



UNIVERSIDAD AUTÓNOMA METROPOLITANA

UNIDAD AZCAPOTZALCO

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

**“SISTEMA DE ACCESO DISTRIBUIDO REMOTO CON ENTIDADES
INFORMÁTICAS”**

PROYECTO DE INVESTIGACIÓN II

PRESENTA

M. en E. MIGUEL GUADALUPE RAMÍREZ FONSECA

DIRECTORES

DR. JOSÉ RAÚL MIRANDA TELLO

DR. JESÚS ISIDRO GONZÁLEZ TREJO

OCTUBRE 2010

ÍNDICE	i
ÍNDICE DE FIGURAS.....	iii
ÍNDICE DE TABLAS.....	v
CAPITULO 1. INTRODUCCIÓN	1
1.1 Justificación.....	3
1.2 Objetivos del proyecto de investigación.....	4
1.2.1 General	4
1.2.2 Particulares	4
CAPITULO 2. ANTECEDENTES Y REVISIÓN DEL ESTADO DEL ARTE	5
CAPITULO 3. ARQUITECTURA GENERAL DEL SISTEMA.....	11
3.1 Arquitectura del sistema de acceso.....	12
3.2 Modelado del entorno de trabajo	15
3.3 Desarrollo e implementación del prototipo de trabajo	16

3.4	Control de acceso vehicular con tecnología rfid.....	18
3.5	Dispositivos y Componentes del Sistema de Control de Acceso con sistemas RFID y tarjetas inteligentes.	20
3.6	Identificación con tecnología rfid	21
3.7	Integración general del Sistema	27
3.8	Avances del Trabajo de investigación.....	31
CAPITULO 4. RECURSOS.....		40
CAPITULO 5. CALENDARIZACIÓN.....		41
REFERENCIAS		42

ÍNDICE DE FIGURAS

Figura 3-1 Esquema general de un sistema de acceso con entidades distribuidas	13
Figura 3-2 Esquema de un sistema de acceso cerrado	13
Figura 3-3 Sistema de Acceso con entidades informáticas	14
Figura 3-4 Diagrama Esquemático del Prototipo de un Sistema de Control de Acceso Vehicular	15
Figura 3-5: Arquitectura conceptual del sistema	17
Figura 3-6 Esquema Conceptual del prototipo para modelar el entorno de trabajo	17
Figura 3-7 Tarjeta Inteligente (Inteligencia, 2007).....	22
Figura 3-8 Tarjeta de Crédito: Banda Magnética	23
Figura 3-9: Elementos que forman una Tarjeta Inteligente	24
Figura 3-10: Tarjeta Inteligente y Lector/Escritor	24
Figura 3-11: Diagrama a Bloques de una Tarjeta Inteligente sin contacto	25
Figura 3-12 Esquema General del Sistema de Acceso y Prototipo	28
Figura 3-13 Esquema General del Sistema de Acceso y Prototipo RFID	28

Figura 3-14 Estructura del área de memoria de la tarjeta inteligente.....	29
Figura 3-15 Diagrama a bloques del procedimiento de autenticación en tres pasos	29
Figura 3-16 Seguridad de punta a punta en un sistema de acceso.....	30
Figura 3-17 Sistema de Control de Acceso Vehicular con un nodo.....	31
Figura 3-18 Diagrama esquemática de un Sistema informático	32
Figura 3-19 Diagrama esquemático de un Sistema RFID con EI	32
Figura 3-20 Pantalla de Inicio del Prototipo de Prueba	33
Figura 3-21 Pantallas de Configuración del Prototipo de pruebas	33
Figura 3-22 Pantalla de Directorio y Control de Acceso Vehicular del Prototipo	34
Figura 3-23 Pantalla del Directorio y Control Vehicular Inicio de registro.....	34
Figura 3-24 Logística de Acceso con TI	35
Figura 3-25 Pantalla de Directorio y Control Vehicular. Alta de usuario	36
Figura 3-26 Pantalla de Control de Acceso del Prototipo	36
Figura 3-27 Pantalla de Gestión e interacción del lector RFID	37
Figura 3-28 Módulo de Lectura de la información de los sectores y bloques de una TI	37
Figura 3-29: Estructura de La Entidad Informática para Control De Acceso Vehicular	38

ÍNDICE DE TABLAS

Tabla 1: Cronología de los sistemas de bases de datos. Fuente: Diseño propio a partir de (Silberschatz, Korth, & Sudarhan, 2006)	8
Tabla 2: Comparación de Sistemas de Gestión de Bases de Datos	9
Tabla 3: Historia de Dispositivos RFID y TÍ's	23
Tabla 4: Recursos utilizados para desarrollar el proyecto	40
Tabla 5 Cronograma de actividades a desarrollar para el desarrollo del proyecto	41

CAPITULO 1. INTRODUCCIÓN

La sociedad está en continua evolución y su desarrollo se ha incrementado en gran medida gracias a la facilidad que hoy en día se tiene para acceder a la información desde cualquier punto geográfico a partir de un gran número de dispositivos fijos o móviles con capacidades de comunicación y cómputo.

Estas facilidades de comunicación y el incremento vertiginoso de la capacidad de cómputo producto de la innovación tecnológica, han permitido la generación, la distribución, el acceso y la manipulación de la información que se requiere para llevar a cabo las diversas actividades culturales y económicas que demanda la sociedad actual, por esta razón, a esta era se le ha llamado “Sociedad de la Información y Conocimiento”.

Es importante mencionar que la UNAM en su portal "Sociedad de la Información y el Conocimiento" (UNAM, 2007), hace hincapié en el paradigma evolutivo y cambiante que potencializa la creación y divulgación de la información utilizando las tecnologías digitales para el manejo del flujo de información, las comunicaciones y los diversos procesos que se encuentran en la sociedad y que da lugar a nuevas formas de organización social y productiva.

Sin embargo, esta misma evolución ha propiciado que se desarrolle un nuevo paradigma informático el cual demanda mayores y mejores cualidades y capacidades de los sistemas informáticos tales como: el rendimiento, la seguridad, la accesibilidad, la disponibilidad, etc. Además, que le permita interactuar con otros sistemas, otros dispositivos y de diversas formas para el uso de una información común.

Este nuevo paradigma informático demanda el diseño, el desarrollo y la construcción de sistemas informáticos que garanticen el acceso a los datos y a su respectiva gestión de una manera más versátil y cuya estructura facilite el desarrollo de los algoritmos o los servicios para adquirir, manejar y actualizar la información con la mayor confiabilidad y rapidez.

Los sistemas de gestión de información han surgido y evolucionado como resultado de la creciente demanda de diversos sectores científicos y sociales, porque en la actualidad se requiere de un entorno seguro y confiable para obtener y manejar la información desde cualquier lugar. Este entorno debe tener de manera integrada un conjunto de servicios ofrecidos por un sistema de acceso distribuido remoto que interactúe con las bases de datos, las cuales deben estar estructuradas para realizar los procesos de adquisición, de gestión, de almacenamiento, de integración, de uso y de visualización de la información.

Al conjunto de datos almacenados se le llama “**Base de Datos**” y al conjunto de programas o aplicaciones que permiten acceder a ellos se les llama “**Sistema Gestor de Base de Datos**”. El objetivo principal del gestor es proporcionar la forma de almacenar y recuperar la información de la base de datos de manera práctica y eficiente además de evitar diversos problemas como serían el de integridad y el de atomicidad. El gestor debe garantizar una respuesta optimizada al acceso concurrente de forma segura y logrando que los procesos de transacción sean rápidos (Silberschatz, Korth, & Sudarhan, 2006).

El presente proyecto de investigación está planteando una solución a la problemática que se presenta en el proceso de acceso a una sola base de datos mediante dispositivos de identificación por radio frecuencia (RFID) de forma remota y distribuida, utilizando un enfoque basado en “**Entidades Informáticas**” (EI). Este tipo de entidades permite la comunicación del sistema, independientemente del dispositivo o medio en que se realice la transmisión de la información.

El enfoque basado en Entidades Informáticas pretende que la información contenida en una base de datos central pueda ser consultada e incluso gestionada por los usuarios en su modalidad local ya sea por terminales, por etiquetas RFID, tarjetas inteligentes RFID e incluso por otros dispositivos inteligentes de manera remota.

Esto significa tener componentes informáticos pequeños que mediante sus EI interactúen para realizar tareas específicas y de esta manera obtener el acceso a una cantidad mayor de elementos informáticos como servicios distribuidos apoyados en diversas tecnologías

de conectividad y comunicación, siendo la predominante la tecnología que ofrece la Web con sus protocolos estándar que permiten la vinculación con prácticamente cualquier sistema informático del mundo.

1.1 JUSTIFICACIÓN

En la actualidad se cuenta con aplicaciones muy robustas para acceder a los datos sin importar que se encuentren almacenados en una base de datos local, en una base de datos distribuida o si los datos se encuentran dispersos. Se dice que son robustas porque estas aplicaciones son hechas o proporcionadas por un sólo proveedor y dependen en gran medida de los dispositivos o componentes que lo forman (Hardware). Esto crea una desventaja ya que si los proveedores o realizadores son diferentes, aumenta la probabilidad de presentarse problemas para el acceso a estos datos con rapidez, confiabilidad y seguridad.

En este proyecto de investigación se aplican los conocimientos adquiridos en la maestría en áreas informáticas de creciente importancia como lo son los sistemas de bases de datos y la complejidad inherente que implica su acceso, el análisis del flujo de la información del sistema y de los diversos servicios que lo constituyen; la gestión de la base de datos junto con los procesos inherentes para realizar la transferencia de la misma así como las transacciones entre la gran cantidad de dispositivos con los que hoy en día se puede acceder a la información contenida en las bases de datos.

