite.

Ahora bien el principal cuello de botella se debe a la cantidad insuficiente de personal para atender a un gran número de alumnos en las áreas de préstamo y devolución. Como solución propuesta para remediar esta situación se plantea que préstamo del material quede en manos de los alumnos

En el caso de la devolución, para evitar algún tipo de fraude contra el sistema como son sustitución del libro (por ejemplo un libro de programación muy buscado por uno obsoleto) e incluso de las etiquetas de los mismos, se requerirá del uso de un bibliotecario.

Para ello se tendrá en la tarjeta un registro de todos los materiales que salgan en préstamos. En este registro se guardarían los identificadores de los libros. A través de esto el proceso sería como en el diagrama 4.3

A través de una terminal e ingresando los identificadores de los libros, el alumno ingresaría en su tarjeta los libros que solicita en préstamo. Por supuesto la tarjeta tendría un máximo de préstamos.

Por medio de un lector y una pantalla en la salida, el personal que revisa su salida puede verificar que los libros de la tarjeta coincidan con los que el alumno retira

Una vez terminado el uso del material

NO

¿Se va a realizar un resello?

SI

r medio de terminales al presentar el libro bibliotecario revisaría que el libro que tán devolviéndose es el mismo que esta gistrado en la tarjeta y que el alumno tiró. Además el número de resellos para esa silla se colocaría de nuevo en blanco

Por medio de las mismas terminales con las que se hace el préstamo se registra el resello en la tarjeta. El número máximo de resellos seria controlado por un contador dentro de la tarjeta asignado a cada uno de los préstamos. Si el número de resellos sobrepasa este número el resello no podrá realizarse

Fig. 4.3 Ciclo para Préstamo y Devolución de Material mediante la TI

Debido a que existirá un numero limitado de préstamos por vez, el alumno al hacer el préstamo de determinado libro, al registrarlo si todas los registros en la tarjeta están ocupados, el alumno deberá sacrificar uno de los ya registrados en su tarjeta.

Bajo este esquema todas las transacciones (entendiéndose por transacción el registro de los préstamos y devoluciones del material) serían fuera de línea lo que ahorraría ancho de banda dentro de la red de la biblioteca lo que en casos de mucha afluencia seria muy bien recibido.

Por supuesto esta situación fuera de línea afectaría la actualidad de los datos, lo que quiere decir que si se deseara saber si un libro esta en préstamo o en resello solo se sabría hasta que la terminal enviara sus datos registrados hacia un servidor central, el cual podría ser el mismo o no que se utilizaría para regular las operaciones de la aplicación lealtad.

Estas trasmisiones de las terminales hacia el servidor podrían hacerse cada determinado tiempo, el cual dependería de que tan actualizada se necesite dicha información. Estas trasmisiones podrían hacerse tan frecuentemente como cada vez que se haga una transacción (lo cual no resulta muy conveniente ya que se perdería la ventaja del ahorro del ancho de banda), cada día o cada vez que se llenara la memoria de la terminal.

IV.1.4. Asistencia

El aspecto de asistencia aunque no tan indispensable de un control como lo es el manejo de los recursos económicos, si es necesario para llevar el seguimiento de los recursos humanos. Un aspecto importante es que para llevar este control a cabo no sería necesario agregar demasiados elementos sino solo lectores donde se requiera llevar este control, los cuales se encontrarían conectados al servidor central.

Las transmisiones desde los lectores podrían definirse que siempre estuvieran en línea ya que a diferencia de una colecta desde una terminal, los lectores no ocuparían tanto ancha de banda.

Como aspecto en seguridad y para evitar que alguien pueda manipular la asistencia y como los lectores deberán estar conectados a una única PC se recomienda que la aplicación que los controle solo actúe como puente entre estos, es decir que el verdadero registro sea llevado por el servidor central utilizando como intermediario a la PC

IV.2.Especificaciones Técnicas.

IV.2.1. Tarjeta

Una vez que se han definido las necesidades de la ENEP donde el uso de la tarjeta seria de utilidad, es momento de iniciar con las especificaciones técnicas las cuales aunque pueden cambiar dependiendo tanto de nuevas necesidades como de los costos implicados se propondrán aquellas que puedan ser lo más flexibles posibles de acuerdo al problema que nos ocupa.

