PROTOTIPO DE AUTENTICACIÓN PARA SEGURIDAD Y CONTROL DE ACCESO A LAS AULAS EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

Barón Rueda Pablo Andrés U00010330

Portilla Villamizar Miguel Alexander U00010982

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
AUTOMATIZACIÓN INDUSTRIAL Y CONTROL
BUCARAMANGA
2008

PROTOTIPO DE AUTENTICACIÓN PARA SEGURIDAD Y CONTROL DE ACCESO A LAS AULAS EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA

Barón Rueda Pablo Andrés U00010330

Portilla Villamizar Miguel Alexander U00010982

Proyecto de grado presentado como
requisito parcial para optar el titulo
de "Ingeniero de Sistemas"

DIRECTOR
Ing. Miguel Antonio Cadena

ASESOR
Ing. Diego Tibaduiza

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
AUTOMATIZACIÓN INDUSTRIAL Y CONTROL
BUCARAMANGA
2008

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Director

_____

Evaluador 1

_____

Evaluador 2

Bucaramanga, 29 de Enero de 2009

DEDICATORIA

A nuestros padres y hermanos, como testimonio de ternura y amor.

A nuestra alma mater, como prueba de nuestra gratitud inmodificable y la dirección hacia el campo de la ingeniería de sistemas.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

La Universidad Autónoma de Bucaramanga (UNAB), Directivos, Docentes y Administrativos, por la perspectiva que nos brindaron en la búsqueda de los procesos científicos y técnicos en el saber hacer durante la carrera de Ingeniería de Sistemas.

Al Ingeniero Miguel Antonio Cadena, Director de la Investigación, quien permitió que el proyecto se desarrollara bajo los parámetros y políticas de la Ingeniería de Sistemas.

Los jurados evaluadores, Ingeniera Karol Reyes y el Ingeniero Eduardo Carrillo, quienes con su sabiduría e inteligencia técnica captaron con facilidad los procesos organizacionales pedagógicos, técnicos y comunicativos de las diferentes etapas de planeación, ejecución, evaluación y proyección del proyecto.

Al Ingeniero Diego Tibaduiza, quien con sus estímulos y orientaciones como asesor, se concluyo satisfactoriamente el proyecto, el cual, todos los procedimientos técnicos y científicos se llevaron a la práctica para que el prototipo de seguridad y control de acceso de las aulas de la Universidad Autónoma de Bucaramanga, se lograra y que en un futuro se realice la instalación para su funcionamiento y modernidad.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

INTRODUCCIÓN

Durante los últimos años, la Ingeniería de Sistemas, se ha venido complementando con la Ingeniería Mecatrónica, la Biometría y viceversa, facilitando a los programadores que buscan a cada momento el “saber técnico”, las herramientas y procesos para desarrollar perfectamente aplicaciones alternas de diferentes sistemas de ingeniería.

Estos enlaces que contienen conexiones a Bases de Datos en redes locales y externas a todos los niveles y que reconocen características “físicas únicas” de seguridad, (huellas dactilares, venas humanas, tarjetas inteligentes, ranuras) permiten resultados programáticos eficientes y de alta calidad, mediante un dispositivo que puede captar chips, imágenes, sonidos, etc. para poder accionar el prototipo, cuando el usuario necesite el servicio.

Este tipo de dispositivos es el que se busca implementar en la Universidad Autónoma, ya que proporciona una mayor seguridad tanto a aulas como a oficinas, como también un eficiente control a los usuarios y un avance tecnológico de la panta física de la institución. Con el desarrollo de este proyecto se busca dar unas bases y poner los cimientos para la implementación final de estos dispositivos, el cual con el tiempo le dará a la universidad un gran aporte en cuanto a tecnología, seguridad y proyección hacia el futuro.

El tipo de dispositivo que se quiere implementar en la Universidad es el de las Tarjetas Inteligentes, las cuales son tarjetas de plástico que en medio de ellas contienen un chip con microprocesador, el cual es el que permite que estas tarjetas contengan información, la cual puede utilizarse como por ejemplo para sistemas de pago (tarjetas debito), control de acceso, simcards de celulares, etc. La información que allí se guarda es muy variable y va desde nombres,

cedulas, teléfonos hasta cuentas bancarias; la manera en que se puede manipular esta información es por medio de los comandos APDU, los cuales son los que nos permiten manipular la información (guardar, borrar, modificar, leer) que allí este contenida.

La forma en que funciona el lector con la tarjeta es Half-Duplex, ya que solo realiza una acción a la vez (envió o recibo de datos nunca las dos acciones al mismo tiempo), debido a esto, se manejan 2 estructuras diferentes de transmisión: la primera son diferentes comandos enviados para ser ejecutados y segundo respuesta al comando enviado, de esta manera es que se logra la total funcionalidad del dispositivo.

1. PROBLEMA

Investigación de control de Acceso y Seguridad.

1.1 TITULO DE LA INVESTIGACIÓN

“PROTOTIPO DE AUTENTICACIÓN PARA SEGURIDAD Y CONTROL DE ACCESO A LAS AULAS EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA”

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Antecedentes A medida que se avanza en los cambios técnicos y sustanciales de la industria, las empresas de todo el mundo se ven implicadas de mejorar sus programaciones para dar soluciones a los diferentes avances tecnológicos y para ello se han basado en la gestión de los recursos dedicados a los diferentes proyectos de desarrollo, los soportes metodológicos y la tecnología.

Teniendo en cuenta que los avances científicos y técnicos que permiten a las industrias y empresas multinacionales desarrollar diferentes tipos de proyectos de alta calidad para estar a un nivel competitivo en el mundo, las facultades de Ingeniería de las Universidades del País han establecido un método de trabajo global de educación universitaria, para poder construir infraestructuras digitales dirigidas no solo a la enseñanza sino también a la administración.

El proyecto, base fundamental de esta investigación sigue una serie de procesos estructurales para conseguir los objetivos que se tienen trazados, con el fin de integrar los componentes tanto de Hardware como Software para poner en práctica los conocimientos de las Ingenierías de Sistemas y Mecatrónica, implementando un dispositivo que sirva para controlar el acceso a las aulas de la Universidad Autónoma de Bucaramanga y que estos se ejecuten por medio de lectores de Huellas Dactilares o Lectura de una Tarjeta Magnética.

Para poder elegir la opción de implementación que preste a la Universidad un servicio de calidad en la seguridad y el control de acceso de las aulas se harán distintas comparaciones y análisis entre los dos dispositivos seleccionados para tal fin. Entre las comparaciones que lleva la implementación de un dispositivo de tal magnitud, están: el presupuesto, el cual será costeado por los investigadores, ya que no existe ningún patrocinio hasta el momento, la

eficiencia en el servicio que pueda prestar y la disponibilidad que este dispositivo tenga para todo el personal que lo utilice, ya que se debe tener en cuenta la posible pérdida de tarjetas y en algunos casos como para la huella dactilar, la falta de dedos en algunas personas por mutilación o en algunas por heridas que puedan tener en sus dedos que hacen que las huellas no sean reconocidas.

El proyecto tendrá una serie de fases que permitirá analizar y ampliar todos los procesos que conlleva esta investigación con el fin de colocar el dispositivo en funcionamiento en la Universidad para beneficio de toda la comunidad.

1.2.2 Justificación Durante los últimos años, la Ingeniería de Sistemas, se ha venido complementando con la Ingeniería Mecatrónica, la Biometría y viceversa, facilitando a los programadores que buscan a cada momento el "saber técnico", las herramientas y procesos para desarrollar perfectamente aplicaciones alternas de diferentes sistemas de ingeniería.

Estos enlaces que contienen conexiones a Bases de Datos en redes locales y externas a todos los niveles y que reconocen características "físicas únicas" de seguridad, (huellas dactilares, venas humanas, tarjetas magnéticas, ranuras) permiten resultados programáticos eficientes y de alta calidad, mediante un dispositivo que puede captar imágenes y sonidos para accionar el prototipo, cuando el usuario necesite el servicio.

Por estas razones y para que las aulas de la Universidad Autónoma, tengan otro sistema de seguridad funcional y de rápido control, que busque mejorar el sistema tradicional y a su vez, los empleados (celadores) se ocupen de atender y controlar a los usuarios con otras funciones especificas, "este proyecto", es de gran contribución para el mejoramiento de la calidad técnica y administrativa, cuando se aplique el prototipo de control de acceso y se

socialice el proceso con el personal que conforma la comunidad educativa de la Institución.

Con el objeto de encontrar la metodología “de seguridad y control de acceso” más adecuada (Banda magnética o huella dactilar) se elaborara un estudio de viabilidad y costos para determinar la mejor opción, con el fin de realizar todos los procedimientos que permitan establecer los procesos que cumplan con la Misión y Visión del proyecto.

1.2.3 Delimitación del Problema La institución no ofrece a la comunidad educativa que interactúa dentro y fuera de ella un prototipo de seguridad y control de acceso que permita un funcionamiento rápido de entrada y registro del personal, ya que este, se regula en forma manual por el personal de control y seguridad de la Universidad (celadores).

1.2.4 Línea de Investigación

Automatización Industrial y Control.

1.2.5 Estado del Arte La tecnología ha avanzado bastante hasta el día de hoy, y todavía existen demasiados campos por investigar. Ante el tema de la seguridad, se trata de desarrollar cada día más y más formas de poder mantener al ser humano o al individuo muy confiado de donde trabaja, donde vive, e incluso hasta donde guarda sus pertenencias.

En el mercado actual, hay mucha competencia sobre los métodos de seguridad de un edificio, o de un cuarto en específico. Además se han empezado a investigar nuevas metodologías de seguridad. Hoy en día ya se ha empezado a utilizar los aspectos físicos únicos de cada persona, como una

llave para poder entrar a una oficina, y hasta poder tener acceso a un computador. Estos aspectos se llaman aspectos biométricos. La biometría es una característica cuantitativa del hombre; como el peso, longitud, etc., que diferencia a cada uno de los seres vivos. Con respecto a los métodos se seguridad, se han empezado a utilizar estas características como método de identificación de la persona.

- Para poder usar estas cualidades biométricas, se tienen que cumplir ciertos requisitos básicos:
- Universalidad: Que tan común es el rasgo en las personas.
- Singularidad: Que tan diferentes es este rasgo entre una y otra persona.
- Permanencia: Que tan duradera es este rasgo en el individuo.
- Recolectable: Facilidad y adquisición del rasgo en las personas.
- Calidad: Precisión y velocidad del sistema.
- Aceptabilidad: La aprobación que tiene ante el público.
- Fiabilidad: Que tan fácil es engañar al sistema de autenticación.

De acuerdo con estos requisitos, se van descartando ciertos rasgos que pueden no ser tan diferentes entre un individuo y otro. Entonces de acuerdo a las características restantes, la identificación de estas se dividió en dos grupos: el primer grupo se denomina rasgos Biométricos Estáticos; estos rasgos son los rasgos únicos y físicos de cada persona (huella dactilar, retina iris, etc.). El otro grupo lo conforman las características conductuales de cada persona (voz, escritura manuscrita, etc.), a este grupo se le denomina rasgos Biométricos Dinámicos.

De acuerdo a la identificación de estas características, las empresas empezaron a explotar estos mercados, y empezaron a sacar sus productos para poder venderlos, y darle más seguridad al ser humano.

El semestre pasado en la universidad se elaboro un proyecto de este tipo. El proyecto se llama “Vein Check”. Se basa en que los trazos de la venas son

diferentes para cada persona; consiste en verificar los datos biométricos de la parte posterior de la palma de la mano, además de una clave de acceso, para poder abrir una puerta. Este proyecto se basó en demostrar que los diferentes rasgos biométricos de las personas son fácilmente reconocibles gracias a la Biometría.

Teniendo en cuenta que el Banco Santander con sede en la Universidad Autónoma donó unos dispositivos de lectura de tarjeta magnética, las cuales el Banco dentro de su sede las utiliza, pero que al mismo tiempo, los dispositivos donados se encuentran sin ningún uso dentro de la Universidad, se requiere implementarlos y darles el respectivo funcionamiento, debido a que anteriormente nadie se preocupó por la magnitud de la implementación del proyecto, ya que la comunidad de la Institución goza de un carnet que es compatible con este dispositivo.

1.2.6 Resumen del Problema A medida que el tiempo avanza, las diferentes Empresas e Instituciones siempre apuntan a mejorar sus estructuras técnicas y físicas para prestar un mejor servicio a sus usuarios, en el caso de la seguridad es lo mismo, ya que siempre se busca tener tranquilidad y un ambiente positivo para realizar nuestras actividades, por estas razones y para que las aulas de la Universidad Autónoma, tengan otro sistema de seguridad funcional y de rápido control, que busque mejorar el sistema tradicional y a su vez optimizar la institución, se decidió la implementación de “este proyecto”, el cual es de gran contribución para el mejoramiento de la calidad técnica, administrativa y la seguridad, cuando se apliquen los modelos del prototipo de control de acceso y se socialice el proceso con el personal que conforma la comunidad educativa de la Institución.

En cuanto al aporte que tiene este proyecto a la Ingeniería de Sistemas, se puede decir que es de gran importancia, ya que para la realización de este trabajo se necesitan poner en práctica distintos conocimientos adquiridos en el

trascurso de la carrera, tales como la programación, el manejo de datos y la manipulación de dispositivos hardware; pero algo que se puede mencionar es que este tipo de proyectos nos da ideas en cuanto a nuevos temas que se podrían acoplar a la carrera, ya que a nuestro parecer vemos que es necesario que un Ingeniero de Sistemas no solo sirva para manejar software sino que también tenga conocimientos Hardware y programación a bajo nivel, los cuales le servirían para manipular dispositivos electrónicos y realizar diferentes actividades a lo cotidiano, lo cual le serviría para abrirle puertas y explorar otros campos que se acoplan a nuestra carrera.

Palabras Claves.

- Mejoramiento
- Seguridad
- Control
- Digital

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer un prototipo digital de “Control de Acceso”, que permita la comparación de información organizada del usuario contenida en una base de datos, permitiendo o negando el acceso, por medio de un sistema de lector de tarjetas inteligentes conectado a un computador.

2.2 OBJETIVOS ESPECIFICOS

- Generar una aplicación, que compare los datos del usuario que está usando el dispositivo con los registrados en la base de datos Banner, validando la entrada.

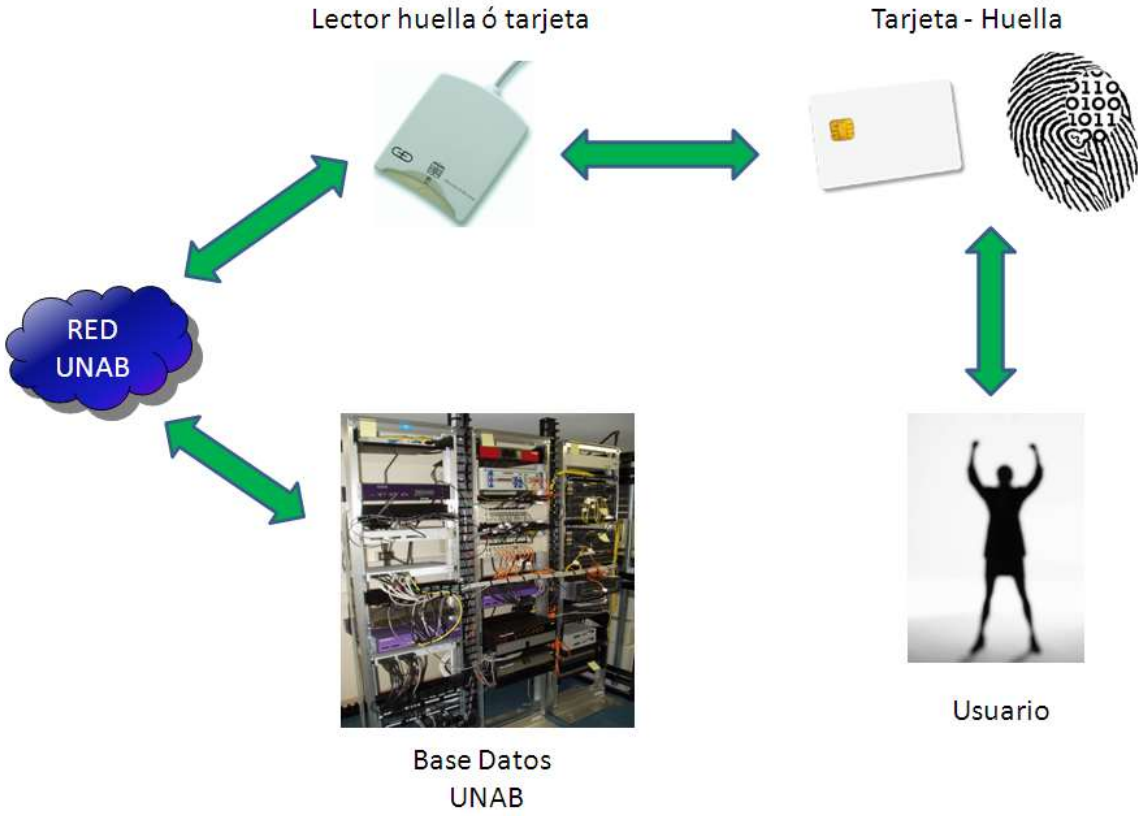
- Determinar la opción más viable entre la tarjeta inteligente y la huella dactilar para el desarrollo del proyecto.

- Evaluar los procesos empleados en la elaboración del prototipo digital y conceptualizarlos con los usuarios para el uso y funcionamiento del dispositivo en un futuro.