El objetivo del desarrollo de un sistema informático donde se simulen los procesos de acceso a los datos mediante un modelo basado en entidades informáticas, es el estudio y la integración de medios ya disponibles por tecnologías nuevas, para dar una respuesta a los problemas que se deben resolver al integrarse como un sistema e identificar las variables más significativas que aumentan o disminuyen la operatividad.

Para lograr un buen acoplamiento en el sistema de acceso, se propone usar el concepto de “**Entidad Informática**”, que en la presente tesis se define como un objeto cuya estructura permite la gestión a un conjunto de servicios para realizar transacciones de información en una base de datos desde cualquier lugar y desde cualquier dispositivo. Posibilita también el manejo de la información desde aplicaciones de otros proveedores.

En relación a los recursos necesarios para el proyecto de investigación, se hará uso de un sistema mínimo de hardware para la simulación de un control de ingreso vehicular con acceso a una base de datos central desde dispositivos con lectura/escritura de tarjetas inteligentes, con la capacidad de manejar sistemas de control basados en controles lógicos programables (PLC) o dispositivos de E/S inteligentes con protocolo de comunicaciones Modbus RTU y computadoras.

1.2 OBJETIVOS DEL PROYECTO DE INVESTIGACIÓN

1.2.1 General

Analizar, desarrollar e implementar un Sistema de Acceso Distribuido remoto con un paradigma basado en “Entidades Informáticas” que permita gestionar la información contenida en una base de datos central de manera dinámica con medios informáticos remotos sin importar de que proveedor sean.

1.2.2 Particulares

- i. Diseñar y desarrollar un sistema de acceso basado en Entidades Informáticas que sea capaz de comunicarse en forma remota con dispositivos de lectura/escritura de etiquetas RFID's, de tarjetas inteligentes o con módulos de automatización de procesos.
- ii. Analizar y evaluar los elementos que integran y que interactúan en el sistema de acceso
- iii. Determinar los parámetros relacionados con la rapidez, la confiabilidad y la seguridad con nodos remotos multiacceso.
- iv. Diseñar y desarrollar un gestor de acceso que permita la transferencia de la información que requiera el sistema.
- v. Evaluar el sistema desarrollado en su totalidad.
- vi. Escribir y presentar un artículo en un congreso.
- vii. Documentación y escritura de la tesis.

CAPITULO 2. ANTECEDENTES Y REVISIÓN DEL ESTADO DEL ARTE

En este capítulo se describen los trabajos de investigación publicados por otros autores que se encuentran relacionados con el proyecto investigación. Asimismo, se presenta antecedentes de cómo han evolucionado los sistemas de gestión de información. En cada uno de ellos se plantean los siguientes puntos: publicaciones, inducción a las bases de datos, reseña breve de la evolución de los sistemas de gestión de datos.

Otros puntos no son tratados ya que son del tipo aplicativo como lo es la implementación de los sistemas de automatización, redes de conectividad entre los sistemas de control, protocolos de comunicación industrial, etc., sin embargo, durante el desarrollo de la tesis si se requiere se integran cuando sus variables influyen sobre los objetivos de la investigación.

Automatic Control of Students' Attendance in Classrooms Using RFID

Las tecnologías de identificación automática por RFID están actualmente de moda y si bien hay mucho desarrollado se siguen abriendo campos nuevos de investigación. Silva, Filipe y Pereyra en la tercera conferencia internacional de Sistemas y redes de comunicaciones del 2008 así lo plantearon en su trabajo de investigación que se enfoca al acceso de áreas restringidas mediante el uso de un sistema que utiliza RFID distribuido con RFID sobre Ethernet en una institución educativa y la problemática que día a día se tiene. (Silva, Pereyra, & Filipe, 2008).

Este trabajo de investigación se abocó al registro de todos los estudiantes que serán atendidos en una clase y teniendo la información actualizada para ser consultada por el

alumno y maestro, así como validar la información y cuantos alumnos están siendo atendidos en una clase en particular en instituciones con más de 200 salones y aproximadamente 3000 estudiantes. Se utilizaron lectores UHF, tags pasivos, Linux, un servidor de monitoreo central y archivos binarios y de texto en una base de datos central.

A Collaborative Access Control Based on XACML in Pervasive Environments

Kyu y sus colegas (Kyu, Hyuk, Won, & Eun, 2008) presentaron una investigación de control de acceso remoto en ambientes dominantes en sistemas de red heterogéneas pudiendo tener servicios web diversos que comparten de manera colaborativa la información.

Se basa en un enfoque en el que predominan las políticas de acceso que garantizan la seguridad en los servicios web, las regiones de ubicación geográficas (espacio y/o puntos geográficos) y el tiempo de respuesta global dado que se involucran recursos web, dispositivos móviles y redes inalámbricas.

Para ello se utiliza XACML (eXtensible Access Control Markup Language) que es un lenguaje basado en XML para la protección de datos empresariales y que fue desarrollado y aceptado por OASIS como estándar XACML. Este lenguaje se basa en la petición/respuesta que sirven para realizar e integrar algoritmos con políticas que expresan autorización con propósitos colaborativos en el control de acceso en ambientes dominantes utilizando el enfoque de control de acceso basado en reglas (RBAC) para que sólo accedan usuarios autorizados.

Base de datos y sistemas de gestión de base de datos

El objetivo principal de una base de datos es almacenar información de forma segura y facilitar el proceso de acceso para la modificación o recuperación de ésta. Las Bases de Datos también han evolucionado de acuerdo al desarrollo tecnológico de los sistemas de cómputo y de los medios de almacenamiento. En la Tabla 1 se muestra una breve cronología de su evolución desde el enfoque de gestión de los datos.

Para que una base de datos permita a los usuarios el acceso a los datos, se necesitan lenguajes de aplicación y los sistemas que integran la base de datos actuales proporcionan para este fin lenguajes que definen los datos y estructuran el esquema de la base de datos. También, se requiere de un lenguaje que permita su manipulación para expresar consultas y se pueda modificar la base de datos.

El lenguaje de manipulación de datos permite recuperar información, insertar nueva información, borrar y modificar la información y pueden ser de dos tipos: Lenguajes de manipulación de datos procedimentales donde el usuario especifica que datos se necesitan y como obtenerlos; y el lenguaje de manipulación de datos declarativo donde solo se necesita especificar que datos se requieren sin especificar cómo obtenerlos (Silberschatz, Korth, & Sudarhan, 2006).

La especificación de las propiedades de los datos y sus definiciones se realizan mediante un lenguaje de definición de datos. La estructura de almacenamiento y sus métodos de acceso utilizados por el sistema de base de datos se especifican con comandos propios de este lenguaje.

Mediante este lenguaje se dan las restricciones de dominio a cada atributo es decir si el dato es para declarar si es de tipo “entero” o tipo “fecha”. Otras restricciones serían las de integridad referencial y las de autorización entre otras.

Los sistemas de bases de datos han integrado lenguajes de consulta como el “Structured Query Language” mejor conocido como SQL, el cual se ha convertido en un estándar de los Sistemas de Gestión de Base de Datos Relacionales. También se han integrado a los sistemas manejadores de bases de datos la Interface Gráfica de Usuario (GUI: Graphical User Interface) para una interacción más amigable (Moreno, 2008).

Los lenguajes orientados a objetos también han posibilitado el acceso a las bases de datos de forma remota mediante ODBC (Open Database Connectivity), que garantiza el acceso a la base de datos. También se han desarrollado y evolucionado sistemas de gestión orientados a objetos (ODBMS: Object Database Manager System) así como lenguajes de consulta a objetos (OQL: Object Query Language).

Años	Evolución
Década 50's	Lectura sincronizada y secuencial. Tamaño de datos mayor que la memoria principal. Uso de cintas magnéticas para almacenar los datos y uso de tarjetas perforadas. La gestión de información procesaba los datos en orden determinado, mezclando los datos de cintas y de tarjetas perforadas.
Década 60's y 70's	Acceso Directo a los datos de manera aleatoria debido al almacenamiento basado en discos duros. Base de datos de red y jerárquicas con gestión de datos con estructura en listas y árboles para su almacenamiento y acceso. Modelo relacional (Modelo CODASYL -Edgar Frank Codd 1970) basado en grafos de relaciones entre datos. Diseño de Base de Datos: Modelo Entidad- Relación (P. Chen 1976) 1ª. Generación del sistema de Gestión de base de datos Sistema IMS (Information Management System) de IBM
Década 80's	Desarrollo de técnicas para la construcción de BD's relacionales eficientes (Suste, R) Primer Producto de Base de Datos Relacionales SQL/DS se enfoca a aplicaciones de procesamiento de transacciones Sistemas Comerciales:DB2 (IBM), Oracle, Ingres y Rdb (DEC).
Década 90's	Enfoque centrado en desarrollo a nivel lógico por parte del programador Diseño de lenguaje SQL(Structured Query Language) de IBM orientado a la toma de decisiones y consultas Base de Datos Paralelas Soporte relacional orientado a objetos en bases de datos. Sistemas con bases de datos con tasas de transacciones muy altas; demandas de alta confiabilidad y alta disponibilidad.
Siglo XXI	Interfaces Web para las bases de datos XML y su correspondiente lenguaje de consulta estructurado XQUERY Técnicas de "Informática Autónoma/Administración Informática para minimizar el esfuerzo de administración.