IV.2.1.1. Características Generales

Aunque pudiera parecer que sería necesario una tarjeta con mucha capacidad por la cantidad de datos que se tiene contemplado administrar a través de la TI, en realidad la capacidad necesaria seria no mas de 2Kbytes, esto por supuesto dependiendo si solo se abarcara los puntos anteriormente vistos que son:

- Manejo de Dinero a través una aplicación lealtad.
- Administración de préstamo bibliotecario.
- Administración de la asistencia de maestros.

Pero si fuera probable que las necesidades pudieran crecer en un futuro la capacidad por supuesto tendría que crecer a la par. Por supuesto esto influiría en el costo. Por ahora este estudio de especificaciones se enfocará a las necesidades anteriormente descritas.

Las características físicas de la tarjeta, necesarias para satisfacer los requerimientos abarcan:

- **Manejo de Protocolos Criptográficos**
  Debido a que se administrara dinero por medio de la TI, es muy importante que la información se encuentre debidamente protegida. Es por ello que se recomienda que la tarjeta a utilizar permita el manejo del protocolo Triple DES con una llave de al menos 56 bits[xliv] ya que con este nivel de llave se necesitaría invertir mucho dinero y tiempo para poder descifrarlo.

- **Manejo de Multiaplicaciones**
  Para esta característica es importante tener en cuenta que las tarjetas que se adquieran deben tener una arquitectura abierta. Esto quiere decir que:

  - Aunque existen tarjetas que ya proveen algunas de las prestaciones que se necesitan, las mismas no permiten ampliarse hacia nuevas aplicaciones. Este tipo de tarjetas no es recomendable su utilización(a menos claro que si permitieran su expansión).

  - Que todos los medios necesarios para operarlas (creación modificación y mantenimiento) sean entregados a la institución o en todo caso al encargado del proyecto. Esto es para evitar una dependencia tecnológica de determinada empresa o marca. Dentro de este rubro se incluye que por supuesto deberán seguir todos los estándares ISO anteriormente descritos.

- **Tipo de CHIP**
  Esta característica se refiere a qué tipo de comunicación utilizará el chip ya sea de contacto o sin contacto. Para esta consideración se deberá tomar en cuenta la necesidad de velocidad en el uso de las tarjetas como sería el caso de asistencia, pero debido a que esta se encontrara dirigida únicamente para maestros y su cantidad no es significativa, es por ello que la tarjeta a utilizar deberá ser de contacto a menos claro que se planee agregar esto a la asistencia de alumnos lo cual requeriría de una inversión mas elevada.

- **Tipo de Multiaplicación**
  Las tarjetas como se ha definido previamente tienen un espacio fijo para almacenar aplicaciones, pero en este punto es donde se inicia la divergencia. En la actualidad existen del tipo en las que una vez escrita determinada aplicación esta no puede ser borrada o modificada por lo que ese espacio no puede volver a utilizarse.
  Existen otras, las cuales al escribir estas pueden ser modificadas sus aplicaciones estas son las llamadas Java Cards. El problema de este tipo de tarjetas es que su costo es mucho mayor.
  Debido que para este proyecto se considera que su presupuesto no es elevado además de que sus usos no serán muy sofisticados, se

recomienda el uso de tarjetas no modificables las cuales entran dentro de nuestras necesidades.

IV.2.1.2. Estructura Lógica de la Tarjeta

Con estructura lógica se entiende al esquema que se utilizará para la distribución de los datos almacenados dentro de la tarjeta. Cada uno de estos deberán ser distribuidos de manera que cada aplicación ocupe el espacio óptimo.

Después de definir en la sección anterior el tipo de multiaplicación a utilizar se considera que el espacio de la tarjeta deberá ser asignado en forma precisa ya que si no es correctamente definido esta no podrá ser modificada y lo que es peor si deseáramos agregar nuevas aplicaciones para hacer crecer la operación de la tarjeta esto nos limitaría en forma grave.