3. FUNDAMENTO TEÓRICO

3.1 MODELO CONCEPTUAL

Figura No.1: Modelo Conceptual

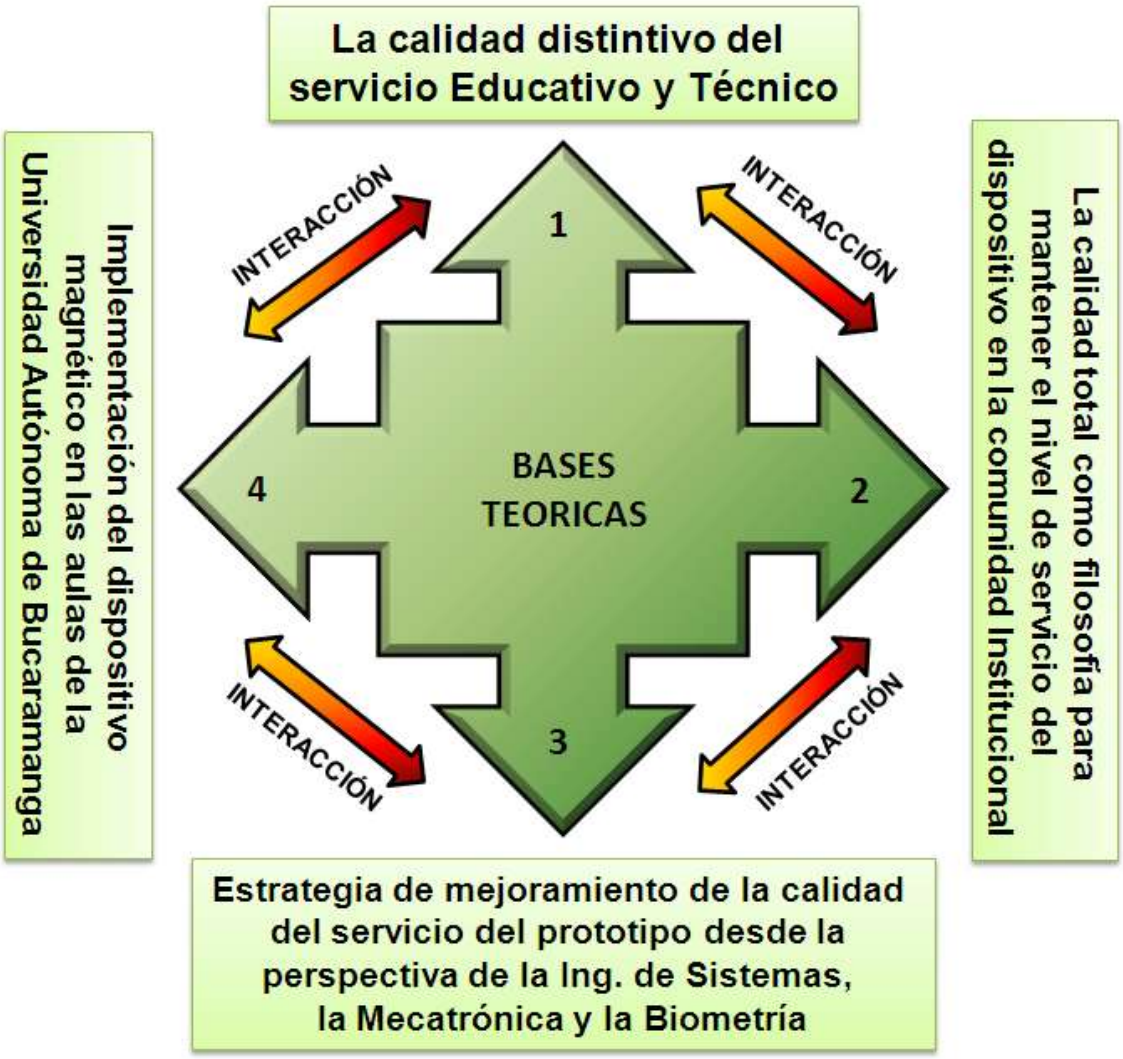


Fuente: Grupo Investigador

La figura anterior representa el flujo de datos de la implementación del dispositivo, empezando por el Usuario, el cual por medio de la tarjeta o la huella dactilar se identifica en el dispositivo y esté por medio de la red de la Universidad va hasta la Base de Datos para verificar si los datos existen y así confirmar si el acceso es válido o negado al usuario.

3.2 BASES TEÓRICAS

Figura No.2: Bases Teóricas



Fuente: Grupo Investigador

3.2.1 Concepción Científica El propósito general de las bases teóricas, conlleva a interiorizar y analizar conceptos a la luz de la ciencia y tecnología, que se relacionen con el objeto de la investigación, los procesos de aplicación y los diferentes avances para que den solución a la situación problema.

Los tópicos desarrollados tienen como referencia el dispositivo manejado mediante la tarjeta magnética o la huella dactilar, como se muestra en las figuras 1 y 2.

La calidad como distintivo del servicio educativo y técnico, serian múltiples y variadas las definiciones de educación y la tecnología como también autores que han escrito sobre los diferentes enfoques y ambientes, pero existe la claridad que la concepción intelectual ha sido manejada por los individuos como contenidos dentro de todos los procesos de calidad técnica y educativa.

Esta pedagogía es una estrategia mediante la cual el individuo, grupo y sociedad en general desarrollan actitudes, aptitudes, habilidades y forman valores con el objeto de avanzar en lo científico y técnico dentro del contexto de los “sistemas”, para luego transformarlos en el “saber hacer” para el mejoramiento integral de las empresas, las universidades y las personas.

Las entidades que han logrado un nivel de desarrollo técnico, personal y colectivo lo han planeado, asimilado y alcanzado mediante la transformación e implementación y la búsqueda del mejoramiento técnico a través de los procesos científicos, metodológicos, tecnológicos y la practica en el desarrollo de los diferentes proyectos investigativos.

“Todo pueblo que alcanza un cierto grado de desarrollo se halla naturalmente inclinado a practicar la educación porque esta es el principio mediante el cual, las empresas y la comunidad humana conserva y transmite su peculiaridad física y espiritual” (*tomado de: WERNER, Javier, Paideia: Los ideales de la cultura Griega, Fondo de la cultura Económica, 1980, Pág. 3-16*).

Para los griegos la educación, fue el medio para hacer del ser humano un hombre perfecto en el campo físico, moral e intelectual, por ello el énfasis, se dio para que su cuerpo fuera cada día más fuerte y bello, con una voluntad poderosa, gestora de grandes propósitos y metas, con una conciencia clara,

justa y transparente, para que se sobrepusiera a las dificultades y adversidades de la vida, diseñando acción de vida y así, pudiera alcanzarlas plenamente, para la convivencia humana pacifica y honesta, con el fin de comprender, analizar y criticar constructivamente y este a su vez pudiera vivir en armonía con la naturaleza y consigo mismo, pero fundamentalmente para que pudiera lograr el ideal de vivir como hombre. Este planteamiento fue lo que los griegos llamaron “sabiduría” con el objeto de formar hombres sabios dentro de un proceso sistemático, practico y técnico.

“La educación se concibe como un proceso permanente de carácter social y personal” (*tomado de: MEN (Ministerio de Educación Nacional), Lineamientos Generales de los Procesos Curriculares, Santa Fé de Bogotá, Noviembre 1994, D.E. Pág. 33-34*).

El proceso social hace referencia a la trascendencia histórica de la calidad total en la “razón de ser” para mantener el nivel del servicio del “dispositivo” en la comunidad institucional como estrategia de mejoramiento de la calidad del servicio del prototipo desde la perspectiva de la Ingeniería de Sistemas, Mecatrónica y la Biometría.

Del análisis de estos principios de las bases teóricas se desprende que esta tecnología será de gran apoyo para la implementación del dispositivo magnético en las instalaciones de la universidad con proyección a negocios, empresas o cualquier entidad pública o privada que requiera el servicio.

Como el hombre durante el paso de los años ha buscado formas de asegurar sus pertenencias, datos, archivos y demás cosas importantes de cotidianidad, con el fin de conservarlas como documentación privada, ha explorado muchos medios de seguridad y en estos avances a utilizado determinados elementos que lo identifiquen tanto a él como a sus propiedades, frente a los demás. En el siglo XIX las personas de clase alta, utilizaban las tarjetas de papel grueso (cartulina) para poder identificarse frente a las demás personas, dándoles sus

datos personales a su interlocutor o incluso para indicar que habían acudido a visitarle y no le habían encontrado.

Según Raúl Sánchez Reillo, comenta que “este sistema es el que se conoce actualmente como tarjetas de visita” (*tomado de: SÁNCHEZ, Reillo, Raúl, Profesor del departamento de Tecnología Electrónica, Universidad Carlos III de Madrid, España, PC Actual, Pág. 297*) y que en la actualidad no es ya propio solo de la clase alta, sino de todo el mundo, y no solo para indicar los datos personales sino también para los datos laborales.

Sin embargo, y aunque son actualmente son muy utilizadas las tarjetas de visita de cartón, tienen varios inconvenientes que en determinados entornos y aplicaciones era necesario evitar. A lo largo del siglo XX han aparecido diversas alternativas para solucionar los problemas fundamentales que han surgido como el deterioro del papel, la imposibilidad de obtener información de forma automática (electrónica), la susceptibilidad de copia y la seguridad de la información almacenada.

3.2.2 Tecnologías Biométricas

La Biometría es una tecnología que permite la identificación de un usuario en un dispositivo mediante el análisis de sus características físicas (voz, retina, huellas dactilares, etc.), este tipo de tecnología es usada principalmente para control de acceso y seguridad en diferentes establecimientos e instituciones [3].

Además de las características físicas de personas esta tecnología también se aplica a firmas, códigos, bandas magnéticas, etc. O cualquier información que identifique a un usuario especifico, algunos de los dispositivos que se basan en esta tecnología son:

3.2.2.1 Banda Magnética La banda magnética es uno de los métodos más usados desde hace mas de 20 años, se usa principalmente en las tarjetas de crédito, debito. La banda magnética de color negra o marrón encontrada en la parte de atrás de las tarjetas, es donde está la información grabada en tres pistas (Figura3), las dos primeras están regidas por la norma ISO7813 y la ultima según la ISO4909.

Figura No.3: Dimensiones Tarjeta electrónica, banda Magnética y tipos de datos guardados

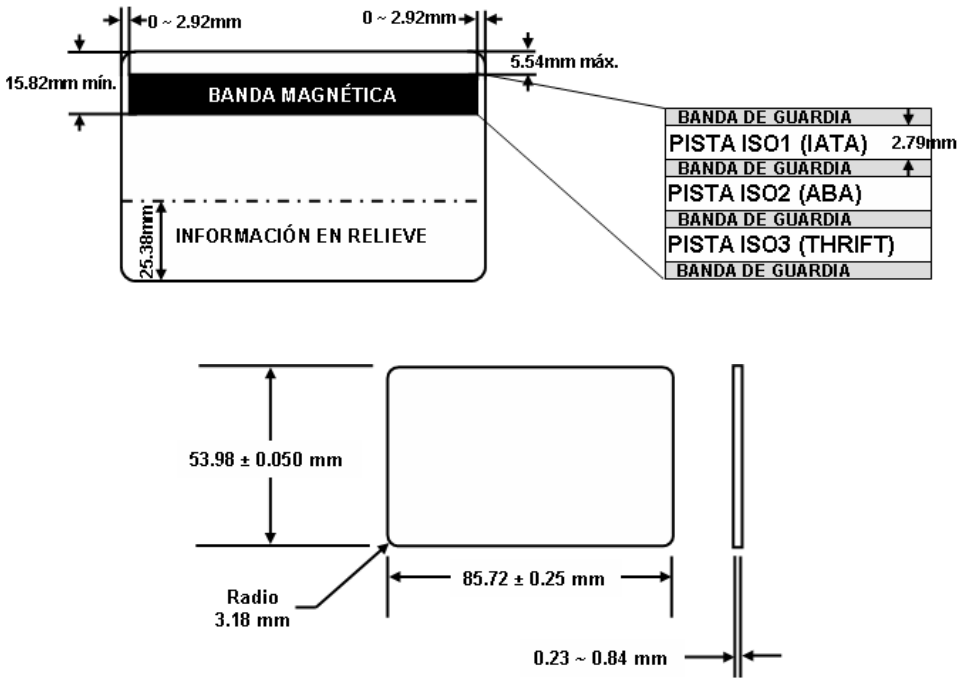


Imagen tomada de http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica.shtml

Hay dos formas de hacer las bandas magnéticas, estas pueden ser aplicadas directamente en la tarjeta; o pueden ser hechas por separado, y luego ser adheridas a la tarjeta. De acuerdo al material de la banda magnética y la coercitividad, se define el color: si es de baja coercitividad (Lo-CO) y de oxido de hierro, es de color marrón; si es de alta coercitividad (Hi-CO) y hecha de ferrita de bario, es de color negro. Las bandas son hechas de las partículas magnéticas del material, mezclados con una resina que forman una mezcla espesa, luego es cubierto con un sustrato. Después, las partículas son alineadas para eliminar el ruido, luego se pasa por un campo magnético para

encuadrar todas las partículas. Por último, cuando la tarjeta, ya está completa, las partículas contenidas en la banda, pueden ser magnetizadas en dirección sur o norte, al cambiar la dirección de las partículas de sur a norte y viceversa, se permite inscribir la información en la banda. Lo interesante de estas bandas, es que la información contenidas en ellas, pueden ser cambiadas con facilidad.

La amplitud de la señal depende de densidad de las partículas contenidas en la banda, entre mas partículas se encuentren, mayor es la amplitud de la señal. La amplitud de la señal depende del lector que se vaya a usar; para los lectores usados por la industria bancaria, la norma ISO/IEC 7811, define que amplitud de señal, debe tener la banda; en otras palabras, la norma define la densidad de las partículas magnéticas contenidas en la banda; también define la densidad de bits que se encuentran, los datos.

Los bits encontrados en la banda son definidos por la polaridad de las partículas encontradas en ella (Figura4), de acuerdo al esquema de codificación, entre los cuales se encuentran el F2F y el MFM.

Figura No.4: Lectura de datos de la banda magnética comparada con una lectura de voltaje

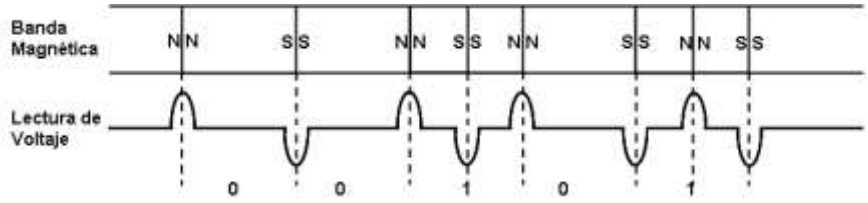


Imagen tomada de http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica.shtml

Las pistas se pueden codificar de acuerdo al esquema y al tipo de lector, en algunos requieren las tres pistas, otros solo dos u otros solo una. Cada pista tiene su propio formato de acuerdo al uso que se le va a dar a la tarjeta; a continuación se describirá cada una de las pistas:

- Pista 1: Se basa en el formato IATA (International Air Transport Association), tiene una densidad de grabación de 210 bpi (bits per inch),

son 7 bits por carácter (incluyendo el bit de paridad), y puede almacenar hasta 79 caracteres alfanuméricos.

- Pista 2: Se basa en el formato ABA (American Bankers Association), tiene una densidad de grabación de 75 bpi (bits per inch), son 5 bits por carácter (incluyendo el bit de paridad), y puede almacenar hasta 40 caracteres alfanuméricos.
- Pista 3: Se basa en el formato TTS (Thrift Third Standard), tiene una densidad de grabación de 210 bpi (bits per inch), son 5 bits por carácter (incluyendo el bit de paridad), y puede almacenar hasta 107 caracteres numéricos o caracteres especiales.

Este tipo de tecnología es ampliamente usado en el mundo, pero uno de los riesgos de esta es que depende del trato que se le dé a la tarjeta, y también el hecho de cuidarla mucho, porque fácilmente se puede extraviar. Además debido a la amplitud de equipos y facilidad de poder grabar los datos, se han detectado casos de clonación de tarjetas, que permite a los delincuentes, hacer una copia de todos los datos que esta contiene en la banda magnética [2].

3.2.2.2 Huellas Dactilares Hoy en día, han nacido bastantes dispositivos de lectura de huellas dactilares, los cuales se complementan con la conexión a un computador, el cual contiene un software que recibe los datos del lector conectado a este, y mediante un algoritmo matemático verifica los datos ingresados de la imagen con los datos previamente grabado en una base de datos. La base de datos contiene toda la información de las personas que tienen acceso, ya sea a un salón, una caja fuerte, o aun hasta para tener acceso a diferentes archivos o carpetas contenidas en el disco duro. Lo que hace que las huellas dactilares sean tan utilizadas actualmente, son sus características esenciales:

- Son irrepetibles, (ningún ser humano tiene las mismas huellas que otro).

- No cambian a lo largo de la vida.
- Son las únicas legalmente reconocidas como prueba fidedigna de identidad.

Las huellas dactilares se forman en el ser humano a partir de la sexta semana de vida intrauterina y sus características no varían a lo largo de toda la vida del individuo. Como se observa en la Figura5, cada huella es totalmente diferente a la otra, nunca habrá ninguna huella dactilar de un ser humano igual a la de otro, ni siquiera entre hermanos gemelos. Además, al sufrir algún corte pequeño, el tejido se regenera sin cambiar de estructura, es decir las curvas, arcos y demás líneas que se encuentran en la huella se reconstruyen volviendo a su forma original.

Figura No.5: Huella Digital

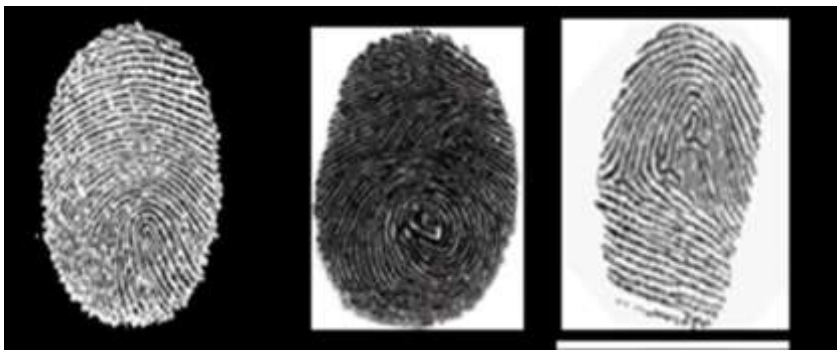


Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

El único daño que puede haber en una huella podría ser una herida profunda que afecte la dermis, la piel forma una cicatriz que cambiara los detalles de la huella. La huella está conformada principalmente de dos partes, unas salientes denominadas crestas papilares, y unas depresiones llamadas surcos interpapilares. ¿Cómo se deja la huella en una superficie cualquiera? Las crestas papilares del dedo, contienen las glándulas sudoríparas; el sudor que producen estas glándulas, contiene un aceite, que es retenido entre las diferentes depresiones o surcos interpapilares, así pues cuando el individuo presiona o sostiene un objeto y a este le presiona la yema de los dedos, deja

residuo del sudor, dejando así un negativo de la huella dactilar del individuo, como las que se pueden observar en la Figura5.

La forma más fácil de probar esta teoría en casa, es presionando el dedo sobre una hoja o portada de un cuaderno o libro de color negro, luego aplicarle talcos en pequeña cantidad, y a continuación se le quita el talco pegando pequeños golpecitos detrás de la hoja o portada, sin soplarlos ni pasarle la, mano por encima, solo pegándole por detrás de la superficie delgada. Cuando el talco sea removido del lugar donde presiono con el dedo, vera que su huella dactilar quedo marcada sobre la superficie.

Como las huellas dactilares son todas diferentes, también tienen ciertos aspectos parecidos, ya sea en forma o diferentes puntos característicos contenidos en la huella. Según la forma, se han identificado 4 tipos principales de patrones de huellas. Como se puede ver en la Figura6, las huellas de cada individuo pertenecen a uno de los grupos, representados aquí, y una vez más se recalca, que no existen 2 seres humanos, con las mismas huellas dactilares, al igual que otros aspectos de la biometría.