Tabla 1: Cronología de los sistemas de bases de datos. Fuente: Diseño propio a partir de (Silberschatz, Korth, & Sudarhan, 2006)

Las consultas son importantes en las bases de datos y en relación a los sistemas orientados a objetos, OQL es un lenguaje de consultas muy similar a SQL pero con muchas más habilidades. Su diferencia principal es que SQL es que actúa en base a relaciones y entidades y OQL actúa sobre los objetos y no sobre las relaciones (Tari & Bukhres, 2001).

Actualmente SQL ha evolucionado para ser un sistema de gestión de base de datos orientado a objetos que incluye relaciones entre las entidades para las consultas. En la Tabla 2 se muestra una comparación entre los sistemas de gestión de base de datos, se puede observar su evolución que prácticamente sigue vigente a la fecha.

Comparación de sistemas de Gestión de Base de Datos			
Criterio	RDBMS	ODBMS	ORDBMS
Standard para definir	SQL2	ODMG-2.0	SQL3
Soporte con características orientados a objetos	No lo soporta; Es difícil mapear una programa entre el objeto y la base de datos	Amplio Soporte	Soporte limitado; Muchos tipos de datos
Uso	Fácil de usar	Bien para programadores; Algún acceso de SQL ACCESS para usuarios finales.	Fácil de usar excepto por algunas extensiones
Soporte para relaciones complejas	No soporta tipo de datos abstractos	Soporta una gran variedad de tipo de datos y interrelaciones complejas.	Soporte a tipo de datos abstractos y relaciones complejas
Desempeño	Bueno desempeño	Relativamente menos eficiente	Altas expectativas de excelente desempeño
Madurez del producto	Relativamente viejo y muy maduro	Este concepto tiene un par de años y es relativamente maduro	Todavía está en el proceso de desarrollo e implantación
Uso de SQL	Apoyo extensivo de SQL	OQL es similar a SQL, pero con características adicionales como "Complex objects" y "object-oriented features"	SQL3 está siendo desarrollado con características orientadas a objetos para incorporarlas.
Ventajas	Su dependencia de SQL, y su optimización de consultas es relativamente fácil para consultas sencillas	Puede manejar todo tipo de aplicaciones complejas, puedes reusar el código	Habilidad de consultar aplicaciones complejas y la habilidad de manejar aplicaciones grandes y complejas
Desventajas	Inhabilidad a manejar aplicaciones complejas	Desempeño pobre para consultas complejas y es inhábil para sistemas de gran escala.	Desempeño pobre en aplicaciones del web
Soporte posventa	Ha tenido un gran éxito. Tiene un extenso mercado y muchos vendedores	En el presente, falta el apoyo de los vendedores por el tamaño del mercado de RDBMS	Tiene un buen futuro. Parece que todo los vendedores de RDBMS quieren este producto
Recursos: International Data Corporation, 1997 (Devarakonda, 2001)			

Tabla 2: Comparación de Sistemas de Gestión de Bases de Datos

Estos sistemas de gestión de bases de datos son costosos y la curva de aprendizaje y especialización en ellos es alta, por lo que desarrollar sistemas de gestión de bases de datos a partir de Entidades Informáticas puede ser una mejor opción. De aquí la importancia y el interés de modelar sistemas de estructuras de datos que posibiliten el acceso a la información a bajo costo, con seguridad, confiabilidad y rapidez.

La forma en que se organizan los datos ha tenido también varios enfoques, siendo los más representativos el de Redes, el Jerárquico, el Relacional, el Orientado a Objetos y el de Bases de Datos Lógicas (Date, 2003).

Otro enfoque en cuanto a la forma de estructurar y organizar los datos es mediante modelos que se enfocan a la estructura de la base de datos y que mediante un conjunto de herramientas conceptuales, describen sus datos, sus relaciones, su semántica y las restricciones de consistencia. Estos permiten describir el diseño de la base de datos en los niveles lógico, físico y de interface gráfica. Estos modelos son el Relacional, el Entidad-relación, el Orientado a Objetos y el de Datos Semi-estructurados (Silberschatz, Korth, & Sudarhan, 2006).

CAPITULO 3. ARQUITECTURA GENERAL DEL SISTEMA

La metodología utilizada para desarrollar la arquitectura del sistema se estructura tomando como eje central un paradigma basado en “Entidades Informáticas” y se utiliza un entorno de trabajo que permita el desarrollar diversas estrategias que permiten el estudio de la gestión de la información interactuando con un sistema de control y dispositivos de Entrada y salida (sensores y actuadores) de manera autónoma o interactuando con una base de datos de forma remota.

El diseño de la arquitectura utiliza tecnología RFID la cuál esta actualmente integrándose en diversas áreas por la portabilidad que tienen y además porque puede almacenarse información de manera segura.

Esta tecnología RFID posibilita realizar investigaciones científicas que propicien desarrollos encaminados a sistemas confiables en la autenticación e incluso en el manejo de información personal.

En el presente proyecto se implementa y aplica en un sistema de control de acceso vehicular. Tiene como etapa inicial el desarrollar y construir un entorno de trabajo donde convergen tecnologías RFID diversas en hardwares y software usando tarjetas inteligentes y etiquetas pasivas.

Para la cuantificación de datos y observación de resultados se necesita una plataforma de trabajo con hardware propio que permita simular el control de acceso vehicular con la suficiente versatilidad y flexibilidad (se pretende que a futuro puedan incorporarse

dispositivos con capacidades de cómputo y conectividad diversa sin cambiar el hardware principal).

En la segunda etapa se desarrolla un gestor de información para la interactividad entre: los dispositivos de lectura, la autenticación y en caso de requerirse con las bases de datos ya existentes; los diversos dispositivos de sensado y de ingreso de información así como los dispositivos de control, sensores, actuadores y elementos de visualización sin usar el modelo basado en entidades informáticas.

El tercer eje y motivo principal del presente estudio es el uso de un paradigma basado en entidades informáticas cuyo enfoque se basa en un conjunto de elementos abstractos, estructurados y definidos a partir de la información solicitada por el gestor de la base de datos y del dispositivo que requiere el acceso.

3.1 ARQUITECTURA DEL SISTEMA DE ACCESO

La arquitectura desarrollada busca la gestión de la información con el fin de tener acceso a los datos del usuario del vehículo; a la identificación utilizando Entidades Informáticas; a la distribución de los datos como resultado de su gestión; a administrar la conectividad entre los diversos componentes del sistema y a garantizar las transacciones de información entre los componentes del sistema.

La figura 3.1 muestra en forma de un esquema general el sistema, mostrando dispositivos diversos en cuanto a capacidades de comunicación, conectividad, manejo de información y que actualmente son comunes como lo son computadoras portátiles, celulares, PDA's, terminales, etc.

También muestra la infraestructura de trabajo en cuanto al hardware a servidores, almacenamiento y aplicaciones interactuando con usuarios y dispositivos. Para el presente trabajo se usarán los dispositivos que correspondan a tecnología RFID.

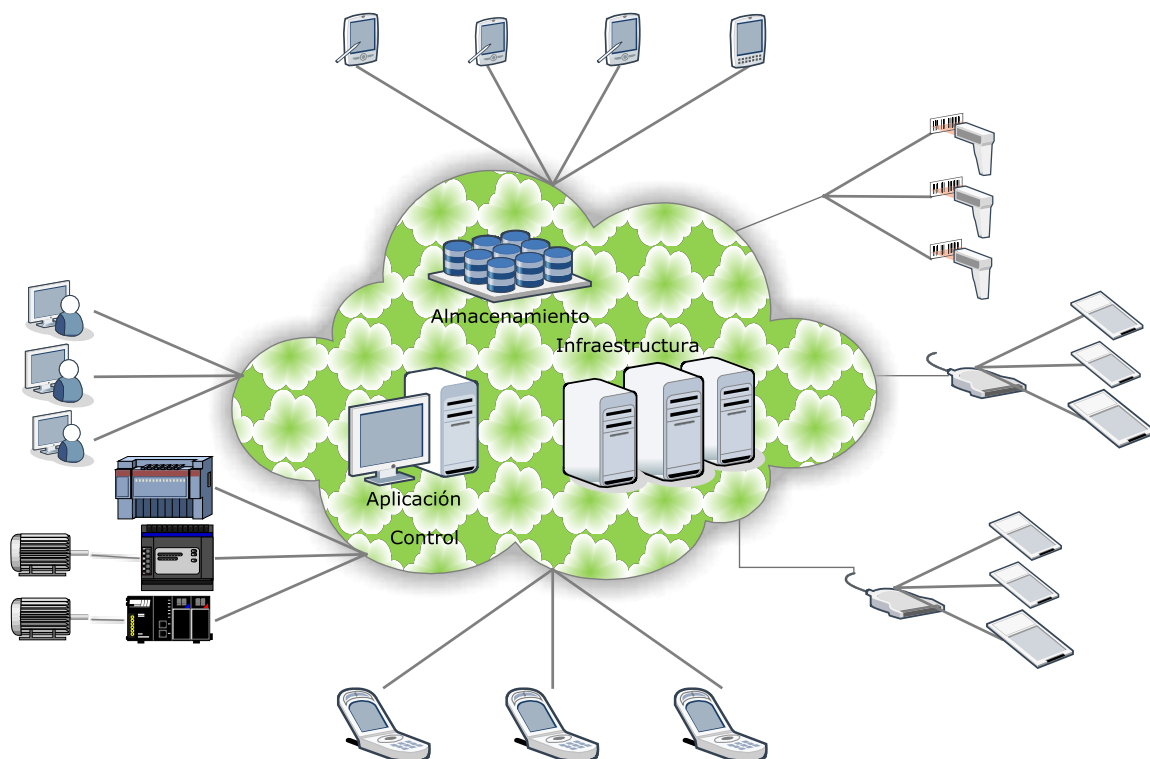


Figura 3-1 Esquema general de un sistema de acceso con entidades distribuidas

Esta arquitectura posibilita varias estrategias de solución en lo que respecta al diseño del sistema informático, la figura 3.2 lo esquematiza resaltando el hecho de que cada proveedor utiliza su propio hardware y ofrece soluciones cuya restricción es que son sistemas cerrados y aunque actualmente hay mas conectividad se tiene un costo en cuanto a tiempo y rendimiento.