Ahora bien para poder definir qué estructura deberá contener nuestra aplicación es necesario establecer qué datos contendrá la misma y para ello se especifican los requerimientos que previamente se detallaron con los cuales incluyen los campos que contendría la tarjeta.

- **Datos Generales**

Como elementos generales se consideran a todos aquellos elementos dentro del sistema que pueden ser utilizados por cualquier aplicación sin importar su función particular. Debido a que el sistema administrara datos tanto de alumnos como de maestros se incluirán a continuación los datos generales de ambos elementos.

Nombre del Campo	Longitud	Permisos	Observaciones
Alumnos			
Numero de Cuenta	9	L	
Fecha de Expiración la Tarjeta(DDMMYYYY)	8	L	
Maestros			
CURP o RFC	8	L	
Fecha de Expiración la Tarjeta(DDMMYYYY)	8	L	

L.-Lectura
E.-Escritura
M.-Modificación

- **Aplicación Lealtad**

Los datos dentro de la aplicación lealtad incluyen a aquellos que permitirán llevar el control del efectivo dentro de la institución. Una situación de la que se debe advertir a los usuarios es que si la tarjeta es extraviada el dinero no podrá ser recuperado. El manejo se llevará a cabo por medio de puntos o fracciones de punto. Debido a que dentro de la tarjeta la información se almacena en forma hexadecimal el máximo de puntos con sus

decimales será de 655.35 puntos tomando también en consideración que es improbable que algún alumno desee almacenar mas de esta cantidad en esta tarjeta.

Nombre del Campo	Longitud	Permisos	Observaciones
Saldo Máximo	*3 Enteros* *2 Decimales*	L/M	Los permisos antes mencionados deberán estar restringidos a: **I.** Lectura por cualquier dispositivo destinado para tal propósito. **II.** Modificación únicamente realizada por dispositivos que autentiquen la transacción mediante métodos criptográficos y NIP Se refiere a la cantidad máxima que puede ser cargada dentro de la aplicación
Saldo Actual	*3 Enteros* *2 Decimales*	L	Cantidad de puntos que se tienen en total actualmente
Fecha de Última Transacción (DDMMYY)	*6*	L	Fecha en que se realizó el ultimo consumo
Fecha de Activación DDMMYY)	*6*	L	Fecha en que se activo la aplicación lealtad para esta tarjeta

L.-Lectura M.-Modificación
Nota: Para los saldos se puede manejar fracciones de punto como si fueran moneda corriente

- **Biblioteca**

Los datos que se utilizarán en la biblioteca son aquellos que se encargarán de

- Almacenar las claves de los libros en préstamo
- Almacenar las fechas de préstamo del material

Es necesario tener en cuenta que los datos que a continuación se describen se repetirán dependiendo del número de prestamos que se permitan. Además el tamaño asignado a esta aplicación deberá contemplar que el número de resellos podría aumentar.

Datos de la Aplicación

Datos por Material

Nombre del Campo	Longitud	Permisos	Observaciones
Clave de libro en préstamo	*22**	*L/M*	***La clave del libro almacenada deberá compararse contra el libro físico al retirarlo del acervo
**Fecha de Salida	8 (DDMMAAAA)	L	Fecha en que se retiro cada libro.
**Fecha de Retorno	8 (DDMMAAAA)	L/M	***Fecha en que debe regresarse el archivo
**Máximo de Resellos	3		***Registra el conteo de los resellos y que va ser actualizado a través de las terminales

L.-Lectura
M.-Modificación

*Este valor podría variar
**Estos valores se repetirían dependiendo de cuantos libros en préstamo se pretenda definir.
***La protección de modificaciones indebidas se realizará bajo las mismas restricciones de la aplicación lealtad aunque no necesariamente con las mismas llaves.