Figura No.6: Tipos de Huellas Digitales

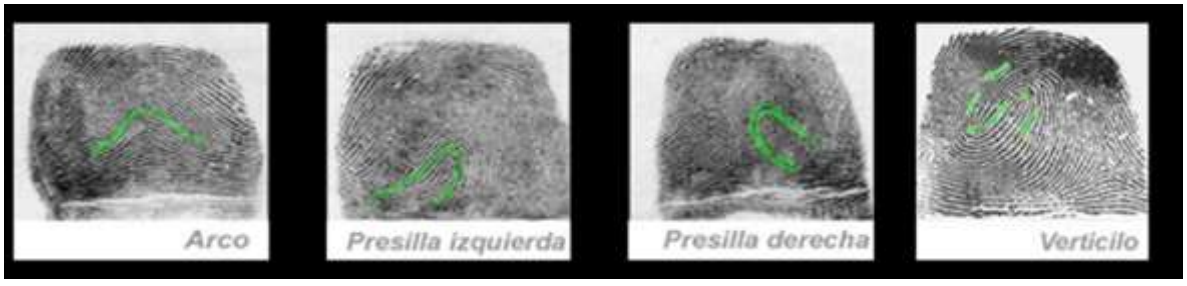


Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

Los puntos característicos o minucias (minuta), término usado en la medicina forense, son 7: islote, bifurcación, punto, cortada, horquilla, empalme y encierro (Figura7). Estas minucias son los datos que son captados por el Sistema de

Identificación Automatizada de Huellas Dactilares, o como es más Conocido AFIS, según su nombre en inglés (Automated Fingerprint Identification System). Estos puntos se recopilan en grupos y son captados por los sistemas para poder identificar a una persona para confirmar quien es. El sistema de AFIS fue principalmente diseñado para el FBI y Scotland Yard, para ayudarles a encontrar a los criminales. Debido a su gran impacto y aceptación mundial, hoy en día es uno de los sistemas de seguridad de acceso biométricos más usados en el mundo.

Figura No.7: Tipos de Minucias características de la huella

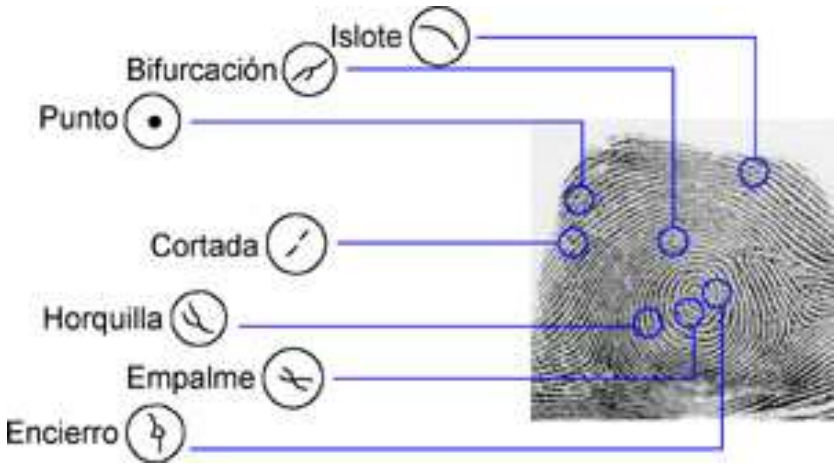


Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

El sistema AFIS es simplemente un identificador de personas mediante sus huellas dactilares, en donde usa un algoritmo para identificar las minucias, y compararlas con una base de datos, y encontrar al individuo dueño de las huellas. Como se dijo antes, este sistema se creó principalmente para el FBI y Scotland Yard, para poder identificar los dueños de las “armas homicidas” o rastros dejados en una escena del crimen. Un ejemplo de este sistema se ve todos los días en la televisión, donde los actores que hacen los papeles de criminalistas, encuentran las huellas en las armas homicidas, en el cadáver, y en los alrededores de la escena del crimen; ellos cogen las huellas, y las pasan

por el software de AFIS y si es un criminal, anteriormente detenido, se podría encontrar en la base de datos que tienen los policías o criminalistas.

El sistema AFIS es utilizado en la técnica de identificación mediante huellas dactilares, hoy en día, se venden dispositivos con lectores de huellas para accesos a cuartos, en los cuales se requiere cierto nivel de autorización, acceso a computadores y a diferentes archivos contenidos en el, control de asistencias, ya sea para reuniones, salones, auditorias, trabajo, etc., y muchos otros usos. Estos sistemas trabajan de la siguiente manera (Figura8):

1) Un lector de huellas digitales, capta la huella del individuo.
2) El lector envía los datos captados a un computador que contiene el software de identificación de huellas.
3) El computador empieza por la identificación de las minucias contenidas en la huella.
4) Entre las diferentes minucias, se trazan segmentos de líneas uniendo unas con otras.
5) Luego el ordenador, captura un conjunto de números, (coordenadas), que luego envía a la base de datos.
6) Si en la base de datos está el conjunto de numero, significa que el usuario esta registrado y tiene el acceso autorizado, de lo contrario, significa que no tiene acceso autorizado.

Figura No.8: Proceso de decodificación de la huella digital.

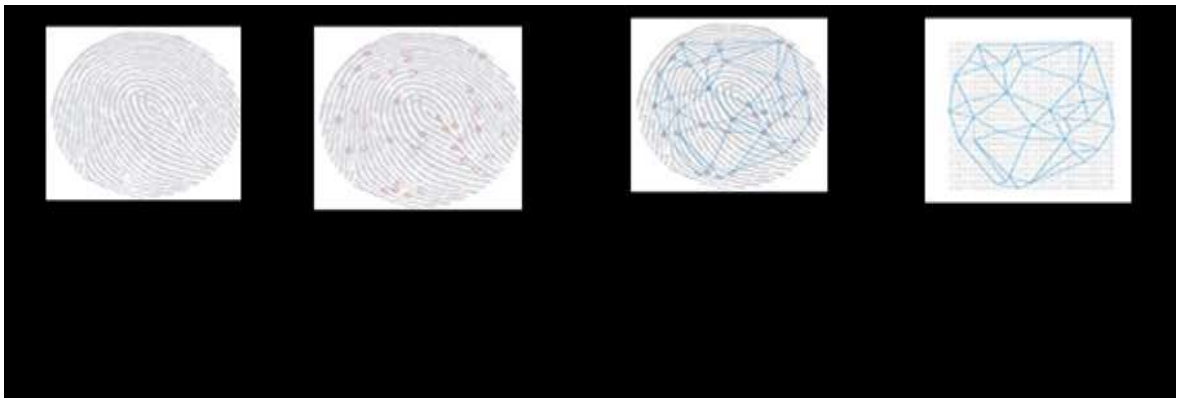


Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

El conjunto de datos que el computador captura con coordenadas, es decir, después de identificar las minucias y trazarlas, la huella es puesta sobre una especie de plano cartesiano, donde se capturan las coordenadas (Figura9), de cada minucia capturada, y estos se guardan en la base de datos y se comparan para autorizar la entrada del individuo.

Figura No.9: Forma de identificación de características.

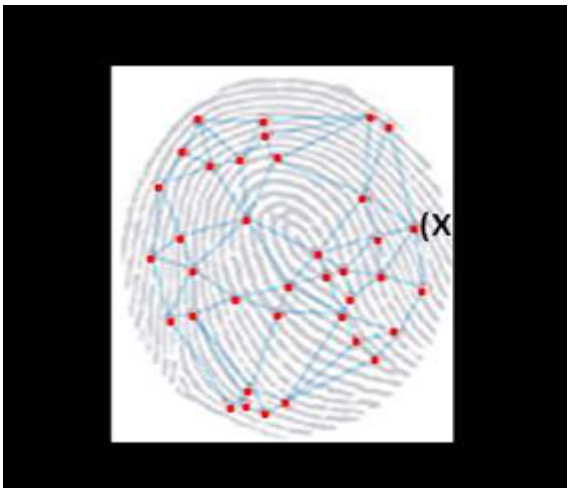


Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

Este es un sistema de seguridad muy utilizado en el mundo, pero al igual que todo, puede traer problemas ya sea debido a una mala captura, o a una mala verificación.

Los errores causados por una mala captura, pueden ser debido a:

- La calidad del lector: si el lector no es confiable y muy baja calidad de captura, la huella puede salir demasiado borrosa como para que el software detecte las minucias.
- Accidentes: si el individuo ha sufrido accidentes en los dedos después de haber guardado la huella en la base de datos, pueden haber errores, debido a que ciertos accidentes causan cambios permanentes en la yema del dedo cambiando también así la forma de la huella, haciéndola diferente a la que está en la base de datos.

- Alguna capa de suciedad: Debido al ambiente o entorno de trabajo en el cual se encuentre la persona, puede tener alguna sustancia sobre el dedo (ej. cemento), y esto llevara a una mala captura del dedo.

Por otro lado las malas comparaciones se muestran en la Figura10:

Figura No.10: Comparación entre el % de errores y el nivel de exigencia de los equipos

Imagen tomada de http://ciberhabitat.gob.mx/hospital/huellas/index.html

- Falsa Aceptación: Cuando se autoriza a alguien que no tiene acceso. Como se observa en la Figura10, para obviar este tipo de errores, se exige un mayor nivel de exigencia tanto en el software como en el lector.
- Falso Rechazo: Cuando no se autoriza a alguien que si tiene acceso.

Al inverso de la anterior, al tener un mayor nivel de seguridad en los equipos, se producen más errores de este tipo. Para concluir y terminar, este tipo de errores, hay que identificar el patrón tanto en el software como en el hardware, ya que con el método de las huellas dactilares se obtienen uno de los más altos porcentajes de confiabilidad y además con el dispositivo de lectura y el software de identificación no hay peligro de perder la llave de acceso [3].

3.2.2.3 Tarjetas Ópticas

Figura No.11: Tarjetas Ópticas

Imagen tomada de http://www.evartel.com.ar/imagenes/tarjetas_opticas.jpg

Es una tarjeta de almacenamiento de datos durable y segura, que únicamente puede ser leída por un laser; este tipo de tarjetas están formadas por dos niveles principales, uno reflectivo y otro no reflectivo. En el nivel reflectivo se codifica la información que se va a almacenar y poseen tres tipos de almacenamiento:

- Mayor capacidad: 6,00 MB
- Estándar: 4,2 MB
- Menor capacidad: 1,86 MB

El tipo de grabación que se usa en estas tarjetas es Worm, esto hace que la información que se incorpore a la tarjeta no pueda ser borrada o alterada por ningún motivo, lo que hace que la información guardada siempre sea exacta. Una de las principales características favorables de estas tarjetas es que la información contenida en ellas no es afectada por campos magnéticos ni electroestática y además puede soportar temperaturas de hasta 100°C.

Las tarjetas ópticas pueden almacenar diferentes tipos de información como por ejemplo: imágenes, fotos, firmas, huellas dactilares, datos de retina, radiografías, tomografías, texto, voz, etc.

3.2.2.4 Tarjetas Inteligentes

Figura No.12: Tarjeta Inteligente

Imagen tomada de: http://www.elplazas.com/images2/tarjeta_inteligente.jpg

La tecnología de las tarjetas que contienen un chip (circuito integrado), llevan 3 Décadas de existencia. La primera idea conceptual, se dio en Marzo de 1970 cuando el Dr. Kunitake Arimura, presento la primera tarjeta de plástico con un circuito integrado, empotrado en su interior y la llamo “Arimura Card”, donde precisó el proceso por el cual incorpora uno a mas circuitos integrados en una tarjeta para la generación de distintos tipos de señales. El hecho que marcaria el reconocimiento de los trabajos de Dr. Arimura, en el mundo Occidental fue la limitación de dicha patente a Japón, quedando libre en el resto del mundo. Para explorar dicha patente se fundó el “Instituto Arimura” y se fijo que todas las tarjetas que circularan por Japón, estuviesen o no fabricadas allí, debían estar licenciadas por dicho Instituto.

En 1974 un periodista Francés llamado Roland Moreno, concibió una tarjeta de plástico con un dispositivo programable en su interior (circuito integrado), dotado de mecanismos de autoprotección y capaz de gestionar transacciones económicas. Tras patentar el prototipo en Francia funda la empresa

INNOVATRON (Société Internationale Pour L'inovation) que se dedicara a extender la tarjeta y las patentes por la mayoría de países industrializados, con lo que se consiguió una ventaja competitiva con respecto a la patente del Dr. Arimura: La Expansión Internacional.

En Japón se siguió avanzando de manera que en 1978 apareció una nueva primicia: las tarjetas sin contactos, sin embargo, la industria de la tarjeta, a nivel mundial vendrá fijada por los avances de la empresa INNOVATRON, ya que su evolución se puede ver a través de las primeas patentes formuladas por EE.UU.

El 27 de Julio de 1976 (US 3971916): esta primera patente identifica los conceptos básicos de una "tarjeta chip" y su terminal asociado, detallando el control de acceso a la memoria, la protección de determinadas partes de esta y la forma de uso de la tarjeta para crédito y debito.

El 8 de Febrero de 1978 (US 4007355): extiende el concepto de comunicación involucrando a 2 grupos de participantes, típicamente los titulares y los suministradores.

El 30 de Mayo de 1978 (US 4092524): se desarrollaron ampliaciones en el control y la utilización de un PING.

El 25 de Julio de 1978 (US 4102493): se llevo a cabo la localización de la Circuitería dentro de la tarjeta, junto con algunas mejoras en la seguridad inherente y a finales de 1978 (US 4404464): se crearon los mecanismos de lectura de tarjetas.

La primera licencia que da INNOVATRON es a CII (Compagnie Internationale Pour L'informatique) Honeiwell Bull, a la que se conocerá a partir de 1986 por el único nombre de Honeiwell Bull, uno de los fabricantes lideres de ordenadores en Francia, pero por otro lado la división de electrónica de una

multinacional de Petróleo Flonic Schlumberger obtiene en 1979, la segunda licencia seguida por Phillips en ese mismo año con una licencia que solo cubría el territorio Francés.

Esta tecnología empezó a mejorar cuando aparecieron las primeras licencias en EE.UU, ya que este país era el gran motor tecnológico en esos años, sin embargo en EE.UU la gran tradición y fuerza que tenia la industria de las tarjetas de Banda Magnética y el hecho de utilizar los cheques para el pago de pequeña cuantía hizo que no se apostase, hasta hace un par de años, por ser esta tecnología de forma fuerte. Por otro lado debido a diversas circunstancias surge un gran apoyo del Gobierno Francés a esta tecnología, por lo que se montaron todo tipo de experiencias pilotos que ayudaron a la implementación de estas tarjetas y por eso Francia es considera gran motor de esta tecnología.

Para obtener los primeros desarrollos y tipos de tarjeta chip, los 3 fabricantes (Bull, Schlumberger y Phillips) reciben la licencia y dedican grandes recursos a convertir el concepto de Roland Moreno en una realidad. Sus esfuerzos materializados en diversos prototipos, admitieron un efecto innovador en la industria de la microelectrónica, y se alcanzaron niveles de integración que eran indispensables en la primera mitad de los años 70, pero al llegar al objetivo final Schlumberger impulso dos líneas de trabajo totalmente diferenciadas, mientras que Phillips y Bull abogaban por una solución basada en microprocesadores pero Schlumberger, desarrollo sus prototipos basándose en lógica programada.

Entre los años 76 y 78 Bull concibe una tarjeta con microprocesador cuyo primer prototipo, corre a cargo de un Ing. Francés llamado Eugene Michel y confía a Motorola la realización técnica del chip y los contactos. La arquitectura del microprocesador utilizada fue la del 6805, con una memoria de 8Kb. Por otro lado Phillips comienza su desarrollo basándose en el microprocesador 8021 de Intel que posteriormente cambiaria por 8051 y en el que utilizo una memoria EPRON de 16Kb.

La conclusión que se puede sacar fácilmente de estos primeros desarrollos es que ambos fabricantes no concebían en un principio la creación de tarjetas re-escribibles, ya que para eso habría que utilizar memorias borrables electrónicamente (EEPRON) que por entonces se encontraban en pleno desarrollo y era realmente costosa.

Mientras Bull y Phillips trabajaban en su proyecto Schlumberger, analizaba la viabilidad de crear una tarjeta de “circuito integrado”, con cierta inteligencia que pudiera competir en relación costo-seguridad con las tarjetas de banda magnética, las cuales estaban en el mercado y eran difíciles de destronar. Además, desde el inicio Schlumberger aposto por la creación de una tarjeta chip que tuviese las mismas dimensiones y características que las tarjetas financieras y que por lo tanto, siguiesen las normas IS7810 y 7811, creando una tarjeta con lógica cableada, incorporada a una memoria escribible electrónicamente (EPROM) de 4,6Kb y por ultimo desarrollaron la tecnología necesaria para incorporar un fusible dentro de un bloque de silicio, que sirviera para su destrucción y prohibir el acceso a determinadas zonas de la memoria.

Todo este desarrollo de Schlumberger desemboca en la realización de una tarjeta con pocas habilidades funcionales y reducida capacidad de programación después de su inicialización, pero con las dimensiones de la tarjeta de Banda Magnética, muy robusta y con un precio muy reducido, lo que le permitió competir y convirtió a Schlumberger en el primer fabricante mundial de tarjetas con circuito integrado hasta finales de los años 80.

El desarrollo de Phillips desemboco en una arquitectura distribuida, en la que el microprocesador y las memorias se encuentran independientes en el microchip. Este diseño hacia necesario, la existencia de un bus de comunicación entre los distintos microchips y esa era la fuente de los principales problemas de estos prototipos ya que este bus presentaba una determinada fragilidad que al doblar la tarjeta se rompía y además facilitaba la posibilidad de acceder a los datos.

Poco tiempo después, Bull presenta una tarjeta que finalmente tiene las dimensiones de la tarjeta Banda Magnética y le coloca el nombre de CP8 y también hace pública su intención de desarrollar en un año, una familia de terminales para tarjetas y a finales de 1981 la tecnología microelectrónica había evolucionado tanto que permitió la fabricación en mas de “chips” con las dimensiones adecuadas para que pudiesen incluirse en tarjetas de 0.76 mm de espesor, que es el de las tarjetas financieras definidas por ISO y por lo tanto podría extenderse esta tecnología a los cajeros existentes por Banda Magnética.

A la vista de los primeros desarrollos se empieza a encontrar una diferencia entre conceptos de cómo implementar una tarjeta chip, por un lado el concepto de Bull y Phillips y por otro el de Schlumberger.

De hecho en la actualidad las tarjetas de lógica programada siguen teniendo gran fuerza en determinados entornos, entonces, se llegó a realizar una gran clasificación de tarjetas que se llamaron así:

- *Tarjetas Inteligentes:* son aquellas que están basadas en un microprocesador y una memoria.
- *Tarjeta de Memoria:* son aquellas de circuito integrado en las que esté no contiene un microprocesador.