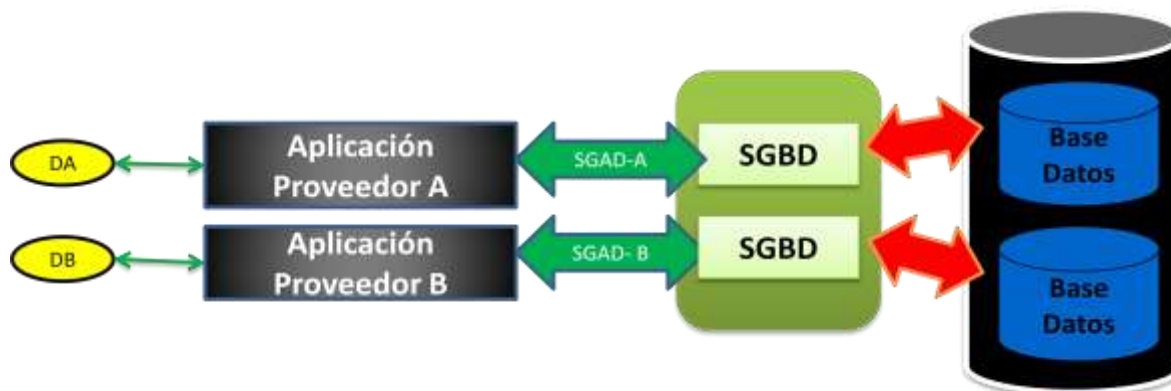


Figura 3-2 Esquema de un sistema de acceso cerrado

La arquitectura informática que se propone basado en el paradigma basado en entidades informáticas se muestra en la figura 3.3 y sigue el enfoque en que esta arquitectura permitirá actualizar, agregar, eliminar, modificar o gestionar la información obtenida de acuerdo a los requerimientos propios de las diversas aplicaciones colaborando entre si y adicionalmente facilitar su análisis. (Bass, Kazman, & Clementes, 2003)

En un sistema de acceso distribuido físicamente pero con acceso lógico remoto no solamente pueden intervenir varias computadoras, sino también diversos dispositivos (D_1 , D_2) con capacidad de comunicación y poder de cómputo. El objetivo, como se mencionó anteriormente, es acceder a la información contenida en una base de datos mediante objetos abstractos que corresponderán a cada dispositivo o computadora para el tratamiento automático de la información y así facilitar al sistema en general el acceso a la información mediante un solo sistema de gestión de información como puede observarse en esta Figura.



Figura 3-3 Sistema de Acceso con entidades informáticas

Este enfoque ofrece también la ventaja de que el sistema tiene la capacidad de integración creciente, dado que permite cambiar los componentes existentes o agregar nuevos componentes cliente a la arquitectura, sin preocuparse por los demás entidades informáticas, ya que éstas operan de manera independiente. Aunado a esto, el sistema resultante tiene la posibilidad de interactuar de manera colaborativa.

En este proyecto, se utiliza una arquitectura estratificada y orientada a objetos, en la cual los componentes del sistema se integran de manera encapsulada, esto es, los datos, las operaciones, el estado y cualquier otra posible información que permita la coordinación y la comunicación entre las entidades según requieran las diversas transacciones. Además,

se trabajará en capas, donde en cada una de ellas se realizan procesos, desde la capa de interface con el usuario hasta la capa de gestión con la base de datos.

La seguridad, la rapidez y la confiabilidad son algunos de los aspectos más importantes de la investigación, la estructura de datos que será conformada, así como la base de datos y su normalización serán definidas dentro del desarrollo del proyecto mismo de acuerdo con las filosofías descritas en la sección del estado del arte.

3.2 MODELADO DEL ENTORNO DE TRABAJO

Para el entorno de trabajo, se desarrolló y trabajó con un prototipo que permite el estudio de la interacción entre las Entidades Informáticas y los componentes que conforman el sistema para lograr los objetivos planteados.

La arquitectura de la figura 3.4 se utilizó para el modelado del entorno de trabajo con el fin de delimitar el estudio y análisis de la información provenientes de sistemas con tecnología RFID. Este prototipo del sistema de acceso se construyó simulando un Sistema de Control de Acceso Vehicular a partir de tarjetas inteligentes con conectividad a una base de datos. El sistema operativo puede ser Windows XP o Windows Vista/Windows 7. Se diseñó una plataforma de trabajo y una Interface Gráfica de Usuario mediante el lenguaje de programación de alto nivel orientado a objetos Visual Basic.

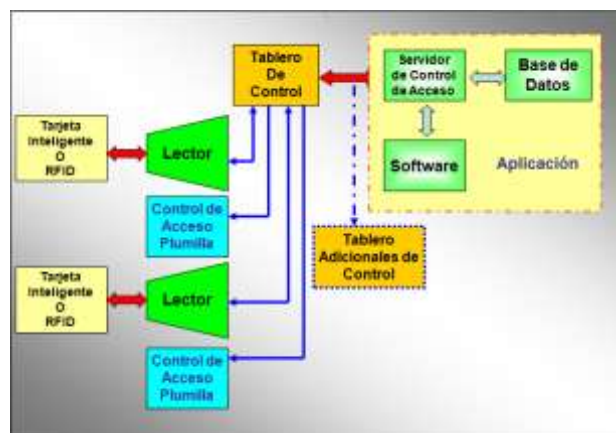


Figura 3-4 Diagrama Esquemático del Prototipo de un Sistema de Control de Acceso Vehicular

3.3 DESARROLLO E IMPLEMENTACIÓN DEL PROTOTIPO DE TRABAJO

El prototipo base gestiona el acceso vehicular mediante un control electrónico. Este prototipo permite modelar por secciones el sistema al integrar de forma progresiva los componentes necesarios para lograr un análisis a detalle, por etapas y de forma simple, del comportamiento del sistema de acceso con entidades informáticas

Las computadoras o dispositivos que pueden interactuar con una base de datos tienen su propio sistema operativo, kernel o aplicación así como diferentes modos y medios de comunicación. En los sistemas de control industrial se utilizan diversos protocolos de comunicación como lo son el ASCII, modbus, etc. Los medios de comunicación más comunes son el infrarrojo, el bluetooth, el zigbee, por cable, el enlace telefónico, la telemetría, etc.

Por lo anterior, estudiar la respuesta del sistema de acceso desde un paradigma basado en Entidades Informáticas para homogenizar criterios de estructura de datos, es una temática interesante e incluso indispensable para evaluar rapidez, confiabilidad y seguridad y si bien en el presente trabajo de investigación se delimita a tecnología RFID pueden integrarse otras alternativas tecnológicas como las arriba mencionadas.

Las ventajas de utilizar Entidades Informáticas es que se pueden utilizar dispositivos comunes tales como computadoras, celulares, PDA's, terminales, tarjetas inteligentes RFID, etc. Además, se puede determinar el tiempo promedio óptimo para las transacciones de acuerdo al tipo de dispositivo.

Las Figuras 3.5 y 3.6, esquematizan el sistema en conjunto y el prototipo base sólo desde el punto de vista de hardware. Muestra también, algunos de los dispositivos para desarrollar la estructura de datos más adecuada y lograr los objetivos de la investigación.



Figura 3-5: Arquitectura conceptual del sistema

Una vez desarrollado el prototipo y el entorno operativo, sigue la estructura de datos que conforman las Entidades Informáticas. Posteriormente se elaboran los algoritmos necesarios evaluar las Entidades Informáticas, los componentes asociados, los procesos y las transacciones que como flujo de datos posibilitan la gestión de información para su transformación o transferencia.



Figura 3-6 Esquema Conceptual del prototipo para modelar el entorno de trabajo

3.4 CONTROL DE ACCESO VEHICULAR CON TECNOLOGÍA RFID

Un Sistema de Control de Acceso permite el ingreso a espacios o áreas que requieren autenticación la cuál puede tener diferentes niveles de acuerdo al nivel de seguridad y control exigido.

Seguridad, Autonomía y Control son tres de las variables que definen los límites en los requerimientos en cuanto a tecnología e investigación en áreas informáticas y su interactividad con el mundo físico.

La seguridad es una variable importante ya que permite la identificación del objeto, usuario, etapa del proceso, etc. La autonomía se define en relación al nivel de intervención humana y el control estará en función de la toma de decisiones para dar los permisos relacionados con la identificación.

El control de acceso podrá proporcionar los registros de entrada y salida del personal, de vehículos, de mercancías, etc., dentro de una o más áreas determinada o bien para su localización.

Esta labor se ha desarrollado de diferentes formas y con diferentes tecnologías siendo uno de los sistemas más utilizado, y por lo tanto el más común; el de aprovechar y utilizar personal de vigilancia para llevar el control de entradas y salidas mediante bitácoras, registros y asignación de gafetes o tarjetas con permisos a veces basados en colores.