Debido a que para la verificación de la asistencia no serán necesarios campos anexos a la tarjeta estos no se incluirán como en las secciones anteriores. En su lugar en una sección posterior se describirá su funcionamiento en detalle. La estructura en forma de esquema se puede apreciar en la figura 4.4

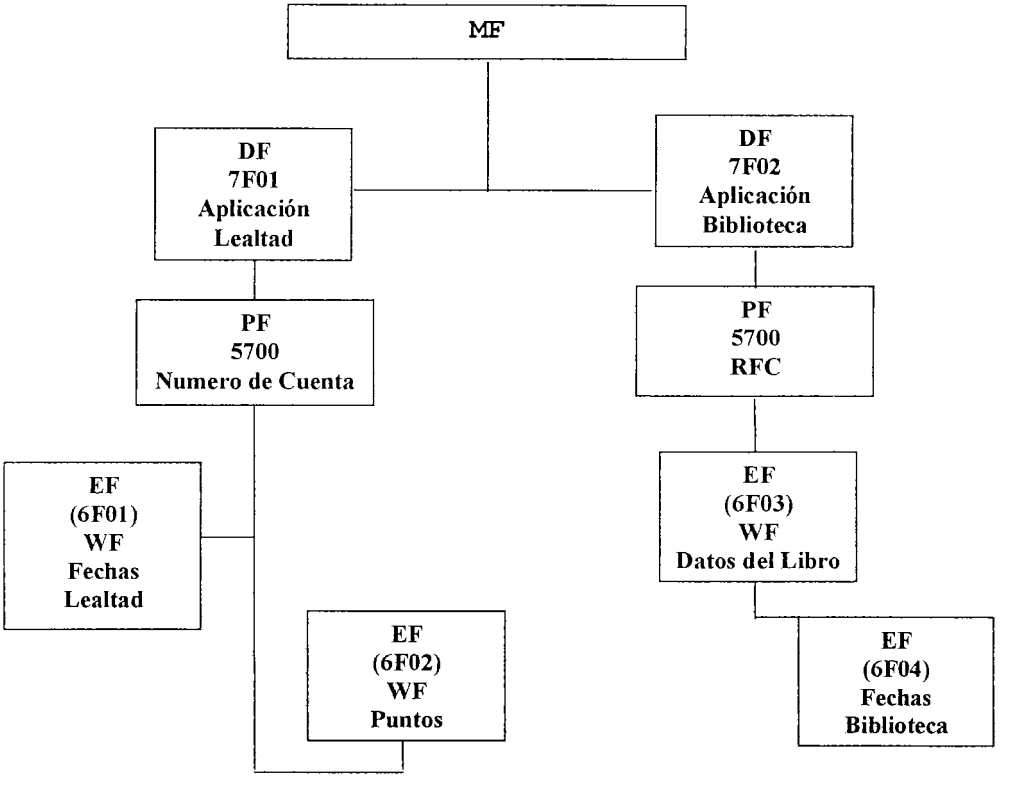


Fig. 4.4 Esquema de las aplicaciones para la TI

IV.2.2. Terminales y Lectores

Como se dijo en capítulos anteriores la tarjeta en si misma no sirve de nada sin los equipos asociados que permiten interactuar al tarjeta habiente con el sistema.

Ahora bien las características del equipo que a continuación se describirán no definen un equipo en especifico sino solo la descripción de los aspectos que deberían abarcar de acuerdo a los estándares ISO definidos en el capítulo 2.

IV.2.2.1. Lectores

Un punto importante a considerar es que debido a que el tipo de lectores dependerá de la máquina a la cual se encuentre conectado, la decisión sobre el tipo de lector se regirá por esta (ya sea por un puerto USB o serial) y por otra parte por las necesidades fisicas de esta.

Estas necesidades son:

- **Asistencia**

Se necesitarían alrededor de tres lectores conectados a una única PC la cual puede o no estar conectada a la red. Debido a que la mayoría de las máquinas actuales solo cuentan con un solo puerto serial se recomienda el uso de lectores con puerto USB

- **Uso de Equipos de Cómputo**:

Este caso puede ser opcional ya que como se vio en detalle en secciones anteriores el cobro por el uso de los equipos de cómputo puede realizarse

  - Por medio de una aplicación residente dentro de cada PC y de lectores la cual al insertar la tarjeta dentro del mismo registre la hora de entrada y al retirarla marque la hora de salida, para que al momento de salir el administrador del centro de cómputo pueda mediante una terminal descontar de la tarjeta de acuerdo al tiempo usado. Es muy importante recalcar que el descuento no deberá realizarse mediante la aplicación residente para evitar posibles intentos de fraudes (el registro de la hora no deberá realizarse mediante el reloj de las PC sino mediante la de un servidor central al que no puedan tener acceso los usuarios). El problema con esta opción es que implicaría el costo de un lector por PC.