Por otro lado, tanto en las tarjetas de memoria como en las tarjetas inteligentes se puede establecer una nueva clasificación dependiendo del método de comunicación empleado y se han llamado así:

- *Con Contacto:* la comunicación se hace desde la conexión física de cada uno de los contactos metálicos de la tarjeta con los correspondientes del lector.
- *Sin contactos:* la comunicación se realiza de forma aérea mediante radiofrecuencia, por lo tanto no es necesario un contacto físico entre las tarjetas y un lector.

Han sido muchas las realizaciones en las que se han mantenido el mismo tipo de chip pero en otras se han cambiado los soportes por otro tipo u objeto acondicionándolo a varios tipos de mecanismos inteligentes [3].

Las tarjetas inteligentes son dispositivos que poseen las mismas características físicas de las tarjetas usadas en bancos (tarjetas crédito y debito), las cuales tienen un microprocesador incrustado que controla el acceso a la información que contienen. Estas tarjetas son actualmente utilizadas para almacenar información de cualquier tipo, como por ejemplo información referente a bancos, salud, teléfonos, información personal etc., también son usadas para control de acceso y seguridad (por su capacidad de encriptamiento, manejo de claves públicas y privadas, etc.), como también para pagos electrónicos (monederos electrónicos, tarjetas de llamadas) y más.

Este tipo de tarjetas es muy popular hoy en día y va aumentando su uso a diferentes aspectos, pero como todo posee ventajas y desventajas, algunas de ellas son:

- Ventajas:
  - Dispositivo seguro por definición
  - Capaces de procesar información (además de almacenarla)
  - Mayor versatilidad (al poder ser programadas).
  - “Gran” espacio de memoria (2 KBs, 4 KBs, ...)
  - Pueden ser usadas en múltiples aplicaciones.

- Desventajas:
  - Lenguajes de programación de tarjetas dependientes del hardware.
  - Programación de las tarjetas en ensamblador.
  - Aplicaciones desarrolladas exclusivamente por el proveedor de la tarjeta.

Lo que hace a estas tarjetas “inteligentes” es el uso del microcontrolador en su chip, lo que ayuda a que se pueda insertar, leer, modificar y manipular toda la información que este contenga, además de esto este tipo chips es muy seguro debido a que este dispositivo es a prueba de falsificación, además posee un control de los accesos a memoria y también cuenta con protección a los datos en algunos casos con un PIN.

Toda la información referente a esta tarjetas se basa en la **ISO 7816**, que es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional De Normalización (ISO) y Comisión Electrotécnica Internacional (IEC). Este estándar nos da toda la información referente a la tarjeta como por ejemplo sus características físicas, eléctricas, mecánicas, la interfaz de programación para comunicarse con el microchip, información sobre los microcontroladores y la manera en que se debe realizar su programación.

Esta ley se divide en 10 numerales, los cuales son:
7816-1: Características Físicas.
7816-2: Dimensiones y ubicaciones de los contactos
7816-3: Señales Electrónicas y Protocolo de Transmisión
7816-4: Comandos de intercambio inter-industriales
7816-5: Sistema de Numeración y procedimiento de registración
7816-6: Elementos de datos inter-industriales
7816-7: Comandos inter-industriales y Consultas Estructuradas para una Tarjeta
7816-8: Comandos inter-industriales Relacionados con Seguridad.
7816-9: Comandos adicionales inter-industriales y atributos de seguridad.
7816-10: Señales electrónicas y Respuesta al Reset para una Smart Card Síncrona.

Estas tarjetas poseen en su superficie 8 contactos, los cuales representan la única interfaz electrónica que existe entre la tarjeta y un lector. Todas las señales eléctricas circulan a través de estos contactos, lo cuales se dividen en:

Figura No.13: Contactos del chip de la Tarjeta Inteligente

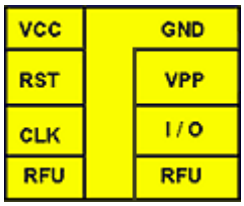


Imagen tomada de: http://es.wikipedia.org/wiki/ISO_7816

- Vcc: es el que toma de corriente o la fuente de poder del chip, la energía que necesita la proporciona el dispositivo hardware con el que la tarjeta interactúa.
- RST: es el Reset.
- CLK: es el reloj determina la velocidad de funcionamiento de la tarjeta.
- GND: se puede decir que es el polo a tierra del chip.
- VPP: es el voltaje externo que sirve para programar la memoria de la tarjeta y donde se encuentra la memoria EEPROM.
- I/O: es el encendido y apagado del chip.
- RFUs: no tienen asignadas funciones por el momento.

La forma en que se puede manipular la información contenida en las tarjetas se realiza por medio de los paquetes de datos APDU (Application Protocol Data Units), estos paquetes pueden contener un mensaje de comando o un mensaje de respuesta. Una tarjeta inteligente siempre espera por un APDU comando desde una terminal; esta entonces ejecuta la acción especificada en el APDU y responde a la terminal con un APDU respuesta. Los APDUs comandos y APDUs respuestas son intercambiados alternativamente entre una tarjeta y una terminal [1].

Los tipos de paquetes APDU comando y respuesta son:

Figura No.14: Tipos de Paquetes de los Comandos APDU

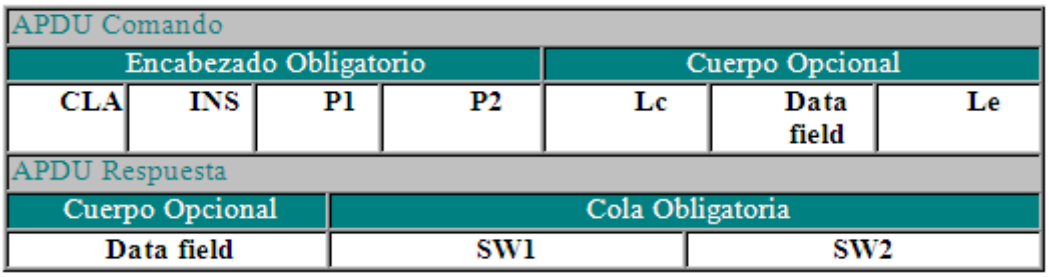


Imagen tomada del libro: Smart Card developer's kit

APDU de Comandos

- CLA: identifica que el request responde al estándar ISO-7816
- INS: código de la instrucción
- P1: primer parámetro
- P2: segundo parámetro
- Lc: número de bytes en el campo de datos
- Data: datos
- Le: número máximo de bytes esperados en el campo de datos del APDU de respuesta

APDU de Respuesta

- Data: cuerpo de datos
- SW_1: primer byte de la palabra de estado
- SW_2: primer byte de la palabra de estado

- **Tamaño y materiales de la Tarjeta Chip**

Todas las características de este tipo de tarjetas esta determinado en el estándar ISO 7816, que define completamente los aspectos físicos y técnicos como por ejemplo: temperatura, flexibilidad, funciones, las características del circuito y los contactos, etc.

Los tamaños de las tarjetas inteligentes son los siguientes:

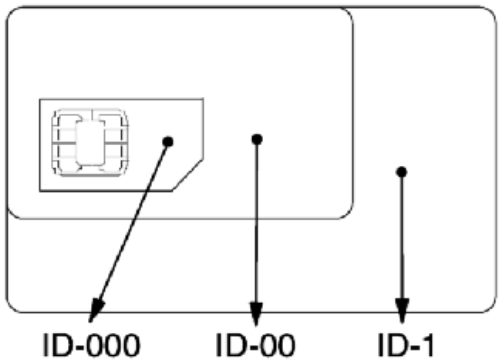
ID-1 nominalmente 85,60 mm ancho por 53,98 mm alto por 0,76 mm espesor.

ID-2 nominalmente 105,00 mm ancho por 74,00 mm alto por 0,76 mm espesor.

ID-3 nominalmente 125,00 mm ancho por 88,00 mm alto por 0,76 mm espesor.

ID-000 nominalmente 25 mm ancho por 15 mm alto por 0,76 mm espesor.

Figura No.15: Tamaños Tarjeta Inteligente



Fuente: Grupo Investigador

Las características físicas de la tarjeta inteligente son las siguientes:

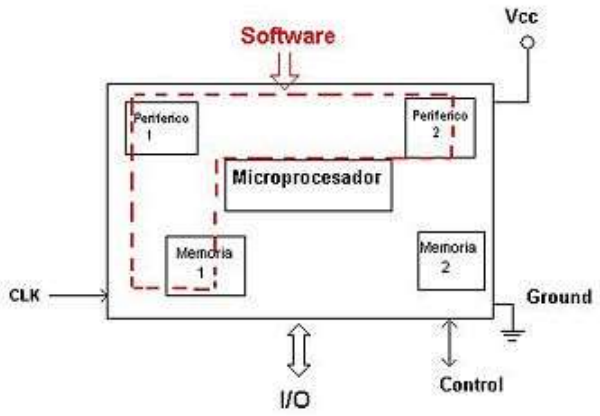
- El material usado en las tarjetas es el plástico, del cual se usan 2 tipos:
  - PVC: plástico con relieve pero no reciclable.
  - ABS: plástico sin relieve pero si es reciclable.

Figura No.16: Tipos Materiales Tarjeta Inteligente

Fuente: Grupo Investigador

- Microcontrolador:
    - 8 bit, 16 bit y 32 bit RISC.
    - 8 Kbyte de memoria no volátil.

Figura No.17: Microcontrolador Tarjeta Inteligente



I

Imagen tomada de: http://upload.wikimedia.org/wikipedia/commons/thumb/c/cb/Microcontrolador.jpg/400px-Microcontrolador.jpg

- Chip de cilicio con un tamaño de 25 mm^2.

Figura No.18: Chip Cilicio Tarjeta Inteligente

Fuente: http://www.monografias.com/trabajos10/tarin/tarin.shtml?monosearch/chipsilicio.jpg

- **Clasificación de las Tarjetas Inteligentes**

Existen dos tipos de clasificación para las tarjetas inteligentes, las cuales son:

- Funcionamiento del circuito integrado:

- Tarjeta chip.

Estas tarjetas poseen uno o varios circuitos electrónicos, además de varios tipos de celdas de memoria ordenadas, también tienen la habilidad de almacenamiento dinámico y la capacidad de lectura, escritura, borrado y procesamiento de datos.

- Tarjeta con memoria.

Estas tarjetas ofrecen almacenamiento de datos, también poseen una memoria no volátil y una cantidad limitada de circuitos para control y seguridad. Este tipo de tarjetas son usadas en aplicaciones simples (telefonía).

- Tarjetas Híbridas.

Este tipo de tarjetas contienen en su interior uno o varios microprocesadores, una banda magnética y un código de barras, además estas tarjetas pueden accesar información de diferentes sistemas de hardware.

- Tarjeta de interfaz dual.

Estas tarjetas contiene solamente un chip que soporta los dos tipos de interfaz, los de contacto y los de sin contacto, permitiendo el acceso de la información por cualquiera de los dos.

- Tipo de Interfaz:

- Tarjetas con contacto.

Estas tarjetas necesitan ser insertadas en un lector para poder cumplir su funcionalidad, ya que poseen un chip en la parte frontal que al ser insertado en el lector correspondiente, hacen contacto y se transfieren los datos entre ellos.

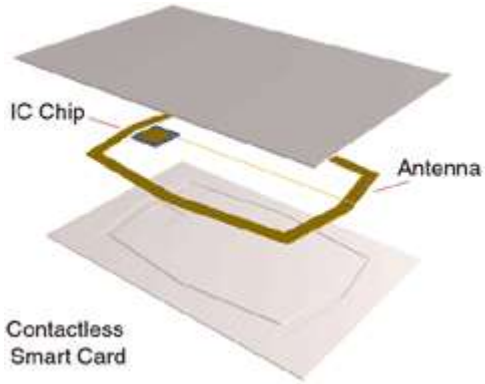
Figura No.19: Tarjeta Inteligente de contacto

Fuente: http://www.monografias.com/trabajos10/tarin/tarin.shtml?monosearch/smartcard

- Tarjetas sin contacto.

Este tipo de tarjetas necesita ser acercada a una distancia mínima de 10 cm del lector para funcionar, debido a que poseen un chip y una antena en su interior, los cuales le permiten comunicarse con transmisores y receptores remotos.

Figura No.20: Tarjeta Inteligente sin contacto



Fuente: http://upload.wikimedia.org/wikipedia/commons/thumb/c/cb/Microcontrolador.jpg/400px.jpg

- **Tipos de memoria usados en las tarjetas inteligentes**

- ROM (memoria de solo lectura).

Contiene el sistema operativo del circuito, el cual controla la comunicación entre el lector y el chip integrado, además el sistema operativo también controla el acceso a los archivos del sistema y después de que se han escrito los datos en su memoria no pueden ser modificados.

- RAM (memoria de acceso aleatorio).

Es una memoria volátil usada por el Microcontrolador para almacenar temporalmente los registros de la tarjeta.

- EEPROM (memoria de solo lectura programable y borrable).

Es una memoria no volátil de lectura-escritura para el almacenamiento de datos, este tipo memoria es el que poseen las tarjetas inteligentes usadas en los carnets de la Universidad Autónoma de Bucaramanga (UNAB). El acceso a esta memoria se controla por medio del sistema operativo del circuito, algunos de los datos que puede almacenar esta memoria son: el pin de un usuario, el número de serie de la tarjeta, y para el caso de los carnets de la Universidad el código del alumno y en el caso de los docentes su cedula. La mayoría de las memorias EEPROM son usadas para almacenar registros biométricos, como por ejemplo: datos financieros, tarjetas de pago, información demográfica y registro de transacciones. La memoria puede ser programada o borrada de decenas hasta cientos de miles de veces y su capacidad está entre un rango de entre 128 Kbytes hasta 256 Kbytes.

- FRAM (memoria RAM ferroeléctrica Fe-RAM).

También es una memoria no volátil, Esta memoria puede leer datos cientos de veces más rápido a bajo voltaje, además combina la velocidad de lectura y escritura de una memoria RAM con la de almacenar datos cuando se apaga la fuente de poder.

- Memoria FLASH.

Es una memoria energizada constantemente, no volátil que puede ser borrada y reprogramada en bloques. Las memorias flash son menos costosas que las memorias EEPROM, pero no puede ser programada y borrada tantas veces y por lo general no puede programarse o borrarse bytes sencillos de memoria [2].

3.3 COMPARACIÓN ENTRE TECNOLOGÍAS

Capacidad de almacenamiento:

Tarjeta Inteligente	**128KB**
Huella Dactilar	**512MB**
RFID	**>512KB**
Tarjeta Óptica	6MB
Tarjeta Magnética	2K
Código de Barras	10B

Número de errores por año:

Tarjeta Inteligente	**100**
Huella Dactilar	**2000**
RFID	**650**
Tarjeta Óptica	800
Tarjeta Magnética	1000
Código de Barras	900

Reescritura:

Tarjeta Inteligente	**Si**
Huella Dactilar	**Si**
RFID	**Si**
Tarjeta Óptica	No
Tarjeta Magnética	Si
Código de Barras	No

Seguridad:

Tarjeta Inteligente	* Configuración de claves de acceso para operaciones de lectura-escritura y configuración. * Encriptación tanto en software como hardware.

	* Protección de acceso en partes de la tarjeta.
Huella Dactilar	* Encriptación de Datos (3 niveles). * Encriptación en software. * Control de acceso Biométrico.
RFID	* Configuración de claves de acceso para operaciones de lectura-escritura y configuración. * Lecturas más rápidas y más precisas. * Encriptación tanto en software como hardware. * Mejor utilización de los activos. * Protección de acceso en partes de la tarjeta.
Tarjeta Óptica	* Grabación WORM, que evita que la información pueda ser modificada o borrada, de cualquier forma.
Tarjeta Magnética	* Encriptación en software. * No posee mecanismos de control para la lectura de información.
Código de Barras	* Únicamente posee encriptación por software.

<u>Porcentaje de error:</u>

Tarjeta Inteligente	**0.03%**
Huella Dactilar	**0.8%**
RFID	**0.05%**
Tarjeta Óptica	n/a
Tarjeta Magnética	2%
Código de Barras	1%

<u>Número de maquinas mantenidas por un técnico:</u>

Tarjeta Inteligente	**100**

Huella Dactilar	**20**
RFID	**50**
Tarjeta Óptica	15
Tarjeta Magnética	20
Código de Barras	20

Variedad de Aplicaciones:

Tarjeta Inteligente	* Permite multiplicidad de aplicaciones, gracias a su característica de reescritura y a la alta capacidad de almacenamiento que puede guardar en una sola tarjeta.
Huella Dactilar	* Soporta múltiples aplicaciones gracias a su tecnología biométrica ya puede ser usado por ejemplo en accesos a oficinas, maquinas, expendedoras, maquinas recreativas, etc.
RFID	* Permiten la multiplicidad de aplicaciones, ya que las etiquetas RFID se ven como una alternativa que reemplazará a los códigos de barras, además gracias a su reescritura pueden ser usadas en varios dispositivos al mismo tiempo.
Tarjeta Óptica	* No permite la multiplicidad de aplicaciones, a pesar de su gran capacidad de almacenamiento, debido a que no puede usarse en aplicaciones donde se deban modificar datos.
Tarjeta Magnética	* No es posible usarla en varias aplicaciones, debido a su poca capacidad de almacenamiento.

Código de Barras	* Al igual que la Tarjeta Magnética no puede usarse en otras aplicaciones por su reducida capacidad de almacenamiento.

3.3.1 Ventajas de las Tarjetas Inteligentes Como se pudo observar en las anteriores tablas, algunas de las ventajas que poseen las tarjetas inteligentes frente a otras tecnologías de acceso son por ejemplo su seguridad, su porcentaje de error, etc. A continuación se presentaran otros aspectos positivos de las tarjetas inteligentes.

Seguridad: estas tarjetas poseen un gran número de mecanismos de protección para sus datos, algunos de ellos son por ejemplo: el pin del usuario, que hace que la tarjeta sea única gracias a la clave personal y otro mecanismo son los algoritmos encriptados, que permiten asegurar la información almacenada. Estas son algunas de las características que nos llevan a decir que las tarjetas inteligentes son más seguras y confiables que las tarjeas de banda magnética, las cuales solamente guardan información en su exterior la cual puede ser fácilmente copiada.

Actualización: debido al tipo de memoria que usan estas tarjetas (EEPROM) tienen el poder de reprogramarse desde un Microcontrolador de manera rápida y fiable.

Evolución: estas tarjetas gracias a sus características, se les pueden añadir más aplicaciones de las que poseen actualmente, lo que lleva a que incrementen su valor y además se incorpora rápidamente a las tecnologías en desarrollo.

Tamaño y material: gracias a sus diferentes tamaños el usuario puede llevar consigo gran cantidad de datos en muy poco espacio, además el material del

que están hechas las tarjetas permite que sean expuestas a altas temperaturas, agua y a usos fuertes sin perder sus característica originales.

Variedad de aplicaciones: una sola tarjeta puede contener varias aplicaciones con diferentes modos de seguridad y de control de acceso.