Lo mismo sucede con el control de acceso de los vehículos de usuarios para ingresar a ciertos lugares e incluso tener acceso a determinadas áreas o secciones de estacionamiento, lo cual dependerá de los privilegios y permisos que hayan sido otorgados.

En la actualidad, se están utilizando dispositivos que permiten el acceso de manera automática utilizando sistemas de control en base a la identificación correspondiente y los

datos obtenidos a través de boletos de papel cuyo fin es cobrar por tiempo de uso de un estacionamiento y solo se basa en la habilitación de plumillas para permitir o no el acceso.

Sin embargo las nuevas tecnologías proveen de dispositivos tales como tarjetas de plástico que contienen un número de identificación asociado a un usuario ya sea utilizando cinta magnética, código de barras, tarjetas inteligentes de contacto, tarjetas inteligentes de proximidad, etiquetas pasivas, teclados, lectores biométricos, etc.

El uso eficiente y eficaz de las tecnologías actuales junto son sistemas informáticos que posibilite llevar el control de quien ingresa o egresa, hora de entrada y salida, horas acumulados, permisos programados, estadísticos, etc., requiere el usar sistemas informáticos para la gestión de la información y en consecuencia la toma correcta de decisiones.

Los sistemas de bases de datos local, distribuida, redundante, sincronizada, etc, y con estrategias de interacción eficiente deben acoplarse con los sistemas de control basados en microcontroladores, PLC's (Controles Lógicos Programables) u otros similares, además del uso de interfaces visuales, todo esto hace indispensable la investigación sobre la gestión de estos sistemas de bases de datos.

Los sistemas de control de acceso han estado adquiriendo cada vez mayor importancia dentro de las diversas organizaciones del mundo, desde las pequeñas empresas hasta los grandes corporativos e instituciones gubernamentales, incorporando nuevas tecnologías a estos sistemas para que cada día sean más autónomos, inteligentes y seguros.

Para el presente proyecto se utilizan las tarjetas inteligentes (TI) como elementos para identificar a una persona o un vehículo, siendo sus aplicaciones más empleadas como monedero electrónico, registro de personas en diversos sitios como hoteles, empresas, áreas restringidas, eventos, reservaciones, máquinas automáticas, etc.

3.5 DISPOSITIVOS Y COMPONENTES DEL SISTEMA DE CONTROL DE ACCESO CON SISTEMAS RFID Y TARJETAS INTELIGENTES.

El entorno de trabajo del sistema de Control de acceso propuesto está compuesto de los siguientes componentes.

- Credencial de Identificación (Etiqueta o Tarjeta Inteligente)
- Lector de acceso (Lector de etiquetas, lector de tarjeta inteligente¹)
- Automatismo de cierre y apertura
- Panel de Control
- Servidor de Servicios de Control de Acceso
- Software
- Base de datos

¹ Los “Lectores” de tarjetas inteligentes pueden tanto leer como escribir en la tarjeta inteligente.

3.6 IDENTIFICACIÓN CON TECNOLOGÍA RFID

Desde mediados del siglo pasado, por los años cincuentas el uso de las tarjetas de plástico se hizo común para identificarse mediante la impresión sobre la misma y una de sus aplicaciones fue como un almacén de información. Posteriormente se le incorporo una banda magnética sobre ella lo cual facilito que pudiese almacenar información digital y con los dispositivos apropiados de lectura poder ser recuperada.

Sin embargo, un requerimiento importante para su uso fue el aumentar la seguridad de la información contenida en estas tarjetas debido a que, con los dispositivos de lectura adecuados, se podría acceder a esta información alojada en la cinta magnética y dado que se utilizaban para hacer transferencias en tiempo real en las diversas redes, se tuvo que adicionar una mayor seguridad que permitiera a su vez una mayor confianza en las transacciones realizadas y/o la autenticación del portador. Técnica que hasta la fecha se sigue usando pero que sigue siendo alto su costo por la transmisión de información.

Una tarjeta inteligente o SmartCard, figura 3.7, expresada en los términos más simples, es una tarjeta con un chip integrado lo cual permite proporcionar un alto nivel de seguridad basado en algoritmos para poder integrar en la memoria de este tarjeta inteligente (TI) claves, y que, además, nos permitan un alto nivel de confiabilidad. Esto ha permitido el desarrollar una gran cantidad de aplicaciones de todo tipo (Betarte, 2000).

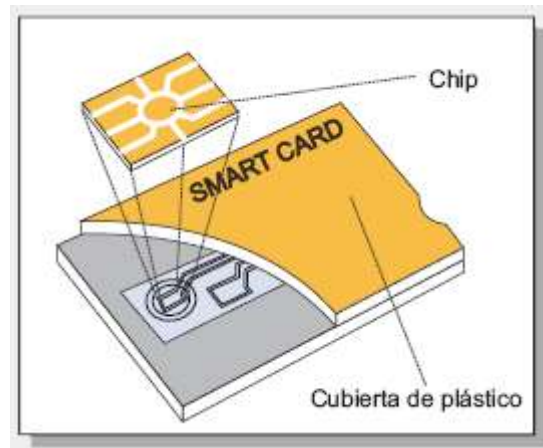


Figura 3-7 Tarjeta Inteligente (Inteligencia, 2007)

Para el presente trabajo se enfatizará en los sistemas de identificación actuales que permitan el acceso o bien permita tener la información necesaria con fines de transacciones, estadísticos o información segura como son las tarjetas RFID (TRFID) y las inteligentes (TI).

En la tabla que se muestra a continuación se hace un breve historial de los sistemas RFID y las TI.

Años	Eventos Siglo XX
40's	Los militares estadounidenses utilizan el sistema RFID desde la Segunda Guerra Mundial para el reconocimiento a distancia de los aviones: Friend or Foe (amigo o enemigo).
1969	Mario Cardullo registra en Estados Unidos la primera patente con tecnología RFID, utilizada para identificar locomotoras.
70's	La tecnología RFID se sigue utilizando de modo restringido y controlado, por ejemplo, para la seguridad de las plantas nucleares.
80's	La primera aplicación de la tecnología RFID, en Europa, es la identificación del ganado en el sector privado. Luego llegan muchas otras utilizaciones comerciales, en particular en las cadenas de fabricación de la industria del automóvil.
90's	<ul style="list-style-type: none"> • Miniaturización del sistema RFID: IBM integra la tecnología en un solo chip electrónico. • Aparece el estándar Mifare de 1 k (94). Se utiliza en el sistema de transporte en Seul (96). • Se desarrolla TI Mifare con coprocesador 3DES y PKI



Figura 3-9: Elementos que forman una Tarjeta Inteligente

La tarjeta inteligente presentada es de material plástico y que responde a los estándares ISO/IEC 7810 en cuanto a resistencia y flexibilidad, sus medidas son de 8.56 cm de largo y 5.398 de ancho con un espesor de 0.076 que permite que sirva de soporte tanto para el chip, contactos y demás conectores y dispositivos externos. (Ver *Figura 3-10: Tarjeta Inteligente y Lector/Escritor*)

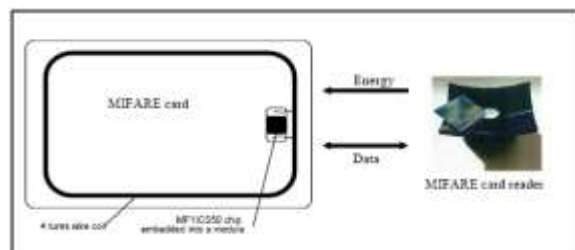


Figura 3-10: Tarjeta Inteligente y Lector/Escritor

Las primeras SC fueron conocidas como “Memory Cards” (MC), y solo podían contener datos de manera temporal y permanente. Posteriormente incorporaron un procesador de 8 bits y 5 Mega Hertz de velocidad con el estándar de comunicación serial de 9600 bps, con contacto o sin contacto. De ahí proviene el nombre de “Tarjeta Inteligente”.

De acuerdo a sus características pueden ser clasificadas como: a) TI con un circuito integrado (CI) de memoria de solo lectura; b) TI con CI y un microprocesador (μP) con conexión por contacto físico y c) TI con CI con μP y conexión electromagnética, (Angel, 2001) como se muestra en la *Figura 3-11: Diagrama a Bloques de una Tarjeta Inteligente sin contacto*

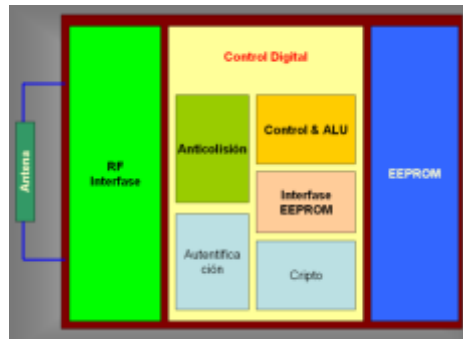


Figura 3-11: Diagrama a Bloques de una Tarjeta Inteligente sin contacto

La información que se almacena en una tarjeta inteligente tiene un alto nivel de seguridad, proporcionan una plataforma de gran portabilidad y permite además realizar una gran variedad de aplicaciones que pueden desarrollarse en diversos lenguajes de programación como puede ser Visual Basic, C, Java, etc.