  - Que la administración del tiempo utilizado se realice en forma manual por el administrador del centro de computo.

IV.2.2.2. Terminales

Los equipos terminales son quienes se encargarán de interactuar con las partes protegidas de la tarjeta es por ello que es necesario que amen de los ya mencionados estándares ISO, también deberán:

- **Criptografía**

  Tener las capacidades de autentificación de tarjetas mediante comandos criptográficos. Estas autentificaciones se realizarán mediante las llaves las cuales deberán estar diversificadas preferentemente.

- **Capacidad para Multiaplicaciones**

  En el caso de las terminales ubicadas dentro de la biblioteca en el caso de que sean las mismas que las utilizadas para el pago de multas deberán tener la capacidad de llevar a cabo la autentificación de ambas aplicaciones y de ser posible maneje diferente llaves para cada una.

- **Almacenaje.**

  Como se dijo anteriormente una terminal funciona en esencia como una PC con sus capacidades reducidas, es por ello que aunque en nuestro caso no será necesario, es importante considerar la capacidad

de almacenaje de la misma en el caso de que alguna aplicación futura necesite la consulta de datos "externos" como podría ser el uso de catálogos.

- **Puertos:**
  El tipo de comunicación que se utilizaran desde los POS hacia los servidores dependerá de las transmisiones a realizar y como en nuestro caso se trata de una arquitectura semi-cerrada (ya que la tarjeta solo se podrá utilizar dentro de la institución en este caso la ENEP, aunque posteriormente se podría abrir a otras instituciones de la UNAM) el tipo de puertos necesarios deberán ser para una red LAN o protocolo TCP/IP. Además deberá permitir el manejo de direcciones IP para que puedan ser tratadas como un equipo mas dentro de la red.

- **Impresora**
  Esta característica deberá ser incluida si se contempla que algún comprobante deba ser dado al alumno al hacer un pago, un cambio de dinero por puntos o alguna otra transacción.

IV.2.3. Comunicaciones

El medio mediante el cual toda la información será transmitida dentro del sistema es de extrema importancia debido a que si en algún punto la conexión es interrumpida, todas las prestaciones de la TI quedarían limitadas.

La forma de transferencia que se contempla para el presente proyecto es través de una red LAN. Dicha red conectaría los servicios de pago de servicios, biblioteca y asistencia de maestros.

La comunicación se hará mediante el protocolo TCP/IP cuya transmisión se puede hacer ya sea por medio de una red dedicada o mediante la red ya establecida en cada sección agregándole los nodos que no existan en la actualidad como serian las conexiones con las cajas y asistencia.

Se recomienda en definitiva que sea mediante la primera opción ya que de esta manera evitaría interferencias en el ancho de banda, además de que evitaría conflictos tanto en la administración como en la seguridad del sistema.

Ahora bien ya sea que se pretenda utilizar la misma red para cada una de las aplicaciones o en forma independiente es necesario que la transmisión de los datos se realice en forma segura por lo menos para la aplicación de lealtad (claro que ser posible todas las transmisiones deberían serlo) esto se logra estableciendo una red fiable.

Para lograrlo existen servicios de seguridad que deben ser establecidos dentro del sistema aprovechando las capacidades criptográficas definidas en secciones anteriores. Dichas capacidades deberán estar habilitadas tanto en las terminales como en el servidor. Los servicios de seguridad son

IV.2.3.1. Confidencialidad

Garantiza que la información será comunicada solo a las partes autorizadas de la recepción. Esto se logra definiendo un sistema de cifrado entre las terminales y el servidor estableciendo un sistema de llaves que deberán estar almacenadas en estos equipos y cuya responsabilidad recaiga en diferentes personas

IV.2.3.2. Integridad de los datos (Autentificación)

Al enviar los resultados desde la terminal hacia el servidor y al tratarse de valores contables, estos no deberán cambiar un solo digito, ya que de ser así el sistema de conciliación no seria confiable y se tendrían valores erróneos para el área de contabilidad.