Mecanismo de conteo: pueden administrar múltiples contadores para almacenar distintos tipos de datos.

Funcionamiento: los lectores para este tipo de tarjetas pueden funcionar sin estar conectados a una red central, algunos de estos lectores no necesitan trabajar con una base de datos para obtener detalles para su operación en algunos de ellos basta con conectarse solo a la tarjeta.

Almacenamiento: el rango de almacenamiento de estas tarjetas se encuentra actualmente entre 128 Kbytes hasta 256 Kbytes de datos dependiendo de la tarjeta usada, además comparada con la tarjeta de banda magnética puede almacenar entre 10 y 100 veces más información.

3.3.2 Uso de Tarjetas Inteligentes en la Actualidad Hoy en día la tecnología avanza cada vez más rápido y en el mundo de las aplicaciones inteligentes se da el mismo factor de crecimiento, haciendo que sus componentes se estén adaptando día a día a las nuevas tendencias y proporcionando nuevas soluciones a las necesidades de los usuarios. Las tarjetas inteligentes actualmente son usadas en numerosas entidades y de diferentes maneras, ayudando a que las personas y las compañías tengan mejores servicios, algunas de las aplicaciones en las que están presentes estas tarjetas son:

- Tarjetas prepago.
- Tarjetas para gasolina.
- Monederos electrónicos.

- Tarjetas de Bancos (crédito y debito).
- Tarjetas de atención medica.
- Tarjetas de telefonía móvil.
- Tarjetas Universitarias (por ejemplo: carnet UNAB).
- Llaves electrónicas.
- Aplicaciones Biométricas.

4. DISEÑO METODOLÓGICO

4.1 TIPO DE INVESTIGACIÓN

El proyecto se desarrollara dentro del enfoque investigativo de participación – acción de corte explorativo, tendiente a develar el concepto de una programación procedimental de desarrollo integrado visual que permita estar relacionado con el concepto de programación estructurada, modularizada y con una programación orientada a los objetivos trazados para que el programador o lo usuarios puedan determinarlos con su mayor potencia en cualquier gestión de aplicación.

El conocimiento logrado a través de este enfoque nos permite tener un concepto claro de cómo funciona el prototipo y la forma de desarrollo de todas las aplicaciones que este contiene.

4.2 PROCESO TÉCNICO

Ante este tipo de investigación, se hace necesario elaborar un proceso técnico de evaluación y seguimiento que permita desarrollar una serie de etapas o tareas para detectar la problemática actual sobre la implementación del prototipo más adecuado que le admita a la universidad los diferentes alcances de control y seguridad dentro de la tecnología y la administración.

4.3 DESCRIPCIÓN DEL PROCESO TÉCNICO

En el proceso de investigación se tendrá en cuenta una estructura que contiene las fases de diseño y un proceso sistematizado para conseguir los objetivos que el proyecto se propone, teniendo en cuenta la interacción que relativamente se establece entre los indicadores, el modelo conceptual (Numeral 4.1) y las bases teóricas (Numeral 4.2).

Figura No.21: Proceso Técnico de Evaluación Diagnostica (Indicadores).

Fuente: Diseño Grupo Investigador

Durante el desarrollo del diseño metodológico se debe tener en cuenta un listado de tareas para los diseños de aplicación, el esquema de las dependencias de una tarea con otra, los criterios de comprobación de las tareas y de los resultados de las mismas, la escritura del código fuente que debe responder a los posibles sucesos que se generen en tiempo de ejecución sobre los controles del soporte grafico de la aplicación, la comprobación de la aplicación sometiéndola a las pruebas necesarias para poder observar si se producen los resultados en cada una de sus partes, la recopilación de información referente al tema en textos, internet, consultas tutoriales, las orientaciones de los asesores y luego crear los paquetes que se deben distribuir a través de herramientas para la compilación y empaquetado de todos los archivos que lo conforman para su implementación y la disponibilidad que este dispositivo tenga para el personal que lo utilice, ya que se debe tener en cuenta la posible pérdida de tarjetas y en algunos casos como para la huella digital la falta de dedos en lagunas personas por mutilación o heridas que puedan tener en sus dedos que hacen que sus huellas no sean reconocidas.

4.3.1 Población Objeto de Estudio La investigación se realizará para la comunidad Institucional y las diferentes instalaciones de la Universidad Autónoma de Bucaramanga.

4.3.2 Muestra Como el estudio es de tipo técnico se tomara como muestra la interacción entre un computador y un lector que permita desarrollar el trabajo de campo y colocar en marcha la propuesta que se desarrollara en el proyecto.

4.3.3 Instrumentos El grupo investigador para lograr una verdadera socialización de los componentes o indicadores antes descritos seleccionara los medios instrumentales más apropiados para la recolección de la

información y el reconocimiento a fondo de la autenticación del material que será utilizado para la implementación del dispositivo de control de acceso.

4.3.3.1 Selección de Instrumentos

- Observación directa e indirecta.
- Revisión documental.
- Jornadas pedagógicas de trabajo.
- Entrevistas y encuestas.
- Diario de campo.

4.3.3.2 Aplicación de instrumentos De acuerdo con el cronograma general (Trabajo de campo sobre los diferentes componentes del proyecto) se elaboraran y aplicaran los diferentes instrumentos a la muestra representativa así:

- Observación directa e indirecta: determina las normas de comportamiento y desarrollo de la comunidad Institucional y los diferentes elementos de aplicación de los dispositivos a seleccionar.

- Revisión documental: se utilizara para precisar los diferentes conceptos con el fin de elaborar el marco teórico que sirva de fundamento al desarrollo del estudio.

- Jornadas pedagógicas de trabajo: son instrumentos metodológicos que se utilizaran para desarrollar procesos de actualización y capacitación con el fin de transformar la situación actual en una realidad estructurada y vivencial.

- Entrevistas y encuestas: serán dirigidas al personal involucrado en el desarrollo del proyecto.

- Diario de campo: se utiliza con el objeto de recoger información básica sobre el área de trabajo y llevar un control estricto del avance de la labor investigativa.

Todos estos aspectos determinaran los problemas y necesidades que se tienen en torno a la seguridad y el acceso a las aulas del plantel, que le permitirá al grupo investigador basado en estos aspectos pronosticar y seleccionar las alternativas de solución que después de evaluadas se podrá formular y ejecutar la mejor propuesta.

4.3.4 Juicio Valorativo Siguiendo el proceso metodológico planteado en el desarrollo de la investigación, se encontró que haciendo la comparación de toda la información, la problemática está centrada en un 99% en la carencia de instrumentos sensibilizadores que permitan la organización y estructuración de un verdadero dispositivo de control de acceso, que apruebe de una manera eficiente el acceso de los usuarios que conforman la comunidad educativa de la UNAB.

4.4 DETERMINACIÓN DE PROBLEMAS Y NECESIDADES

- La institución carece de un sistema de seguridad y asistencia que permita controlar el ingreso a las aulas por parte de los usuarios.

- No existen los espacios de participación comunitaria que permita agilizar los procesos administrativos y técnicos para este sistema de seguridad.

- Se identifico que la empresa DYETRON, contrato con la Universidad con el fin de desarrollar un proyecto viable que permitiera este control de acceso, pero no se llevo a cabo por diferentes inconvenientes y el Director de esta

investigación (Ing. Miguel Cadena), nos oriento con el fin de colocar en funcionamiento dicho sistema.

- Las primeras Tarjetas Inteligentes y lectores que fueron donados por el Banco Santander a la Universidad no fueron colocadas a prueba para establecer su funcionamiento y fueron almacenadas en la Universidad.

- La Universidad junto con la compañía DYETRON capacitaron a un Ingeniero para que se hiciera cargo del desarrollo del proyecto y colocara a funcionar el dispositivo, pero durante el trascurso de esta investigación no se le pudo ubicar para compartir información y experiencias acerca de los dispositivos.

- Al continuar con las investigaciones se logro hacer contacto con la compañía GEMALTO (fabricante de las tarjetas inteligentes), a los cuales se les solicito información (comandos APDU) y estos enviaron respuesta a lo solicitado por el grupo investigador para manipular los datos de las tarjetas, pero estos comandos no funcionaron, debido a que las tarjetas tenían protección y se debía seguir un manual de usuario para su implementación.
- A través de correos electrónicos y llamadas se estableció una nueva comunicación con la empresa DYETRON, donde se le solicitaba información referente al manejo de las tarjetas (escritura, borrado, lectura, etc.) de forma inmediata se recibió unas nuevas tarjetas y que el manual existente en la Universidad contenía los procesos a seguir para la manipulación de estos instrumentos.

- Siguiendo con el trabajo de campo para conseguir el manual de procesos técnicos y manipulación de los diferentes códigos, se determino que no se encuentra en ningún archivo y/o biblioteca de la institución y sin esta metodología es imposible el acceso a la lectura del dispositivo para su completo funcionamiento.

4.5 PRONOSTICO

Se hace necesario buscar otros procesos metodológicos y técnicos de lectores y tarjetas inteligentes con su propio manual de procedimientos para que los códigos aprueben la lectura de las tarjetas y el prototipo digital de control de acceso, conectado a la red interna, que permita o niegue la entrada al usuario que hace parte de la Universidad Autónoma de Bucaramanga.

4.6 ALTERNATIVAS DE SOLUCIÓN

- Motivación a los estudiantes de sistemas y Mecatrónica para que inventen un prototipo de control de acceso que busque solucionar el problema de la entrada y salida de las aulas de trabajo de los usuarios para que el control sea viable y permanente en la universidad.

- Información a los ingenieros asesores y al ingeniero coordinador del proyecto para enterarlos sobre los diferentes procedimientos explorados y las experiencias adquiridas con el fin de elaborar un informe complementario anexo al proyecto.

- Organización estructural y conceptual de una **nueva tecnología** que contenga el manual de procedimientos, los lectores y las tarjetas que conectada la red interna permita la lectura positiva o negativa del dispositivo cuando el usuario necesite utilizar cualquier aula.

- Instalación del prototipo de acceso y control en las diferentes aulas por los estudiantes de sistemas, basándose en el proyecto elaborado por el grupo investigador.

4.7 SELECCIÓN Y EVALUACIÓN DE LA ALTERNATIVA

4.7.1 Selección de la Alternativa Haciendo un análisis minucioso de las alternativas de solución tratadas en esta investigación, hemos llegado a detectar, que la número tres, enmarca globalizada mente a las demás, volviendo las estrategias pedagógicas dentro de la propuesta de desarrollo técnico y procedimental.

"Organización estructural y conceptual de una nueva tecnología que contenga el manual de procedimiento, los lectores y las tarjetas inteligentes que conectada a la red interna permitan la lectura positiva o negativa del dispositivo cuando el usuario necesite utilizar cualquier aula de la Universidad."

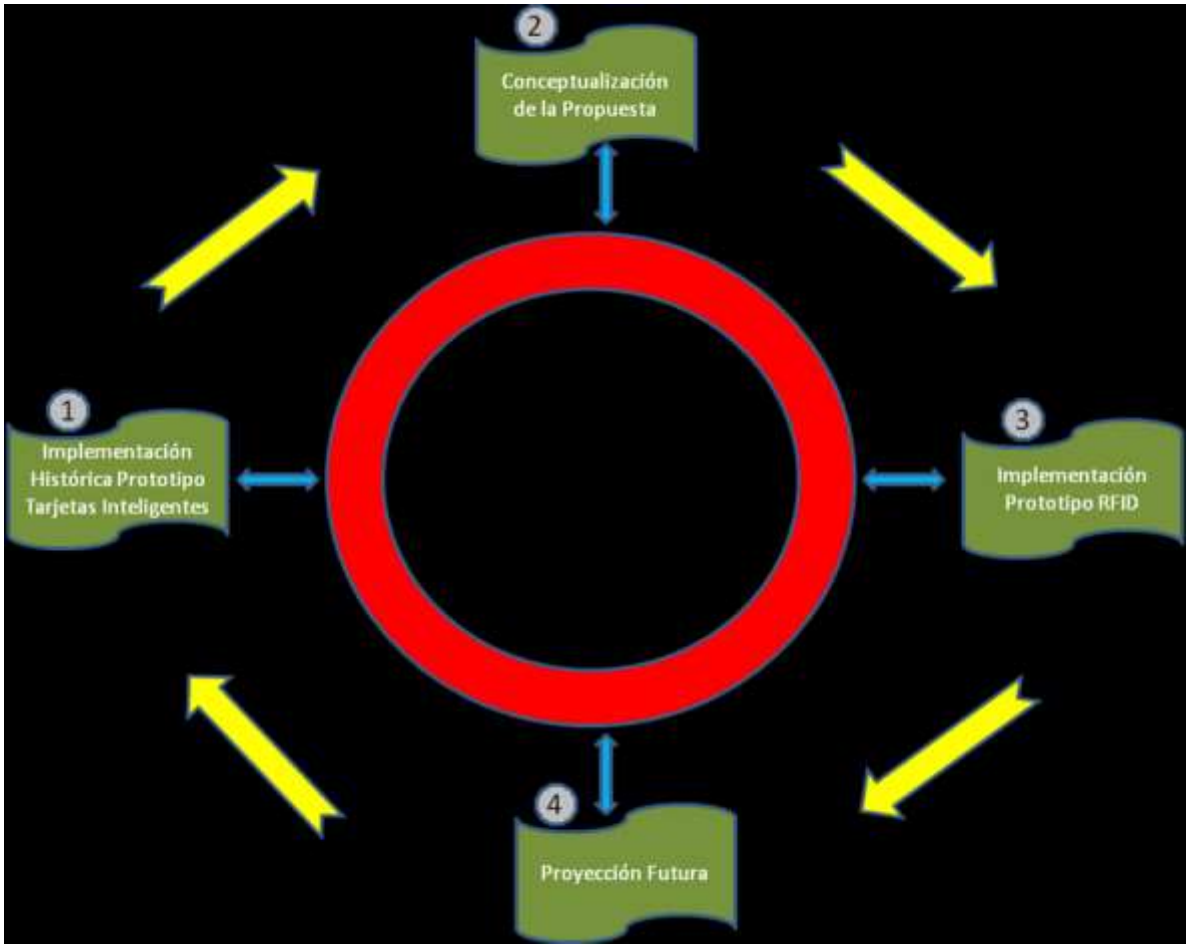
4.7.2 Evaluación de la Alternativa

Evaluando la alternativa seleccionada se encontraron todos los aspectos favorables para darle solución a estas debilidades detectadas en el plantel sobre el ingreso a las aulas, facilitando el cambio total de la administración y utilización de estos medios con el fin de prestar un servicio directo y decisivo en beneficio de la comunidad educativa.

5. FORMULACION Y EJECUCIÓN DE LA PROPUESTA

5.1 PROYECCIÓN DE LA PROPUESTA

Figura No.22: Proyección de la Propuesta



Fuente: Diseño Grupo Investigador

5.1.1 Implementación Histórica Prototipo Tarjetas Inteligentes Todas las comunicaciones de hoy en día, manejan cierto tipo de protocolo(s) de comunicación de datos entre los diferentes puntos o terminales. Las tarjetas inteligentes no son excepción de esta guía. Los protocolos más comunes que

manejan la comunicación de los datos entre el lector y la tarjeta son el protocolo T=0 y T=1, cada uno con sus ciertas características.

Al establecer la comunicación del lector con la tarjeta, esta lleva a cabo un proceso estandarizado de inicialización de la comunicación. El lector se vuelve “maestro” y la tarjeta “esclavo”. La comunicación se maneja de forma Half-Duplex; cuando el lector envía un comando a la tarjeta, este se bloquea hasta que reciba una respuesta. La forma de comprobar que se ha establecido la comunicación, es verificar la recepción del ATR (Answer-To-Reset). El ATR es una cadena de 33 o menos bytes en formato hexadecimal, en los cuales se establecen la forma de comunicación, el ordenamiento de bits, protocolo de comunicación, y unos caracteres históricos opcionales, que contienen datos sobre la compañía que creo de la tarjeta. La Figura 1 muestra un diagrama que resume cómo se establece la conexión, y los estados de la tarjeta en ciertas situaciones [1]

Figura No.23: Diagramas de Estado

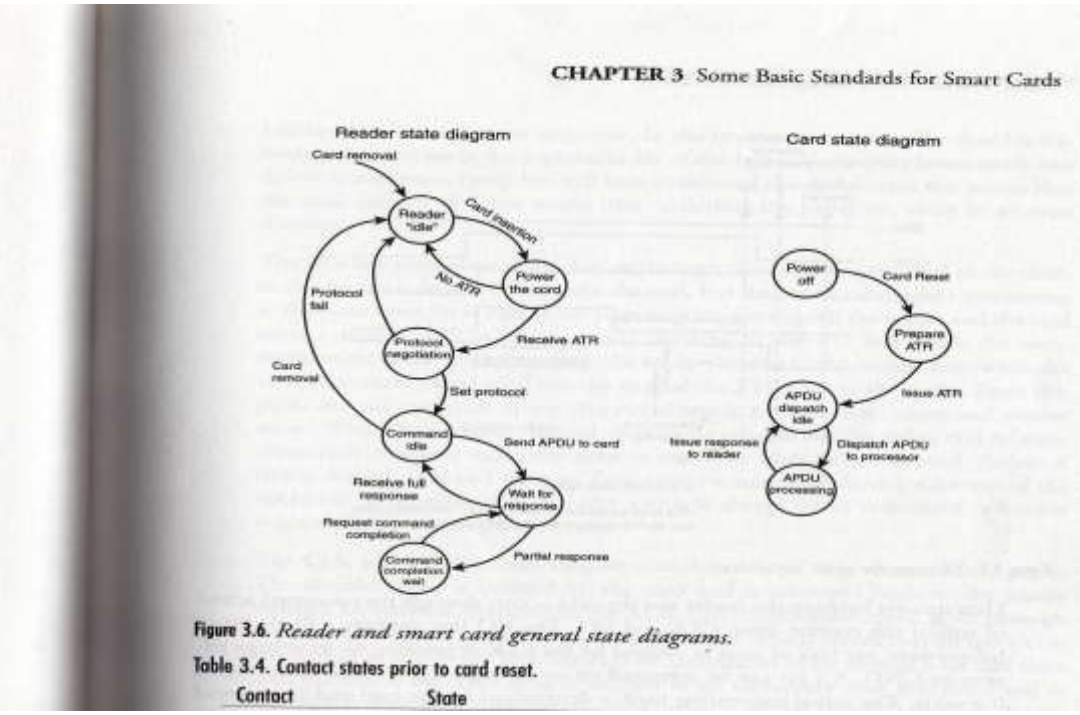


Figura tomada del libro: Smart Card developer’s kit

5.1.1.1 Protocolo T=0 es un protocolo orientado a bytes. Como en los otros protocolos de tarjetas inteligentes, trabaja en un modo de comando-respuesta; manda un comando del lado del lector a la tarjeta, y luego espera recibir una respuesta de la tarjeta.