Esta versatilidad ha producido que se tenga una creciente demanda de aplicaciones desarrolladas con tarjetas inteligentes y el abordar esta tecnología para investigar sus diversos elementos y desempeño con una visión actual e integral hace interesante usarla para innovar soluciones que optimicen la funcionalidad de una gran cantidad de procesos que se tiene en la Universidad de manera conjunta y segura. Por lo pronto se enfocará al control de acceso vehicular.

El uso de las tarjetas inteligentes pueden cubrir aplicaciones como: Monedero electrónico, pago de facturas, etiquetas RFID (Identificación por Radio Frecuencia), gestión de la información y estado académico del estudiante, seguridad y control de acceso, servicios financieros, teléfonos celulares, accesos a la red, aplicaciones para comunicaciones y telemetría, etc.

Estas tarjetas inteligentes han sido diseñadas de manera similar a una credencial o una tarjeta de crédito y que incluso ya tienes funciones de crédito, débito e identificación personal al tener hasta 10 MB de memoria para ser usada para almacenar información.

Deben cumplir con la norma internacional ISO 7816 que ha sido aceptada para las tarjetas inteligentes y que se enfoca a los aspectos de interoperabilidad de tarjetas inteligentes de comunicación en relación con las características, propiedades físicas y la aplicación de los identificadores de chip implantado y los datos. Incluye once categorías que se están actualizando constantemente. (TechFaq, 2008).

La seguridad es importante y por ello las TI's² tienen gran aceptación porque además de permitir una buena portabilidad para el resguardo de claves privadas pueden ser utilizada para otras aplicaciones y por lo tanto proporcionar otros beneficios como puede ser el tener un carnet de salud, el utilizarse como monedero electrónico, como tarjetas de prepago telefónico o de uso de pasaje, identificación para acceso a áreas restringidas, tarjetas de crédito o débito bancario, tarjetas de prepago telefónico o de abordaje, certificados digitales o para autenticarse en redes de seguridad informática y un sinnúmero de aplicaciones más.

Actualmente se están integrando múltiples servicios en las tarjetas inteligentes aprovechando la versatilidad que presentan éstas y no solamente en un entorno restringido como puede ser una institución educativa, gubernamental u otra sino que es muy probable que se vuelva una forma de tener una identificación universal sobre todo si se conjunta con elementos de seguridad adicionales tal como puede ser el utilizar elementos biológicos o biométricos del cuerpo humano (huellas dactilares, reconocimiento de voz, de iris u otros).

Una aplicación posible es el control y administración de los vehículos que ingresan y salen de la unidad Azcapotzalco y de esta manera apoyar al proceso actual de control de acceso vehicular de una manera más sistémica al utilizar las nuevas tecnologías de comunicación e información.

² Las TI's (Tarjetas Inteligentes) también son conocidas como SmartCards

Actualmente la coordinación de acceso de los vehículos y los privilegios se puede decir que son de cuatro niveles: académicos, administrativos, alumnos e invitados-proveedores; teniendo para ellos áreas donde pueden estacionar su vehículo y el control de acceso depende de si se tiene puesta una calcomanía que distinga a profesores y alumnos para que se le entregue una tarjeta plástica que actúa como pase por el vehículo y para ello se tiene personal dedicado que se mantiene supervisando el acceso a las áreas general y de profesores.

Una forma de modernizar y mejorar este proceso es aprovechando las tarjetas inteligentes las cuales además de ser económicas son más funcionales y seguras y utilizadas en conjunto con un sistema informático se podrá gestionar la información de manera sistémica.

De esta manera se puede apoyar al personal a cargo de este control de acceso vehicular en tener una base de datos que contenga a todo el alumnado, administrativos y académicos, invitados y proveedores para privilegiar la entrada con mayor seguridad, versatilidad y de manera controlada.

También posibilita, si así se requiere, identificar al conductor y a las personas que entran o salen de la universidad e incluso asociar al conductor con la placa y llevarlo a nivel de presentar la foto del ocupante si se necesita corroborar la identidad del mismo.

3.7 INTEGRACIÓN GENERAL DEL SISTEMA

El enfoque que se sigue tiene como meta el que pueda desarrollarse, con investigaciones pertinentes, aplicarse prácticamente en cualquier sistema y se esquematiza en la siguiente figura 3.8 muestra el prototipo en un entorno con conectividad en red y la forma en que se incorporarán dispositivos que mediante el paradigma propuesto buscando que presenten, estos sistemas informáticos de gestión, una mejora en el flujo de información y por consiguiente, en la respuesta de las El's y los componentes.

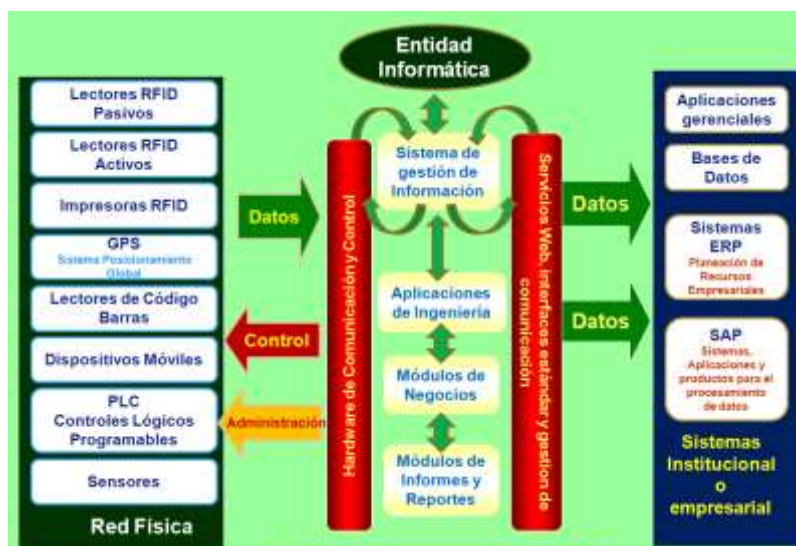


Figura 3-12 Esquema General del Sistema de Acceso y Prototipo

La elaboración del prototipo busca un diseño estructural en cuya arquitectura posibilite el ir integrando diversos dispositivos que permita con el mismo sistema la reutilización de módulos informáticos con los mínimos cambios sustanciales.

En el presente trabajo de investigación se desarrollo el prototipo con solo los componentes indispensables con tecnología RFID como lo muestra la figura 3.9 y que tiene a su vez, como objetivo, el tener una aplicación práctica actual.

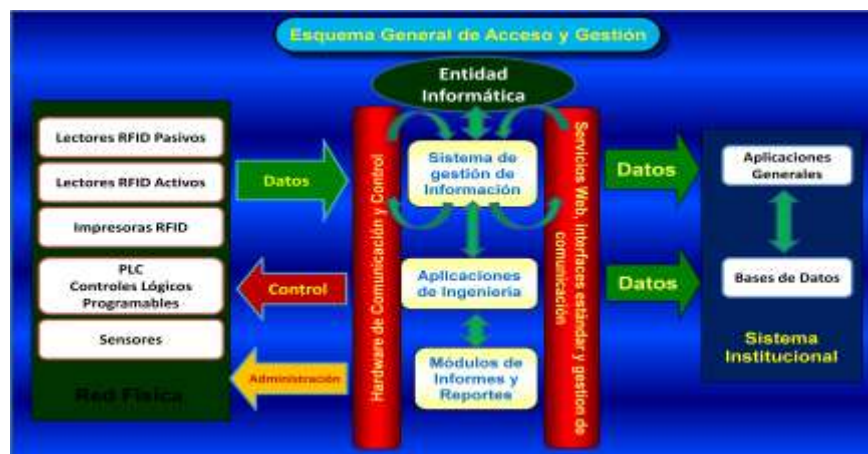


Figura 3-13 Esquema General del Sistema de Acceso y Prototipo RFID

Dentro de la tecnología RFID, las tarjetas inteligentes nos permiten almacenar y gestionar información en su área de memoria y para ello se utiliza una tarjeta que contiene 16

sectores y cada uno de ellos con 4 bloques de 16 bytes (1 kbytes) para realizar, dentro de sus bloques la EI la cuál nos dará la información necesaria para la gestión y transacción de información. En la siguiente figura se muestra la estructura de memoria de la tarjeta inteligente RFID (ACS, 2007).

Sector	Block	Byte Number within a Block															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
15	3	Key A				Access Bits				Key B							
	2																
	1																
	0																
14	3	Key A				Access Bits				Key B							
	2																
	1																
	0																
:	:																
	:																
	:																
	:																
1	3	Key A				Access Bits				Key B							
	2																
	1																
	0																
0	3	Key A				Access Bits				Key B							
	2																
	1																
	0																

Figura 3-14 Estructura del área de memoria de la tarjeta inteligente

La tarjeta inteligente tiene un algoritmo que autentifica la petición de información mediante un proceso de tres pasos posibilitando que la información contenida en ella sea segura ya que las operaciones en la memoria pueden ser encriptadas de acuerdo al tipo de seguridad deseada. La siguiente figura muestra dicho proceso.