Para prevenir que los datos transmitidos puedan ser alterados y en caso de suceder pueda ser detectado se deberá incluir dentro del sistema de transmisiones el manejo de funciones Hash que como se contemplo en él capítulo anterior permiten generar chequeos sobre la información transmitida

IV.2.3.3. Identificación de los participantes

Con la identificación se tiene el objetivo de registrar a todos aquellos integrantes dentro de la red que pueden comunicarse entre ellos y a su vez con el servidor. La identificación va de la mano con la autentificación.

IV.2.3.4. Autentificación de los participantes

La idea de este elemento de seguridad es reducir el riesgo de que algún posible intruso se pudiera enmascarar sobre apariencias legítimas para realizar operaciones no autorizadas. Se requiere una estructura de identificación con las siguientes entidades.

- **Autoridades certificadoras**:
  Que envían claves públicas con la venta de certificados firmados con la clave secreta de la autoridad que verifican la identidad física del propietario de la clave pública.

- **Una base de datos**: Que contiene toda la información relativa a las claves privadas de cifrado con su valor, periódo de validez e identidad de los propietarios. Esta base deberá estar configurada para que los datos de la aplicación lealtad no puedan ser leídos y/o alterados por gente externa al área de contabilidad definiendo restricciones para los usuarios

- **Una autoridad que registre**:
  Su papel principal es definir y asignar nombres únicos a los diferentes participantes[xlv].

IV.2.4. Servidor de Aplicaciones

El equipo que se encargará de controlar el flujo de la información desde todos los dispositivos (léase terminales y lectores) se denomina servidor. Esta unidad deberá estar protegida tomando en cuenta todas las consideraciones que se comentaron en la parte de

comunicaciones lo cual involucra mecanismos criptográficos que le permitirán interactuar con el resto del sistema

Independientemente de lo expuesto en el párrafo anterior el servidor deberá contar con la capacidad suficiente de proceso que le permita recibir, procesar y dar respuesta a las peticiones de cada uno de los dispositivos involucrados.

Es por ello que los requisitos recomendados para el servidor (el cual se recomienda deberá ser dedicado en exclusiva para esta función) incluyen características ampliadas los cuales son:

- **Procesador**
  Aunque es el elemento del equipo que se encargara de hacer todos los procesos desde criptográficos hasta almacenamiento se considera que no es necesaria demasiada capacidad por lo que se recomienda uno de 2 Gigagertz o superior

- **Memoria**
  Es uno de los elementos más importantes ya que si no exista la suficiente memoria, los procesos en línea lo resentirán por lo que se recomienda uno con capacidad de no menos 256mb

- **Disco Duro**
  Las características de esta pieza del equipo dependerán de que cantidad de transacciones se manejaran tanto en la primera fase del proyecto como de sí en este se almacenaran todos los datos para un archivo histórico. Este ultimo punto no se recomienda ya que si llega a colapsarse el sistema, todo el histórico podría no ser recuperable, es por ello que en su lugar se exhorta a que ya sea que se utilicen discos paralelos de unos 20 GB o uno de 30 GB con un sistema de respaldo de cinta o algún otro

- **Red**
  Aunque la mayoría de los procesos que se realizaran hacia y desde el servidor serán fuera de línea es decir realizadas en las mismas terminales, será necesario establecer una que de suficiente soporte a las colectas hacia el servidor.

Además de los requisitos mínimos físicos anteriormente señalados será necesaria una protección de acceso mismo al servidor con dispositivos tipo firewall ya sean de tipo físico o lógico.

IV.3.Administración

IV.3.1. Descripción de la Posible Aplicación Administradora

Independientemente de los elementos técnicos dentro del sistema, el cómo se administrarán los dispositivos por parte de la o las personas responsables de todo el entorno deberá ser tomado como un objetivo primordial debido a que esta proporcionara

y recibirá toda la información de los dispositivos "pasivos".Todo esto deberá realizarse a través de un sistema de computo.