El protocolo T=0 envía 1 byte a la vez, pero para poder enviar 1 byte, son necesarios enviar 10bits. La detección de errores en el protocolo T=0, se hace mirando el bit de paridad, que se coloca al final de los 10 bits enviados, como se ve en la Figura 15. Si no hay error entonces el bit de paridad es par, si hay error entonces es impar. El proceso de recuperación de errores, lo hace el lado del canal que recibe los datos. Al detectar algún error, el lado receptor, pone el estado de la línea de E/S en un bajo estado. Normalmente si no hay ningún error, la línea de E/S esta en un estado alto después de recibir los 10bits, entonces al tener la línea de E/S en un estado bajo, significa que hay un error, entonces el lado receptor espera que el lado transmisor reenvié el byte.

La detección de errores depende principalmente del canal de transmisión; si el canal de transmisión es muy bueno, el proceso de recuperación y detección de errores, es pocamente usado; si el canal de transmisión es muy malo, el proceso detección y recuperación de errores, se usara tanto que en algún momento fallara. Cuando esto pase, y si la tarjeta lo detecta, esta se encuentra programada para que deje de responder a los comandos enviados por el lector, entonces este enviara una señal para reiniciar el protocolo de comunicación para que se empiece a transmitir datos otra vez [1].

Figura No.24: Protocolo T=0

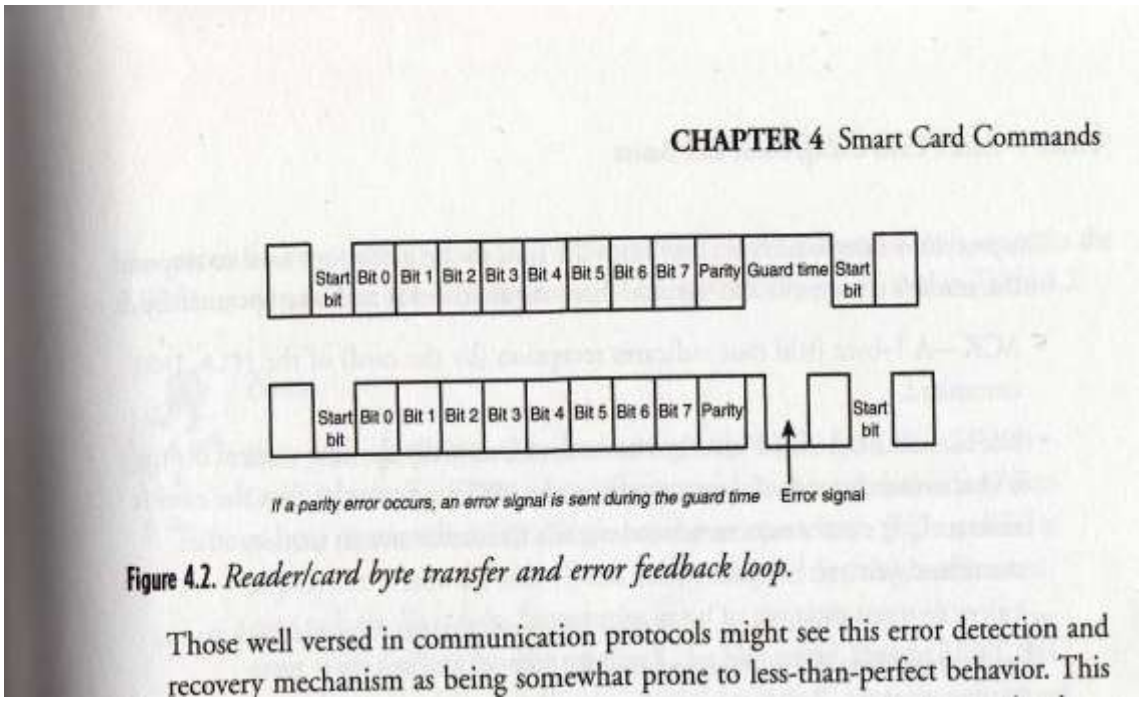


Figura tomada del libro: Smart Card developer's kit

La comunicación entre el lector y la tarjeta es Half-Duplex, es decir uno envía y luego recibe, no pude hacer las dos cosas a la vez (Full-Dúplex), debido a esto, se manejan 2 estructuras diferentes de transmisión: el lector envía unos datos a la tarjeta (como comandos a ser ejecutados), y luego la tarjeta envía una información al lector (en forma de respuesta al comando enviado).

El encabezado de transmisión del protocolo T=0 incluye 5 campos:

- CLA – Un campo de 1 byte que establece una colección de instrucciones; este campo cambia dependiendo del tipo de tarjeta que se esté trabajando (GSM, Tarjeta Inteligente, etc.).
- INS – Un campo de 1 byte que identifica la instrucción a ser usada de la colección de instrucciones definida por el campo CLA.
- P1 – Un campo de 1 byte que especifica parámetros o direccionamiento especificados por los campos CLA INS

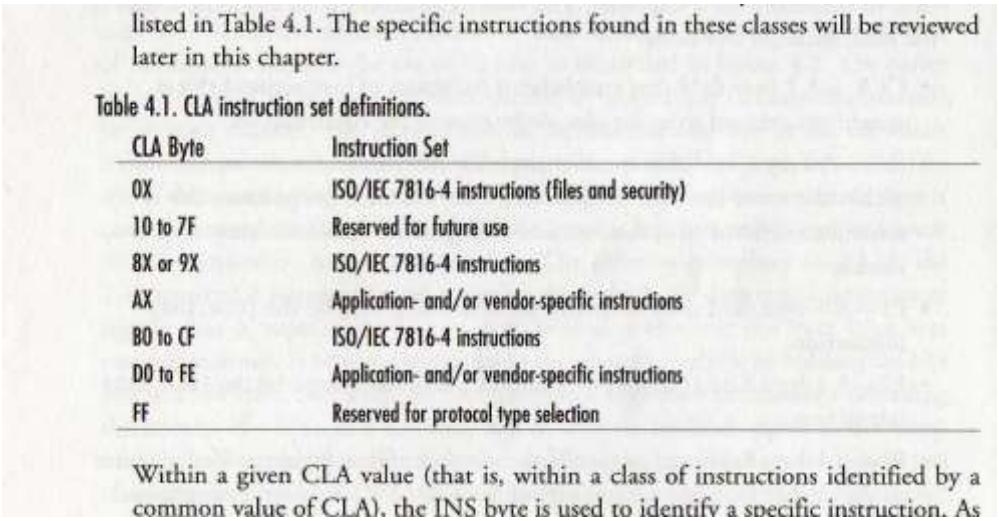
- P2 – Un campo de 1 byte que especifica parámetros o direccionamiento especificados por los campos CLA INS
- P3 – Un campo de 1 byte que especifica el número de datos a ser enviados o recibidos.

Como se había mencionado anteriormente, existe 1 estructura de datos para la transmisión y otra diferente para la recepción. Los campos de datos para la trama receptora constan de 3 campos obligatorios y 1 campo opcional.

- ACK – Un capo de 1 byte que indica el campo CLA INS al que se responde.
- NULL – Un campo de 1 byte que le indica al lector que la tarjeta está trabajando en el comando y que no envié otro comando todavía.
- SW1 – Un campo de 1 byte, usado por la tarjeta para enviar el estado del comando de vuelta al lector, con respecto al comando enviado.
- SW2 – un campo de 1 byte (opcional) que puede ser incluido en la respuesta, dependiendo del comando enviado. Si es incluido, normalmente datos que deben ser pedidos por otro comando. Este campo, representaría el campo P3 del siguiente comando a enviar.

De acuerdo con el tipo de tarjeta se maneja un campo CLA diferente, por ejemplo la tecnología GSM, o las tarjetas SIM Cards que utiliza la telefonía celular hoy en día, que trabajan con el campo CLA identificado con el byte A0; las tarjetas inteligentes trabajan según la ISO 7816-4, y esta regla maneja diferentes campos CLA. En la Tabla 1, se pueden ver los diferentes valores que puede tomar el campo CLA.

Tabla No.1: Valores del campo CLA.



listed in Table 4.1. The specific instructions found in these classes will be reviewed later in this chapter.

Table 4.1. CLA instruction set definitions.

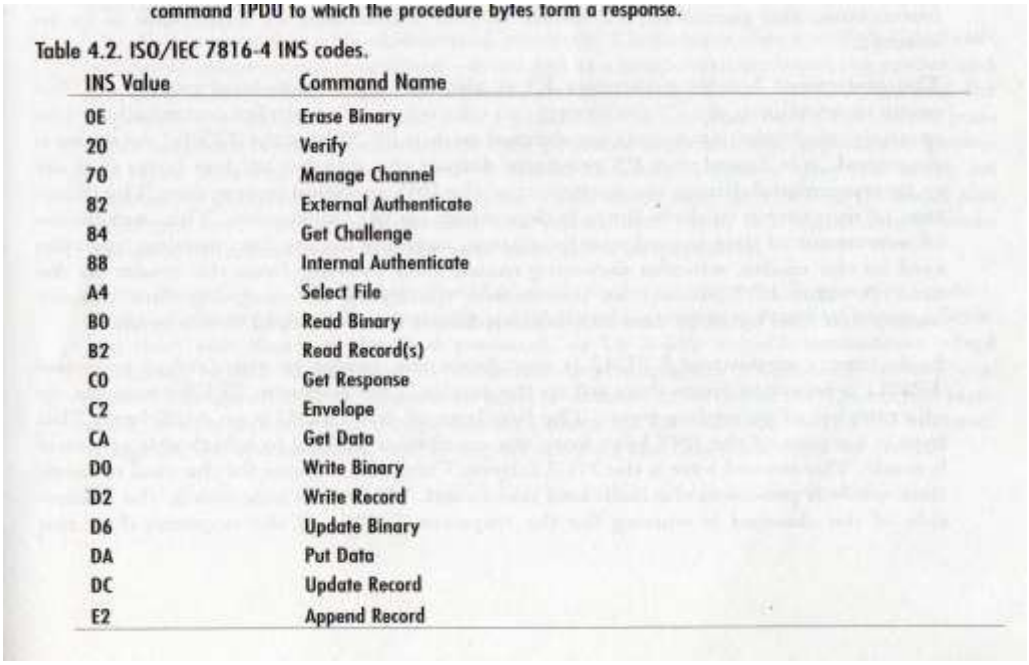
CLA Byte	Instruction Set
0X	ISO/IEC 7816-4 instructions (files and security)
10 to 7F	Reserved for future use
8X or 9X	ISO/IEC 7816-4 instructions
AX	Application- and/or vendor-specific instructions
B0 to CF	ISO/IEC 7816-4 instructions
D0 to FE	Application- and/or vendor-specific instructions
FF	Reserved for protocol type selection

Within a given CLA value (that is, within a class of instructions identified by a common value of CLA), the INS byte is used to identify a specific instruction. As

Tabla tomada del libro: Smart Card developer's kit

De acuerdo al campo CLA, se escoge una selección de instrucciones. En la Tabla 2, se muestran algunas de las instrucciones usadas por la ISO 7816-4.

Tabla No.2: Instrucciones Usadas por la ISO 7816-4.



command TPDU to which the procedure bytes form a response.

Table 4.2. ISO/IEC 7816-4 INS codes.

INS Value	Command Name
0E	Erase Binary
20	Verify
70	Manage Channel
82	External Authenticate
84	Get Challenge
88	Internal Authenticate
A4	Select File
B0	Read Binary
B2	Read Record(s)
C0	Get Response
C2	Envelope
CA	Get Data
D0	Write Binary
D2	Write Record
D6	Update Binary
DA	Put Data
DC	Update Record
E2	Append Record

Tabla tomada del libro: Smart Card developer's kit

5.1.1.2 Protocolo T=1 EL protocolo T=1 es un protocolo orientado a bloques. Esto significa que la trama que se envía a la vez, es una colección de información (o bloque de datos); dentro del bloque puede ser incluido un comando APDU. El hecho de que la trama sea un bloque de información, este debe estar libre de errores, o puede que el protocolo se confunda, además el proceso de detección y corrección de errores es más complejo que el proceso hecho en el protocolo T=0.

La detección de errores en el protocolo T=1, se hace mediante el LRC (Carácter de Redundancia Longitudinal), que es un poco más complejo que el checheo del bit de paridad; o el CRC (Carácter de Redundancia Cíclica), que garantiza la detección de errores de cada bit en el bloque transmitido. Este protocolo utiliza 3 tipos de bloques diferentes:

- Bloque de información – Este bloque es usado para compartir información entre el la tarjeta y el terminal.
- Bloque de Receive-Ready – Este bloque es usado para compartir acuerdos positivos o negativos de un punto a otro. Un comentario positivo significa que el bloque se recibió correctamente, mientras que un comentario negativo indica que un error fue detectado en el bloque recibido (mediante el LRC o CRC).
- Bloque Supervisor – Este bloque es usado para compartir información de control entre la tarjeta y el lector.

Cada bloque contiene 3 campos:

- Campo Prologo – Un campo obligatorio que tiene un tamaño de 3 bytes, e incluye:
  - NAD – Dirección del Nodo
  - PCB – Byte de control del protocolo
  - LEN – Tamaño
- Campo Información – Un campo opcional en el bloque que puede contener hasta 254 bytes.

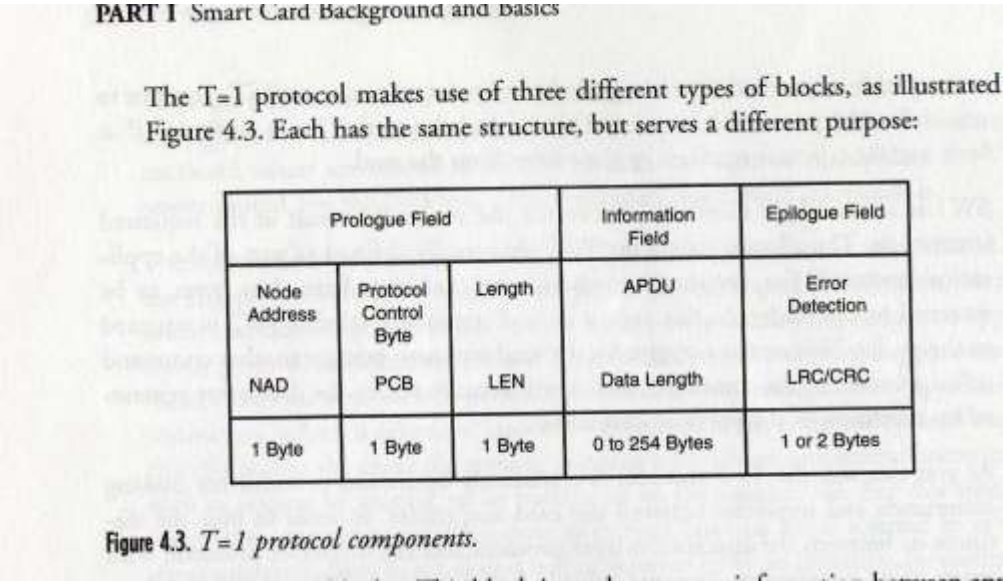
- Campo Epilogo – Un campo obligatorio en el bloque que es de 1 o 2 bytes en tamaño.

El Elemento NAD es utilizado para identificar la dirección de la fuente del bloque y el destino del mismo. Esto facilita la comunicación cuando se usan múltiples canales lógicos para la comunicación entre la tarjeta y el lector. Cuando este elemento es usado, este se compone de 2 sub-campos:

- SAD – Dirección de origen
- DAD – Dirección de destino

En la Tabla 3 se puede observar cómo están acoplados estos campos en el bloque enviado.

Tabla No.3: Componentes del Protocolo T=1



PART I Smart Card Background and Basics

The T=1 protocol makes use of three different types of blocks, as illustrated Figure 4.3. Each has the same structure, but serves a different purpose:

Prologue Field			Information Field	Epilogue Field
Node Address	Protocol Control Byte	Length	APDU	Error Detection
NAD	PCB	LEN	Data Length	LRC/CRC
1 Byte	1 Byte	1 Byte	0 to 254 Bytes	1 or 2 Bytes

Figure 4.3. *T=1 protocol components.*

Tabla tomada del libro: Smart Card developer's kit

Aparte de los protocolos, las instrucciones dadas por el usuario sobre qué se debe hacer con la tarjeta, es decir lo que el usuario le dice a la tarjeta que hacer, se hace por medio de comandos APDU, estos comandos, se trabajan en formatos de datos Hexadecimal. Estos comandos tienen un cierto orden que se establece mediante la ISO y se puede ver en las Figuras 25 y 26.

Figura No.25: Estructura del Comando APDU

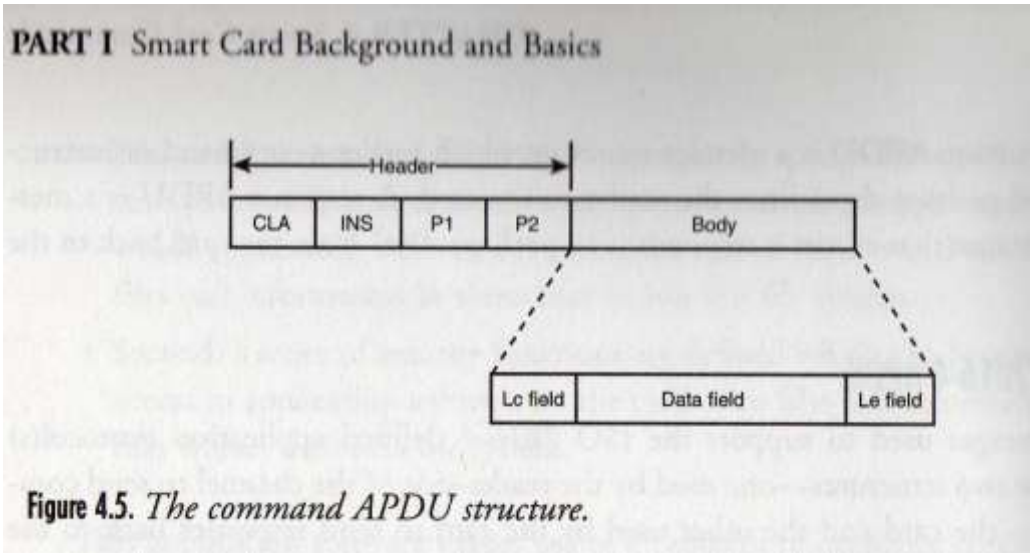


Figura tomada del libro: Smart Card developer's kit

Figura No.26: Estructura de respuesta del comando APDU

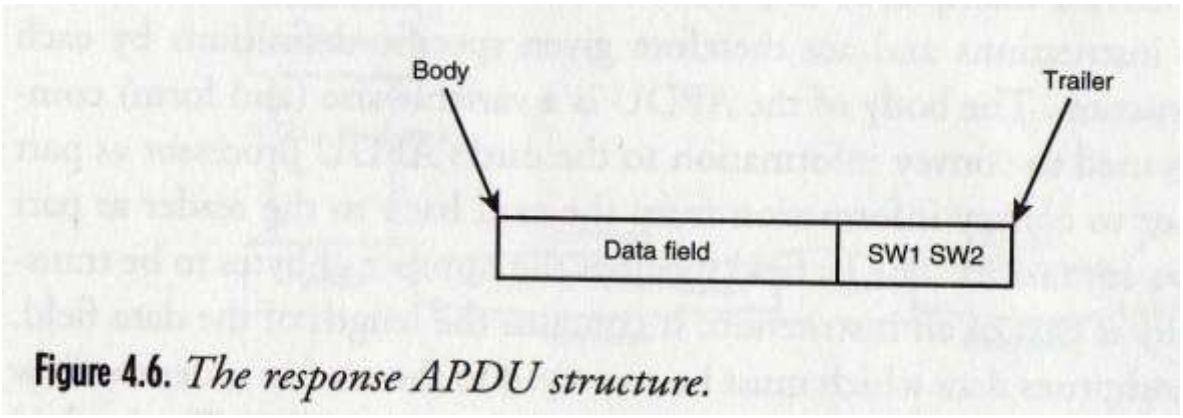


Figura tomada del libro: Smart Card developer's kit

5.1.1.3 Comandos APDU Como se ve en las figuras 25 y 26, hay dos tipos de formas de comandos. La forma de comandos mostrada en la figura 25, son los comandos del usuario, los que dan la orden a la tarjeta de que hacer; este formato se llama Comando APDU de Transmisión (T-APDU). El formato descrito en la figura 26, es la respuesta que la tarjeta le envía al terminal y le muestra al usuario si el comando fue ejecutado con éxito, si hay algún error, le

falta algo o no es compatible con el tipo de tarjeta insertada en el lector; estos comandos se llaman Comandos APDU de Respuesta (R-APDU).