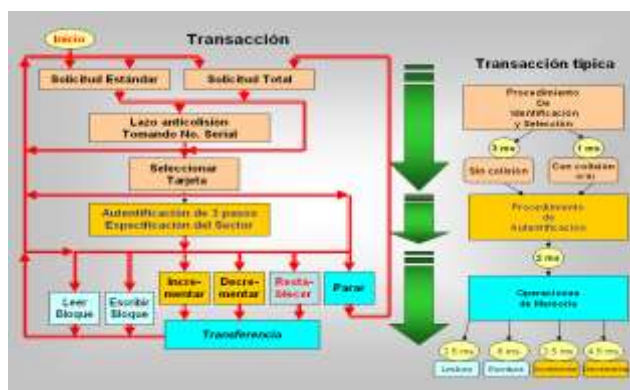


Figura 3-15 Diagrama a bloques del procedimiento de autenticación en tres pasos

El uso de TI's permite tener una mayor seguridad ya que son difíciles de falsificar ya que incluyen una gran variedad de funciones tanto de hardware como de software que detectan intentos de manipulación y reaccionan ante ellos contrarrestando posibles ataque y de acuerdo al nivel de seguridad requerida será el tipo de tarjeta a utilizar y que

incluye no solo la información contenida dentro de su memoria, sino también en la impresión de la misma (foto, colores, diseño, código de barras, etc.).

Estas TI's tienen una versatilidad para combinar datos (data Scrambling) o para criptografiarlos y su fin es proteger la información contenida en el chip o en el proceso de transmisión y recepción de información. Esto es importante ya que la identificación de un vehículo (o de una persona) es lo que conlleva un desempeño exitoso para su respectivo control de acceso.

En el caso de las Tarjetas inteligentes pueden respaldar algoritmos criptográficos simétricos³ para incrementar la seguridad además de que el tiempo de procesamiento es muy bueno. Este tipo de criptografía se usa mucho para el control de acceso y para el cifrado (encriptación) y desenscriptación (decriptación) puesto que presenta una relación alta entre velocidad y la confiabilidad.

La seguridad puede implementarse de manera integral en el proceso para que el flujo de información tenga un canal de seguridad de alta confiabilidad y esto puede lograrse mediante el uso de las tarjetas inteligentes y el empleo de algoritmos de cifrado en los procesos de salida y entrada del lector de la tarjeta y del servidor del control de acceso las aplicaciones.



Figura 3-16 Seguridad de punta a punta en un sistema de acceso

³ Los algoritmos de llave simétrica más comunes actualmente usados DES (Data Standard) Triple DES (ya sea con un formato de dos o tres factores) IDEA (International Data Encryption Standard) AES (Advance Encryption Standard) y MIFAREtm.

3.8 AVANCES DEL TRABAJO DE INVESTIGACIÓN

El prototipo se desarrollo en plataforma Windows utilizando un lenguaje de alto nivel orientado a objetos como lo es Visual Basic para así diseñar y construir la arquitectura que permita de manera preliminar el estructurar los datos, generar relaciones, procesos y servicios que permitan llevar a cabo una evaluación de estos en un sistema que va a ir creciendo para incorporar los demás componentes y dispositivos

El entorno de trabajo integra sensores, actuadores e interfaces hombre-máquina para la interacción general del sistema y de acuerdo a esta información se desarrollan los algoritmos que permitan el control de los diversos dispositivos embebidos en el sistema como pueden ser motores, relevadores y la presentación de información de manera adecuada tal como se observa de manera esquemática en la siguiente figura que mediante un lector de etiquetas se desarrolla el sistema de acceso.

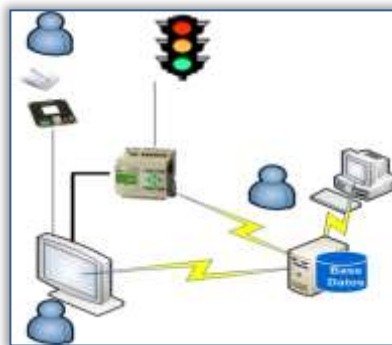


Figura 3-17 Sistema de Control de Acceso Vehicular con un nodo

El Sistema de Control de Acceso Vehicular con un sistema de gestión de base de datos tradicional de un nodo es como se muestra en la siguiente figura en donde de manera esquemática se muestra una aplicación propietaria con su respectivo gestor de base de datos que cumple con objetivos y que tiene como límite las restricciones propias del dispositivo o dispositivos utilizados.

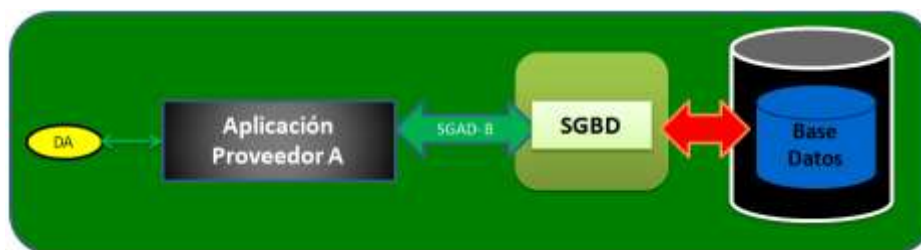


Figura 3-18 Diagrama esquemático de un Sistema informático

Utilizando Tecnología RFID en lo que se refiere a la identificación y autorización de acceso y utilizando elementos de control básicos el sistema quedaría de la siguiente manera.

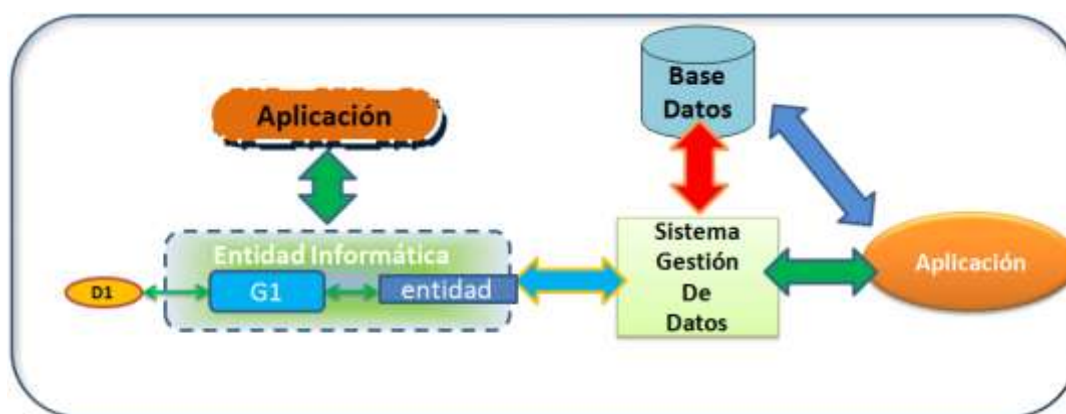


Figura 3-19 Diagrama esquemático de un Sistema RFID con EI

Mediante este enfoque utilizando una computadora local o remota conectando un dispositivo de lectura de tarjetas inteligente y/o etiquetas RFID se desarrollo la aplicación con la logística necesaria que permita cumplir con los objetivos y de manera estratégica se desarrollo una interface hombre-máquina para controlar parte de los eventos y así tener interacción con el sistema.

Las interfaces gráficas para el sistema de control de acceso vehicular estándar se muestran y describen a continuación:

Pantalla de Inicio:

En esta pantalla se tienen las opciones de configuración y prueba de los dispositivos RFID, La lectura de los dispositivos y un directorio que funciona para dar de alta, modificar, eliminar o agregar información adicional por evento.



Figura 3-20 Pantalla de Inicio del Prototipo de Prueba

Pantallas de Configuración dinámica

En las siguientes figuras se muestran las pantallas de configuración del dispositivo de lectura y de la interacción de los transponder RFID. Se muestra el estado de estas cuando se encuentra en estado de espera y cuando se activa al leer una tarjeta o transponder.



Figura 3-21 Pantallas de Configuración del Prototipo de pruebas

Pantallas del Directorio y del Control de Acceso Vehicular

En la siguiente figura se muestra la pantalla del directorio y del control vehicular donde pueden realizarse las operaciones de asignación del identificador a un vehículo y el registro correspondiente con el usuario así como el ingreso, modificación, agregado o eliminación de los datos.

Figura 3-22 Pantalla de Directorio y Control de Acceso Vehicular del Prototipo

En la siguiente figura se muestra la misma figura pero con la lectura de una tarjeta RFID o de un transponder (la identificación puede ser con un llavero, pluma, etc., donde puede estar alojado el sistema RFID)

Figura 3-23 Pantalla del Directorio y Control Vehicular Inicio de registro

Se pueden agregar los datos que asocian las diversas entidades que conforman la base de datos e incluso se tiene un área para mostrar la fotografía de la persona y en la siguientes figuras se muestran tanto la logística básica de acceso como la consulta a la base de datos.