En el aspecto de recepción de datos se tendrá:

- Mostrar los datos trasmitidos desde las terminales (Como se ha dicho anteriormente la actualidad de la información dependerá de que tan frecuentemente se realice la transmisión de la terminal al servidor central) que deberán indicar información como pude ser:

  - En el caso de la caja, cuanto se ha depositado en efectivo, cuanto se ha depositado en puntos por hora, día, semana y/o mes (esto dependerá del periodo del envío de la información al servidor), cuantos puntos (y fracciones de estos) se depositaron a que tarjeta y/o alumno.

  - Para todas las demás terminales, es decir aquellas que se utilizaran para el gasto de puntos deberán proporcionar elementos como la cantidad del total de puntos gastados por hora, día, semana y/o mes (igual dependerá de las colectas), gastos de puntos por tarjeta y/o alumno.

    Obviamente estas terminales al realizar las transferencias, llevaran indicadas desde cual se realizo para que así se pueda obtener cuanto de lo que hay en caja en efectivo corresponde a que sección y el área de contabilidad pueda realizar los balances correspondientes.

  - En el caso de las terminales ubicadas dentro de la biblioteca estas proporcionaran al sistema, información que incluye los préstamos por alumno que se han registrado (que engloba la clave de libro y él número de tarjeta y/o nombre de usuario), los resellos junto con la actualización mismos datos que para el préstamo.

- En cuanto al uso de los lectores estos utilizaran en menor escala la capacidad de transmisión ya que solo se transmitiría en el momento que entran y salen los maestros.

  Este envío se realizara a través de una aplicación instalada en una máquina puente la cual procesaría la información y seria enviada al servidor. Para el caso de los lectores de los centros de cómputo esto se encontrarían solo en forma local conectados a la PC.

IV.3.2. Aplicación de Compensación o Conciliación

Para cualquier sistema sea cual sea, es muy importante tener el control de todas las posibles entradas y salidas no importando del tipo que sea. Es por ello que dentro del sistema planteado la parte que vigilara la entrada y salida del dinero(o mejor dicho puntos) deberá llevar un control de estos.

Ahora bien aunque este tipo de mecanismos deberán ser definidos mediante una mancuerna entre gente de contabilidad y la parte de diseño del sistema a continuación se describirán algunos de los parámetros que podrían tenerse en cuenta:

- Elementos que permitan hacer comparaciones entre los flujos entrantes y los salientes.
- Generación de gráficas para una mejor comprensión del ciclo del dinero (puntos).
- Un administrador independiente de las otras aplicaciones con acceso único

Conclusiones

Resolución

Como se ha descrito a lo largo de este capitulo el establecimiento de un sistema que utilice tarjetas inteligentes requiere de cierta complejidad. A pesar de ellos también es claro después de explorar todos sus beneficios, que estos pesan mucho mas que sus costos, todos esto claro si el sistema se encuentra correctamente diseñado, implantado y administrado.

El principal problema al hacer una tesis como esta es que al ser en cierto sentido teórica debido a que no puede ser puesta en práctica por motivos económicos y logísticos, no se puede apreciar en su justo sentido. Aun así debido a que como se describió en algunas de sus partes proyectos de estas características (no necesariamente escolar) se han realizado en diversos lugares con resultados plenamente cuantificables y redituables.

Las soluciones propuestas en el presente trabajo se realizaron de modo genérico, es decir no especificando ningún elemento explicito para su construcción (llámensele tarjetas, lectores o terminales), todo esto con el fin de establecer una base de donde partir al empezar un proyecto en toda su forma.

El llevar a cabo este trabajo dentro de la ENEP Aragón podría incentivar a la Universidad entera para adoptarlo lo que generaría que esta tecnología que no es suficientemente conocida (y mucho menos utilizada), pudiera estudiarse y utilizarse en otros proyectos dentro o fuera de la institución.

Entre las áreas de la Universidad donde se podrían aplicar los conocimientos que se describen en el presente documento se encuentran:

- Manejo de los accesos a áreas restringidas tales como Centros de Investigación, zonas de restauración, sectores directivos etc.
- Pago de productos en las tiendas de autoservicio y demás expendios dentro de los campus.
- Administración de estacionamientos
- Controles en la autenticación de páginas Web de la UNAM tales como los servicios de Internet, bases de datos, Biblioteca etc.