Ya se conocen los campos CLA, INS, P1, P2, y P3, ahora se hablara del cuerpo del comando APDU, el cual contiene los Campos LC, DATA, y LE. Los campos LC y LE son el mismo campo P3, el P3 reemplaza al LC cuando el lector le dice a la tarjeta el tamaño campo DATA a enviar; el P3 reemplaza al campo LE cuando se le pide una respuesta a la tarjeta y se dice que tantos datos son. Depende de la instrucción cuando el P3 reemplaza al LC o LE, debido a esto, el cuerpo del comando APDU puede tener 4 diferentes formas:

- Ningún dato es enviado a la tarjeta, ni recibido de la tarjeta, entonces el comando APDU incluye solamente el encabezado. Esto es referido como el caso 1.
- Ningún dato es enviado a la tarjeta pero si se recibe información de esta, entonces el cuerpo del comando APDU incluye solamente el campo LE. Esto es referido como el caso 2.
- Datos son enviados a la tarjeta, pero ningún dato se recibe de esta, entonces el cuerpo del comando APDU incluye campo LC y el campo DATA. Esto es referido como el caso 3.
- Datos son enviados a la tarjeta y datos son recibidos de esta, entonces el cuerpo del comando APDU incluye el campo LC, DATA, y LE. Esto es referido como el caso 4.

El comando de respuesta APDU, tiene una estructura más simple que el comando de transmisión. Dependiendo del caso del comando APDU enviado a la tarjeta, se enviara un comando de respuesta específica para este. Es decir cuando el comando espere una respuesta con datos, el campo DATA de la respuesta no irá vacía sino con los datos que se están pidiendo. El APDU de respuesta incluye una cola, que contiene los datos SW1, y SW2 mencionados anteriormente. Cuando se pida información por el comando (ya sea el caso 3 o 4), el campo SW2 contendrá el tamaño del campo DATA de la respuesta. El campo SW1, devuelve el estado de la ejecución del comando enviado. En otras

palabras muestra si el comando se ejecuto, no se ejecuto, no es compatible con el tipo de tarjeta o no esta completo. Estos resultados se identifican con respecto a una serie de códigos que dicen el estado. Se pueden observar en la Figura 27 [1].

Figura No.27: códigos de retorno de la ISO 7816-4

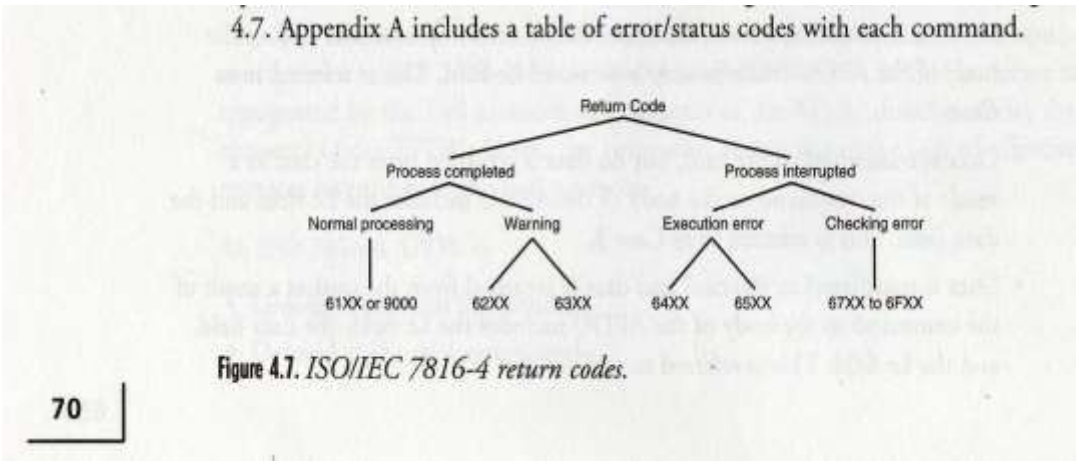


Figura tomada del libro: Smart Card developer's kit

- **Tipos de Comandos APDU (envío):**

Tabla No.4: Comandos APDU Envío

Use	Cla	Ins	Command
+	00	0E	ERASE BINARY
+	00	20	VERIFY
+	00	70	MANAGE CHANNEL
+	00	82	EXTERNAL AUTHENTICATE
+	00	84	GET CHALLENGE
+	00	A4	SELECT
+	00	B0	READ BINARY
+	00	B2	READ RECORD
+	00	C0	GET RESPONSE
+	00	C2	ENVELOPE
+	00	CA	GET DATA
+	00	D0	WRITE BINARY
+	00	D2	WRITE RECORD
+	00	D6	UPDATE BINARY
+	00	DA	PUT DATA
+	00	DC	UPDATE RECORD
+	00	E2	APPEND RECORD

Tabla tomada del Programa Smart Card ToolSet PRO V3.4

- **Tipos de Comandos APDU (respuesta):**

Tabla No.5: Comandos APDU Respuesta 1

Use	SW1	SW2	Color	Verbose
+	90	00	DFFFDF	Ok. Normal processing
+	61	xx	DFFFDF	Ok. Normal processing. Response bytes still available
+	62	xx	FFD9FF	State of non-volatile memory unchanged
+	62	00	FFD9FF	No information given
+	62	81	FFD9FF	Part of returned data may be corrupted
+	62	82	FFD9FF	End of file/record reached before reading Le bytes
+	62	83	FFD9FF	Selected file invalidated
+	62	84	FFD9FF	FCI not formatted according of 5.1.5 (ISO-7816-4)
+	63	xx	FFD9FF	State of non-volatile memory changed.
+	63	00	FFD9FF	No information given
+	63	81	FFD9FF	File filled up by the last write
+	64	xx	CACAFF	State of non-volatile memory unchanged.
+	65	xx	CACAFF	State of non-volatile memory changed.
+	65	00	CACAFF	No information given
+	65	81	CACAFF	Memory failure
+	67	00	CACAFF	Wrong length
+	68	xx	CACAFF	Functions in CLA not supported
+	68	00	CACAFF	No information given
+	68	81	CACAFF	Logical channel not supported
+	68	82	CACAFF	Secure messaging not supported

Tabla tomada del Programa Smart Card ToolSet PRO V3.4

Tabla No.6: Comandos APDU Respuesta 2

Use	SW1	SW2	Color	Verbose
+	69	xx	CACAFF	Command not allowed
+	69	00	CACAFF	No information given
+	69	81	CACAFF	Command incompatible with file structure
+	69	82	CACAFF	Security status not satisfied
+	69	83	CACAFF	Authentication method blocked
+	69	84	CACAFF	Referenced data invalidated
+	69	85	CACAFF	Conditions of use not satisfied
+	69	86	CACAFF	Command not allowed (no current EF)
+	69	87	CACAFF	Expected SM data objects missing
+	69	88	CACAFF	SM data objects incorrect
+	6A	xx	CACAFF	Wrong parameter(s) P1-P2
+	6A	00	CACAFF	No information given
+	6A	80	CACAFF	Incorrect parameters in the data field
+	6A	81	CACAFF	Function not supported
+	6A	82	CACAFF	File not found
+	6A	83	CACAFF	Record not found
+	6A	84	CACAFF	Not enough memory space in the file
+	6A	85	CACAFF	Lc inconsistent with TLV structure
+	6A	86	CACAFF	Incorrect parameters P1-P2
+	6A	87	CACAFF	Lc inconsistent with P1-P2
+	6A	88	CACAFF	Referenced data not found
+	6B	xx	CACAFF	Wrong parameter(s) P1-P2
+	6C	xx	CACAFF	Wrong length Le
+	6D	00	CACAFF	Instruction code not supported or invalid
+	6E	00	CACAFF	Class not supported
+	6F	00	CACAFF	No precise diagnosis

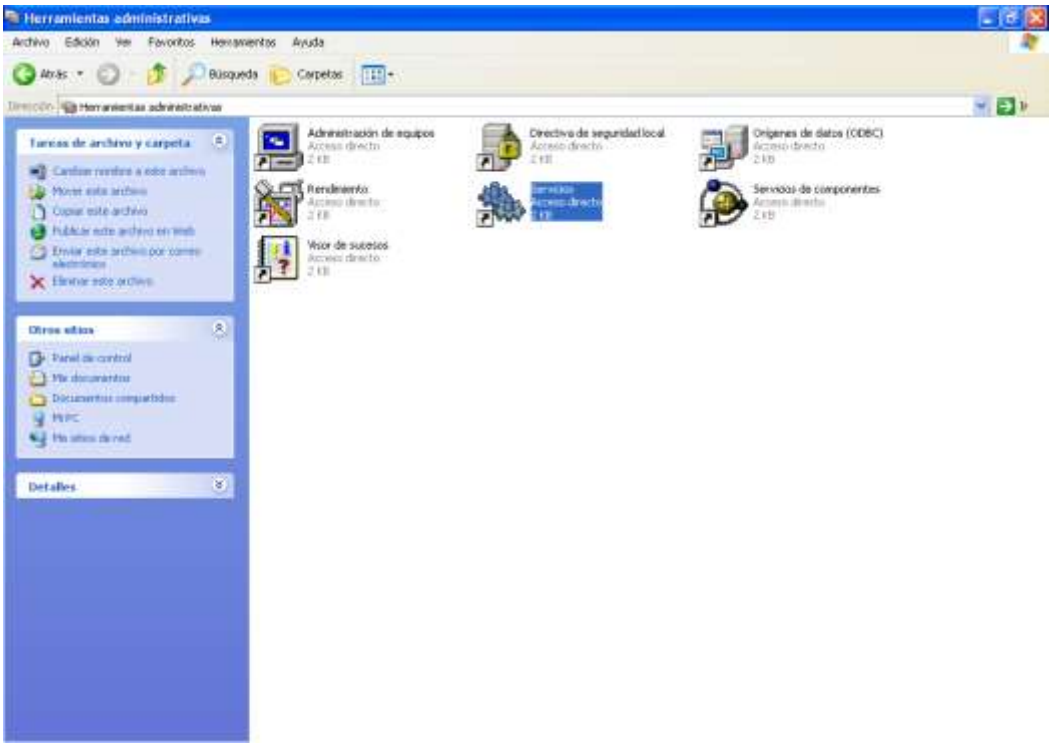
Tabla tomada del Programa Smart Card ToolSet PRO V3.4

5.1.2 Creacion y Montaje de la Base de Datos (ORACLE) Para la implementacion del prototipo es necesario la creación de una Base de Datos que contenga informacion referente a los usuarios que interactuan con el lector para que al momento de usar el dispositivo la informacion guardada en la tarjeta pueda ser comparada con la contenida en la Base de Datos y asi aceptar o negar el ingreso al usuario, pero para el montaje y la creacion de la base de datos se necesitan seguir los siguientes pasos:

1. Instalar Oracle en el PC, usando la version Express Edition 10g.

2. Despues de terminada la instalacion del programa, se pasa a modificar los servicios del PC para que cuando se desea trabajar con la Base de Datos se inician los servicios de Oracle sin conexión a internet para que este programa seleccione la direccion del localhost que seria: 127.0.0.1, esto se hace para que la Base de Datos se pueda ejecutar.

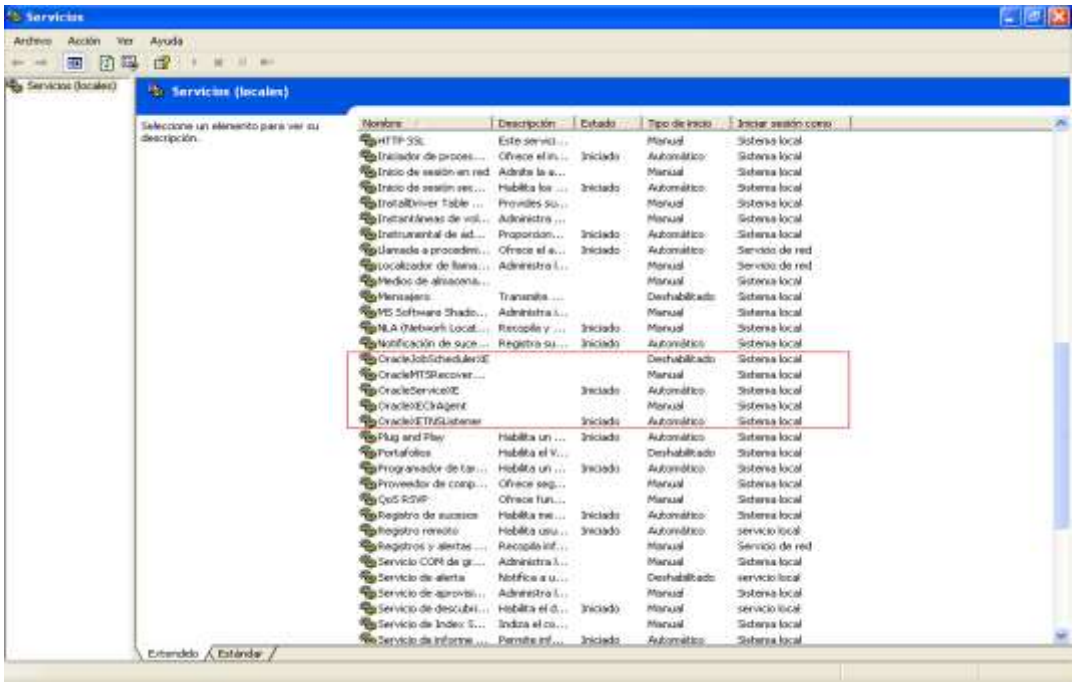
Figura No.28: Creación y montaje de la Base de Datos 1



Fuente: Diseño Grupo Investigador

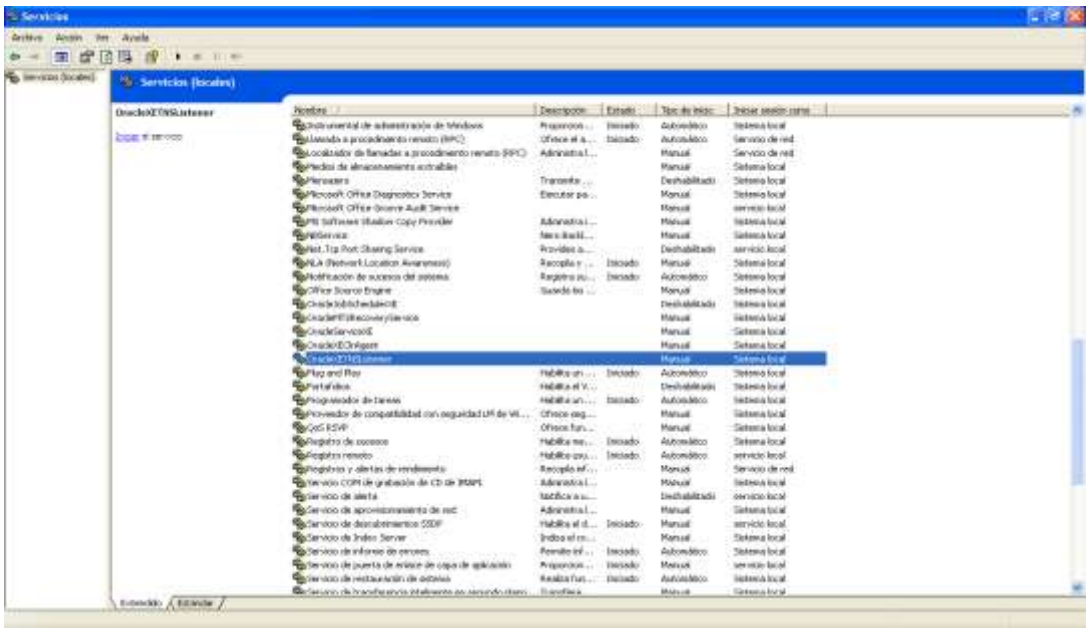
Una vez dentro se buscan los servicios de Oracle:

Figura No.29: Creación y montaje de la Base de Datos 2.



Fuente: Diseño Grupo Investigador

Figura No.30: Creación y montaje de la Base de Datos 3.