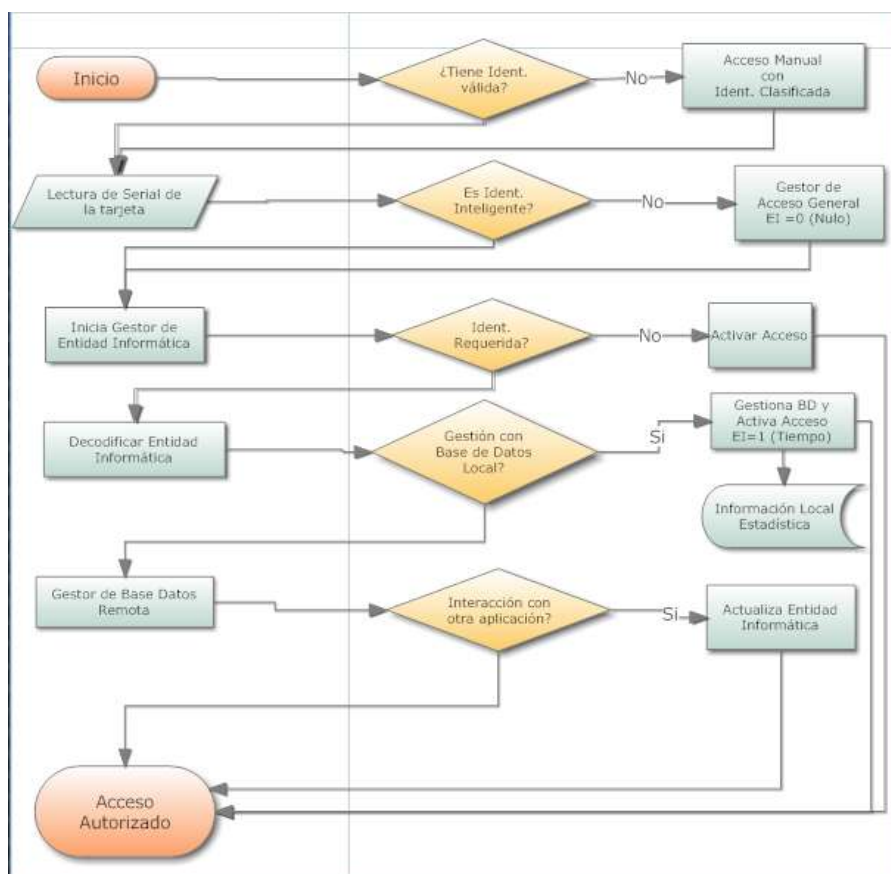


Figura 3-24 Logística de Acceso con TI

Figura 3-25 Pantalla de Directorio y Control Vehicular. Alta de usuario

Pantalla de Acceso y Control

Mediante esta pantalla se puede acceder a la información parcial o total al solo acercar la tarjeta RFID o bien un transponder, además de tener un registro histórico de los eventos posibles que tuvo el vehículo o bien de su usuario.

Figura 3-26 Pantalla de Control de Acceso del Prototipo

Interfaces de Gestión con dos nodos RFID

Las siguientes pantallas muestran dos nodos conformados por lectores de tarjetas inteligentes y etiquetas inteligentes utilizando el enfoque de EI.



Figura 3-27 Pantalla de Gestión e interacción del lector RFID

La siguiente figura muestra el módulo de lectura de bloques y sectores de forma automática de una tarjeta inteligente



Figura 3-28 Módulo de Lectura de la información de los sectores y bloques de una TI

En la siguiente figura se muestra la estructura básica de una entidad informática orientada al control de acceso vehicular



Figura 3-29: Estructura de La Entidad Informática para Control De Acceso Vehicular

Se pretende que este sistema no solo interactúe con tarjetas inteligentes RFID, sino también con sistemas con conectividad bluetooth, infrarrojo, etc. Solo se ha trabajado con tarjetas y transponder RFID inalámbricas y tarjetas de contacto aunque se espera seguir desarrollando para cumplir con las metas propuestas en este trabajo de investigación y abordar una problemática cuya solución podría ser útil.

CAPITULO 4. RECURSOS

Los recursos para el desarrollo del presente trabajo de investigación se enlistan en la Tabla 3, se requiere de un entorno de trabajo para elaborar las actividades que permitan en un inicio el análisis de forma local e independiente y posteriormente de un sistema con enlace en red así como un sistema básico de control. Actualmente se cuentan con todos los recursos en hardware para realizar el proyecto.

<i>Cantidad</i>	<i>Descripción</i>
2	Lector/Escritor de Tarjetas Inteligentes
5	Tarjetas inteligentes
1	Librería API del lector de tarjetas Inteligentes
1	Lector de RFID
5	Tarjetas RFID y trasponder
5	Computadora
1	Control Lógico Programable (o equivalente)
6	Relevadores para simular trabajo de motores
6	Sensores fotoeléctricos o de proximidad para habilitar inicio de proceso
1	Fuente de alimentación de 117 vca
1	Fuente de alimentación de 24 vcd
1	Software para programación de PLC
1	Lote de cables de conexión
1	Acceso a Internet
1	Software de desarrollo Visual Basic

Tabla 4: Recursos utilizados para desarrollar el proyecto

CAPITULO 5. CALENDARIZACIÓN

No.	ACTIVIDAD	M E S													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Revisión del estado del arte y del objeto de estudio	x	x	x	x										
2	Descripción teórica y planteamiento del Sistema	x	x	x	x	x									
3	Reestructuración del Protocolo de Tesis	x	x	x	x	x	x								
4	Estructuración del Proyecto de Tesis					x	x	x							
5	Definición de la arquitectura del sistema					*	x								
6	Desarrollo del prototipo del Sistema de Control de Acceso Vehicular						x	x	x						
7	Desarrollo de una estructura de datos utilizando Entidades Informáticas								*	*	*				
8	Integración e implementación del sistema							x	x	*	*	*			
9	Análisis y evaluación de resultados								*	*	*	*			
10	Elaboración de artículos de congreso								x	x		X			
11	Elaboración de documento de tesis										x	X	*	*	
12	Revisión de tesis												*	*	
13	Examen de grado														*
14	Créditos o materias a cubrir a criterio de la Comisión						*	*	*						

Tabla 5 Cronograma de actividades a desarrollar para el desarrollo del proyecto

REFERENCIAS

ACS. (2007). *"Advanced Card System"*. Recuperado el 19 de junio de 2008, de <http://www.acs.com.hk/>

Advanced Cards System Limited". *"ACR120S SDK User Manual"*. (2007). Hong Kong: ACS.

Bass, L., Kazman, R., & Clements, P. (2003). *Software Architecture in Practice* (2a. ed.). Addison Wesley.

Betarte, G., Cornes, C., Szasz, N., & Tasistro, A. (2000). Specification of a Smart Card Operating System. (Lecture Notes in Computer Science No. 1956), 77-93.

Comer, E. D. (2006). *Redes Globales de Información con Internet y TCP/IP* (Tercera Edición ed.). México: Prentice Hall.

Cortés, C., & Sará, J. (2000). *Sistema de identificación por radiofrecuencia para control de animales bovinos*. Pontificia Universidad Javeriana.

Date, C. J. (2003). *An Introduction to Database System*. Boston. MA, USA: Addison weshey.

De Amescua Seco, A. (2003). *Análisis y Diseño estructurado y orientado a objetos de sistemas informáticos*. España: McGraw Hill.

Devarakonda, R. S. (2001). *Sistemas de Base de datos Relacionado a Objeto - El Camino hacia Adelante*. Recuperado el 5 de Junio de 2009, de ACM – Association for Computing Machinery: <http://oldwww.acm.org/crossroads/espanol/xrds7-3/ordbms.html#IDC>

DRAE. (2008). *Diccionario de la lengua española de la Real Academia Española*. España: ESPASA.

Finkenzeller, K. (2003). *Fundamentals and Applications in contactless Smart Cards and Identification* (2a. ed.). Swadlincote, UK: Wiley & Sons,.

Hansmann, U., & al.], [. (2000). *Smart card application development using Java*. Berlin; New York: Springer.

Hendry, M. (1997). *Smart card security and applications*. Boston: Artech House.

Joyanes Aguilar, L. (2003). *Fundamentos de Programación. Algoritmos, Estructura de Datos y Objetos*. Madrid: Mc Graw Hill.

Jurgensen, T. M., & Guthery, S. B. (1998). *Smart card developerapos kit*. Indianapolis, Ind.: Macmillan Technical Pub.

Kyu, I. K., Hyuk, J. K., Won, G. C., & Eun, J. L. (2008). A Collaborative Access Control Based on XACML in Pervasive Environments", . *Hybrid Information Technology, International Conference on 2008 International Conference on Convergence an*, (págs. pp. 7-13,). icht.

Miranda Tello, J. R. (2000). *Diseño y construcción de un lector de tarjetas inteligentes. Tesis (M. en C. en Ingeniería de Computo con especialidad en Sistemas Digitales)* . (I. P. Nacional, Ed.) México: Centro de Investigación en Computación,.

Moreno, A. (26 de Febrero de 2008). *Red Iris*. Recuperado el 27 de Abril de 2009, de <http://elles.rediris.es/elles9/4-1-2.htm#4.1.2.1>

Presseman, R. S. (1993). *Ingeniería del software* (3a. ed.). Madrid: McGraw-Hill.

Ruble, D. A. (2001). *Análisis y Diseño Práctico de Sistemas Cliente/Servidor con GUI*. México: Prentice Hall, Inc.

Scdeveloper.com. (s.f.). *"Smart Card Development Kits, Cards, Readers, Tools and Resources for Developers"* . Recuperado el 8 de 06 de 2008, de <http://www.scdeveloper.com/SDK.htm>

Silberschatz, A., Korth, H. F., & Sudarhan, S. (2006). *Fundamentos de base de Datos*. España: Mc Graw Hill.

Silva, F., Pereyra, A., & Filipe, V. (2008). Automatic Control of Students' Attendance in Classrooms Using RFID. *2008 Third International Conference on Systems and Networks Communications*, (págs. 384-389).

Tari, Z., & Bukhres, O. (2001). *Fundamentals of distributed objects systems*. John Wiley and Sons.

Ullman, L. (2003). *MySQL*. México: Prentice Hall,.

UNAM, e. (2007). *Sociedad de la Información y Conocimiento*. Recuperado el 10 de junio de 2007, de <http://www.sociedadinformacion.unam.mx/index.jsp>

Wolfgang, R., & Wolfgang, E. (1997). *Smart card handbook*. (H. d. hipkarten, Trad.) New York: Wiley.

Zhigun, C. (2000). *Java Card technology for Smart Cards : architecture and programmers guide*. Boston: Addison-Wesley.