Obviamente para la aplicación de la tecnología de las Tarjetas Inteligentes en esto ámbitos deberá además contar con información adicional adecuada (tanto técnica como estructural) conforme a lo que pide cada elemento ya que no sería posible solo hacer una simple transferencia de los elementos aquí descritos ya que cada situación en donde se use la TI es único.

REFERENCIAS

[i] http://www.artes-graficas.org/glosario/glosario.php?T=E
[ii] Smart Card Handbook. W. Rankl y W.Effing Editorial Wiley
[iii] http://www.cardwerk.com/smartcards/smartcard_history.aspx
[iv] http://sharp-world.com/corporate/news/030122.html
[v] http://www.sharpsma.com/sma/Products/Smart-Cards/pdf/Smart_Card_Product_Annoucement.pdf
[vi] http://www.scmegastore.com/st_prod.html?p_prodid=126&p_catid=&sid=3TZJ680-mA7o90z-05104614088.58
[vii] Advanced Advanced Course on Smart Course on Smart Card Card Technology. Gemplus
[viii] http://www.ith.mx/revista_espacio_ith/numero_1/r01_microprocesador.html
[ix] http://www.pchardware.org/historia/index.php
[x] http://www.ith.mx/revista_espacio_ith/numero_1/r01_microprocesador.html
[xi] http://www.dc.uba.ar/people/materias/oc1/h3.html
[xii] http://www.unizar.es/euitiz/areas/aretecel/docencia/micros/recursos/capitulo1.pdf
[xiii] cactus.fi.uba.ar/crypto/tps/tarje.pdf
[xiv] http://www.lafacu.com/apuntes/informatica/memo/default.htm
[xv] Smart Hand Book .W.Rankl Ed:Willey
[xvi] Smart Hand Book .W.Rankl Ed:Willey
[xvii] Smart Hand Book .W.Rankl Ed:Willey
[xviii] http://www.forefront.com.au/tech/eCode.html
[xix] http://www.banksys.be/BKScomwt/fr/prodserv/czampc.htm
[xx] http://www.firstmonday.dk/issues/issue4_4/vanhove/
[xxi] http://capta.com.mx/shopsite_sc/store/html/8d0vproxa.html
[xxii] http://www.smart-cardsys.com/products/downloads/precise100SC2.pdf
[xxiii] http://www.smartcardalliance.org/alliance_activities/Contactless_Technology_whitepaper.cfm
[xxiv] http://faqs.jmas.co.jp/FAQs/technology/smartcards/faq
[xxv] www.philips.com
[xxvi]http://www.toptrend.com.tw/library/product%20line/Atmel/Product%20Pressentation%20Data/RFID%20Presentation%204.11.00.pdf
[xxvii] www.smartcardalliance.org
[xxviii] http://www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm
[xxix] www.ask.fr
[xxx] Smart Hand Book .W.Rankl Ed:Willey
[xxxi] http://www.pcsdigital.com.ni/ni_tecnologia.htm
[xxxii] www.philips.com
[xxxiii] www.philips.com
[xxxiv] http://www.dcc.uchile.cl/~rbaeza/cursos/proyarq/hlopez/node7.html
[xxxv] http://www.cardtech.com.mx/credenciales.php?opc=BMagnetica
[xxxvi] http://www.cardtech.com.mx/credenciales.php?opc=BMagnetica
[xxxvii] http://www.eurosmart.com/4-Documents/Files/pp0001.pdf
[xxxviii] http://www.jrc.es/iptsreport/vol13/spanish/ict2S136.htm
[xxxix] Brett Tyson, "Practical Authentication Techniques; their application and benefits", paper delivered at the *SmartCards '94 Conference*, Sydney Hilton Hotel, 25 and 26th October 1994, p. 4.
[xl] http://www.seds.com/smartcard_etc.html
[xli] http://cactus.fi.uba.ar/crypto/tps/card.pdf
[xlii] Smart Card Handbook W. Rankl
[xliii] http://informatica.aragon.unam.mx/continua/index.html
[xliv] http://www.ugr.es/~aquiran/cripto/expedien/exped005.htm
[xlv] www.redes.upv.es/asnr/transparencias/AlgoriARquc.pdf