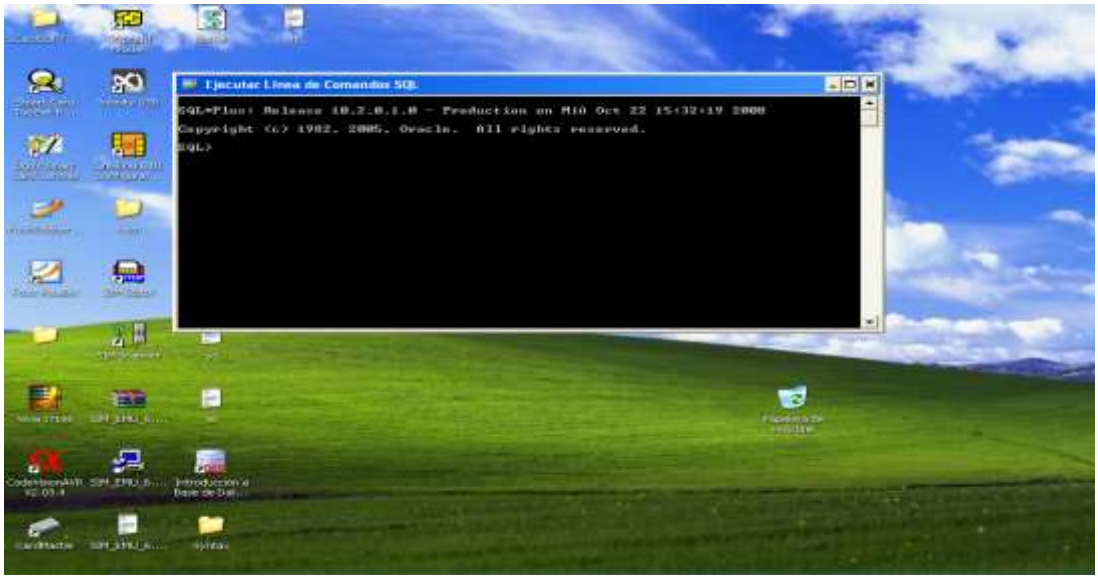
Fuente: Diseño Grupo Investigador

3. Al terminar de colocar los servicios de Oracle manuales, se procede a ejecutar (Linea de Comandos SQL) para crear los espacios de tabla (tablespaces).

Figura No.31: Creación y montaje de la Base de Datos 4

Fuente: Diseño Grupo Investigador

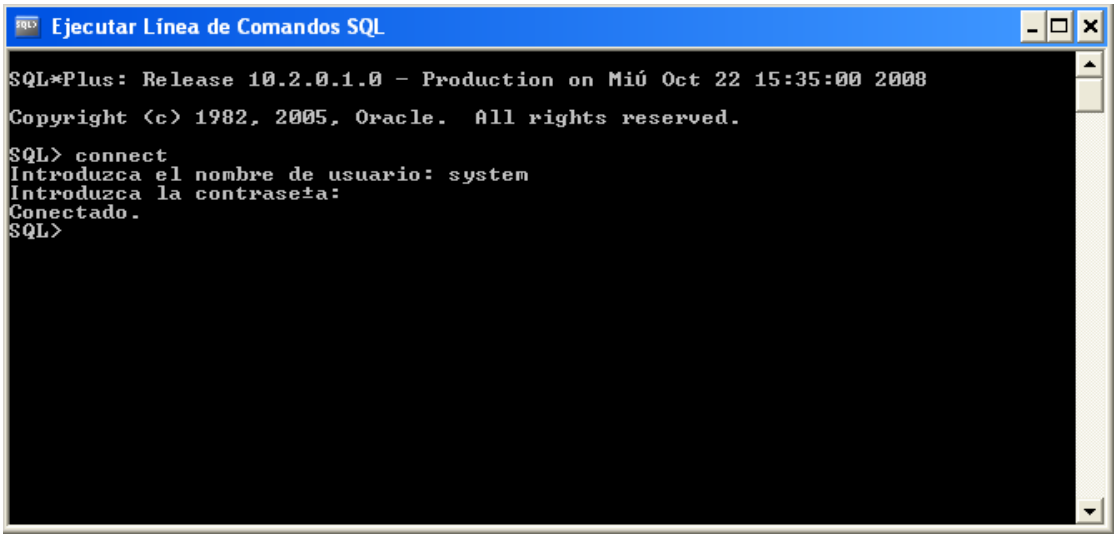
Figura No.32: Creación y montaje de la Base de Datos 5.



Fuente: Diseño Grupo Investigador

4. Una vez abierta la linea de comandos SQL se procede a escribir las siguientes sentencias (las lineas de usuario y contraseña se crean al momento de instalar el oracle):
   - Connect
   - Usuario: system
   - Contraseña: root

Figura No.33: Creación y montaje de la Base de Datos 6.



Fuente: Diseño Grupo Investigador

5. Despues de iniciada la conexión se copian los siguientes comandos en la linea de SQL para crear los espacios de tabla de datos, de indices, el usuario y su asigancion a ese espacio de tablas y los permisos asignados al usuario:

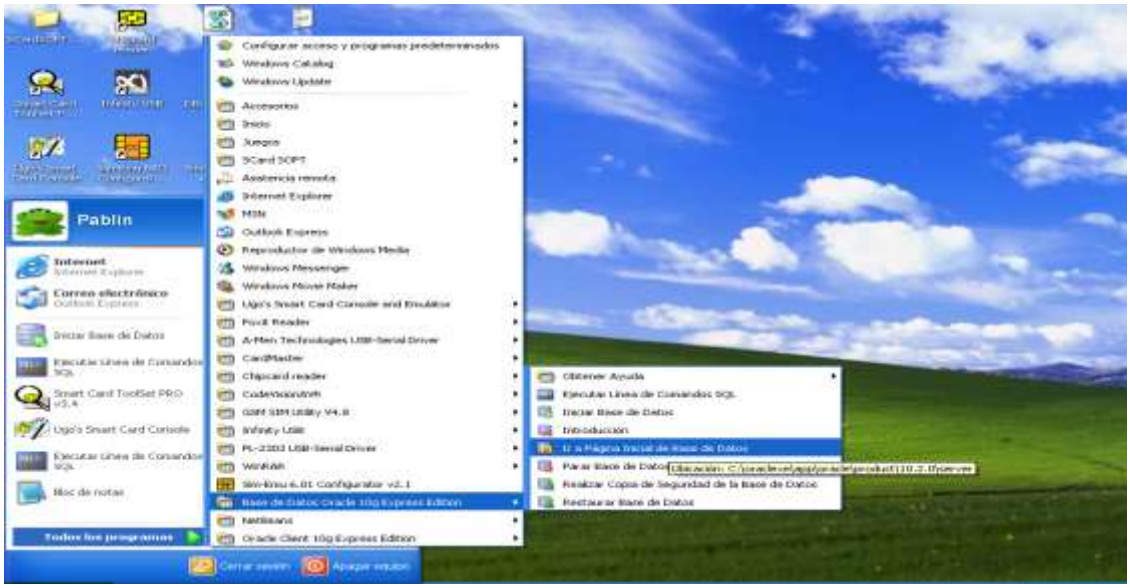
Figura No.34: Creación y montaje de la Base de Datos 7.

```
CREATE TABLESPACE D_LECTOR
     LOGGING
     DATAFILE 'C:\oraclexe\oradata\XE\D_LECTOR.dbf' SIZE 10M
     AUTOEXTEND
     ON NEXT 2M MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL
     SEGMENT SPACE MANAGEMENT  AUTO
;

CREATE TABLESPACE I_LECTOR
     LOGGING
     DATAFILE 'C:\oraclexe\oradata\XE\I_LECTOR.dbf' SIZE 3M
     AUTOEXTEND
     ON NEXT 1M MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL
     SEGMENT SPACE MANAGEMENT  AUTO
;

CREATE USER LECTOR
 IDENTIFIED BY LECTOR
 DEFAULT TABLESPACE D_LECTOR
 TEMPORARY TABLESPACE temp
;

GRANT CONNECT, RESOURCE, DBA TO LECTOR
;
```

Fuente: Diseño Grupo Investigador

6. Luego de ejecutar los anteriores comandos se procede a entrar a la pagina de acceso a la Base de Datos:

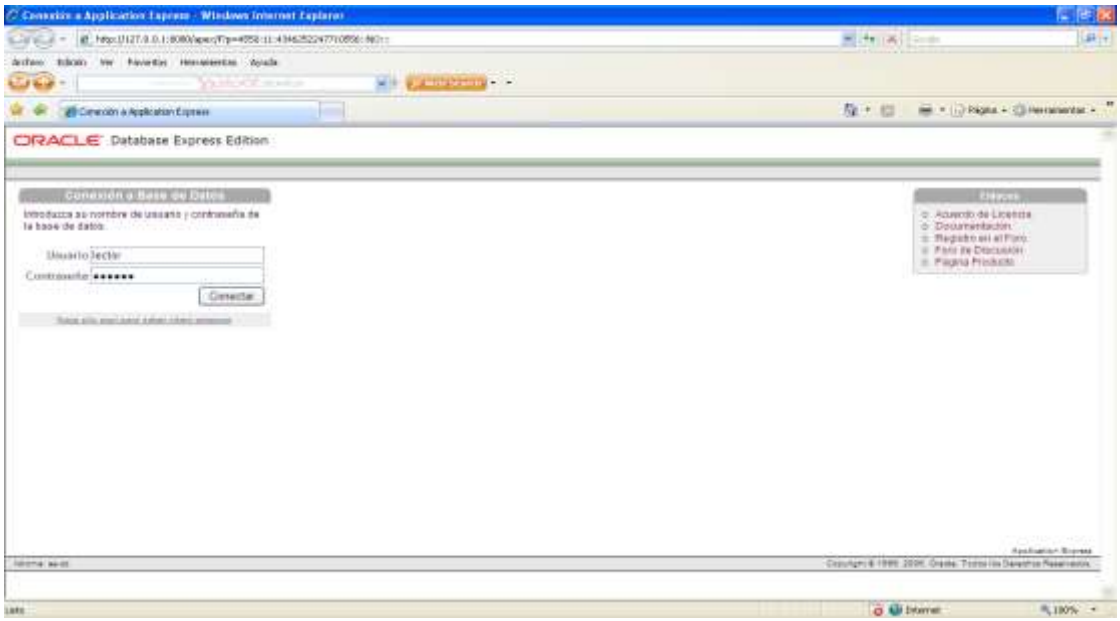
Figura No.35: Creación y montaje de la Base de Datos 8.



Fuente: Diseño Grupo Investigador

7. Una vez estando en la pagina de entrada se escriben el usuario y la contraseña creados en los comandos del numeral 5.

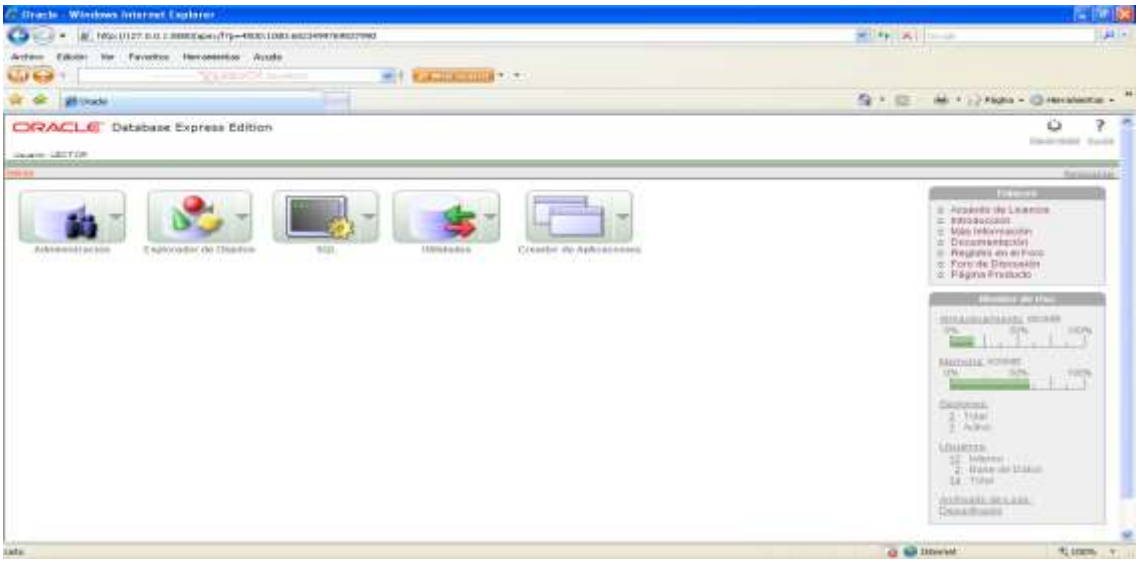
Figura No.36: Creación y montaje de la Base de Datos 9.



Fuente: Diseño Grupo Investigador

8. Despues de accesar con usuario y contraseña aparecera la siguiente pagina:

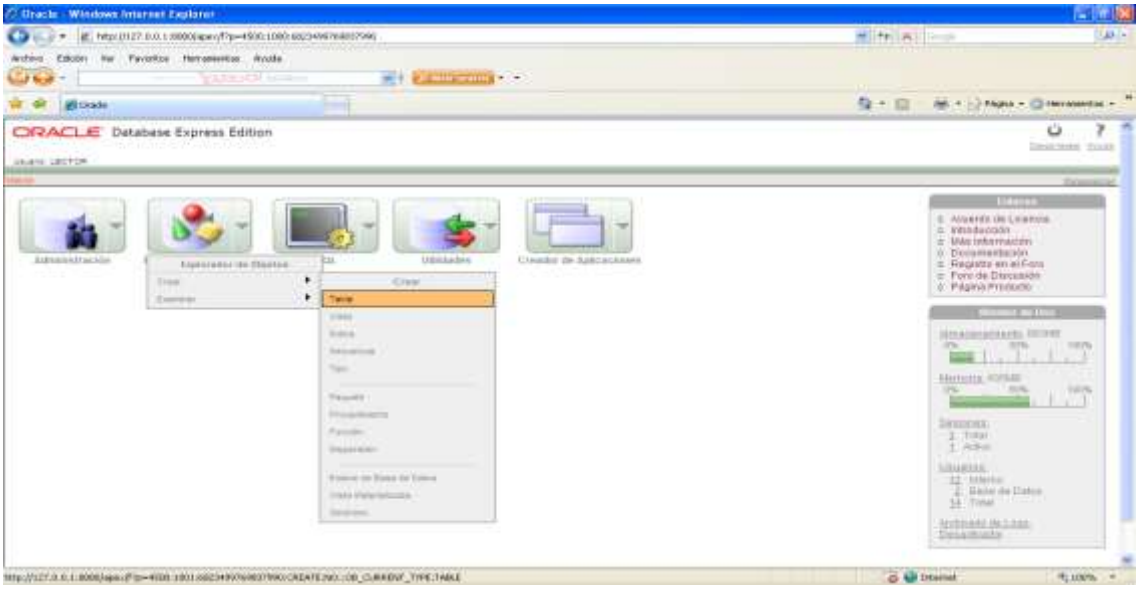
Figura No.37: Creación y montaje de la Base de Datos 10.



Fuente: Diseño Grupo Investigador

9. Para cear la tabla de datos se entra en:

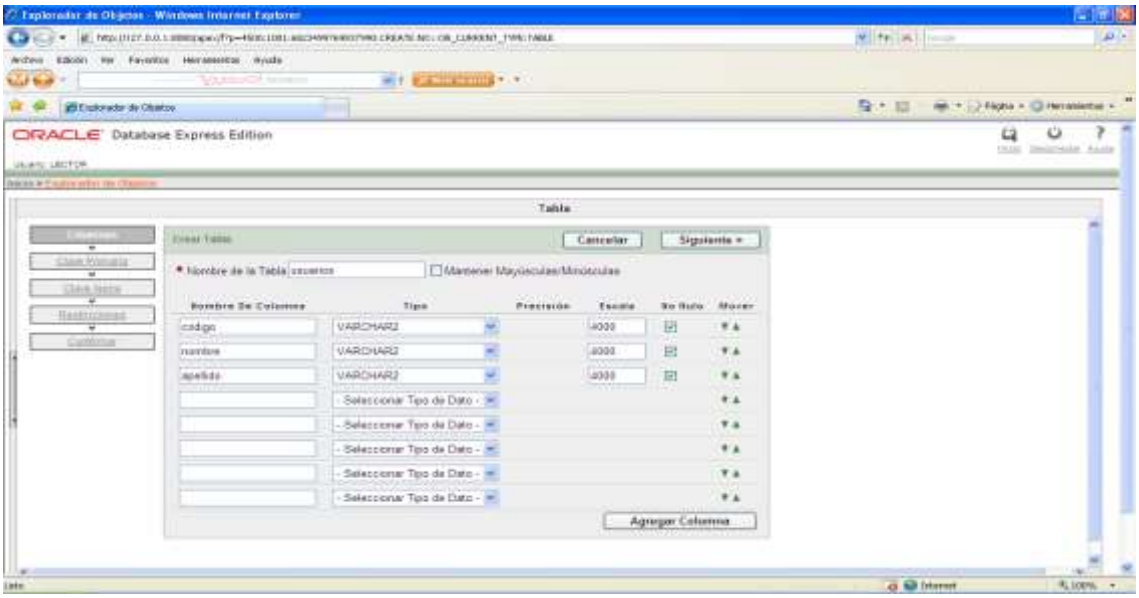
Figura No.38: Creación y montaje de la Base de Datos 11.



Fuente: Diseño Grupo Investigador

10. Al hacer click en crear tabla aparecera la siguiente pantalla donde se escribe el nombre de la tabla y sus campos, como se puede observar en la siguiente imagen:

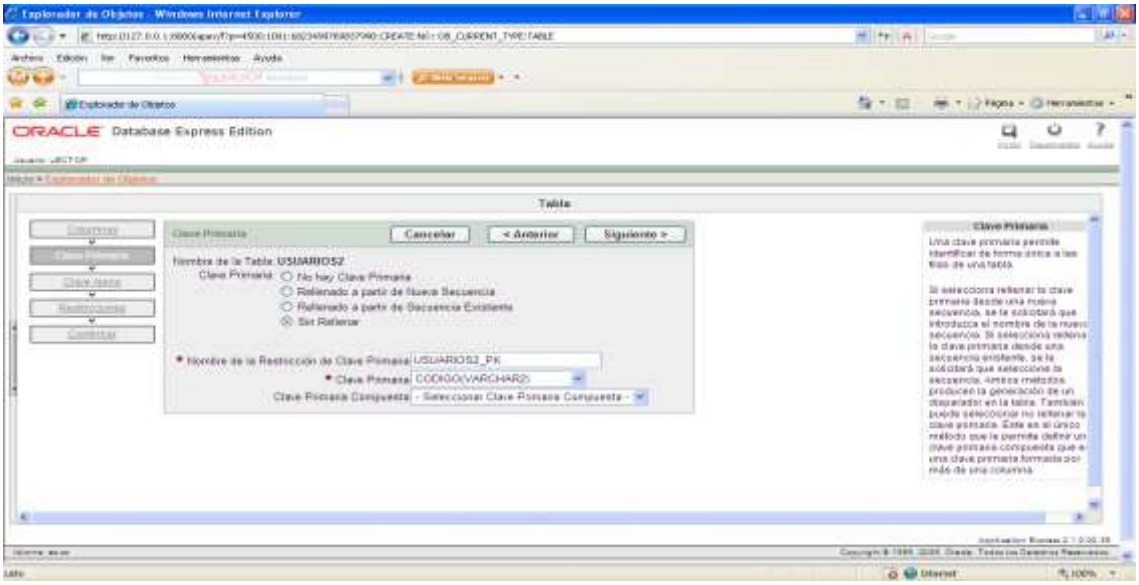
Figura No.39: Creación y montaje de la Base de Datos 12.



Fuente: Diseño Grupo Investigador

11. Al dar click en siguiente aparece la pantalla para crear la llave primaria de la tabla:

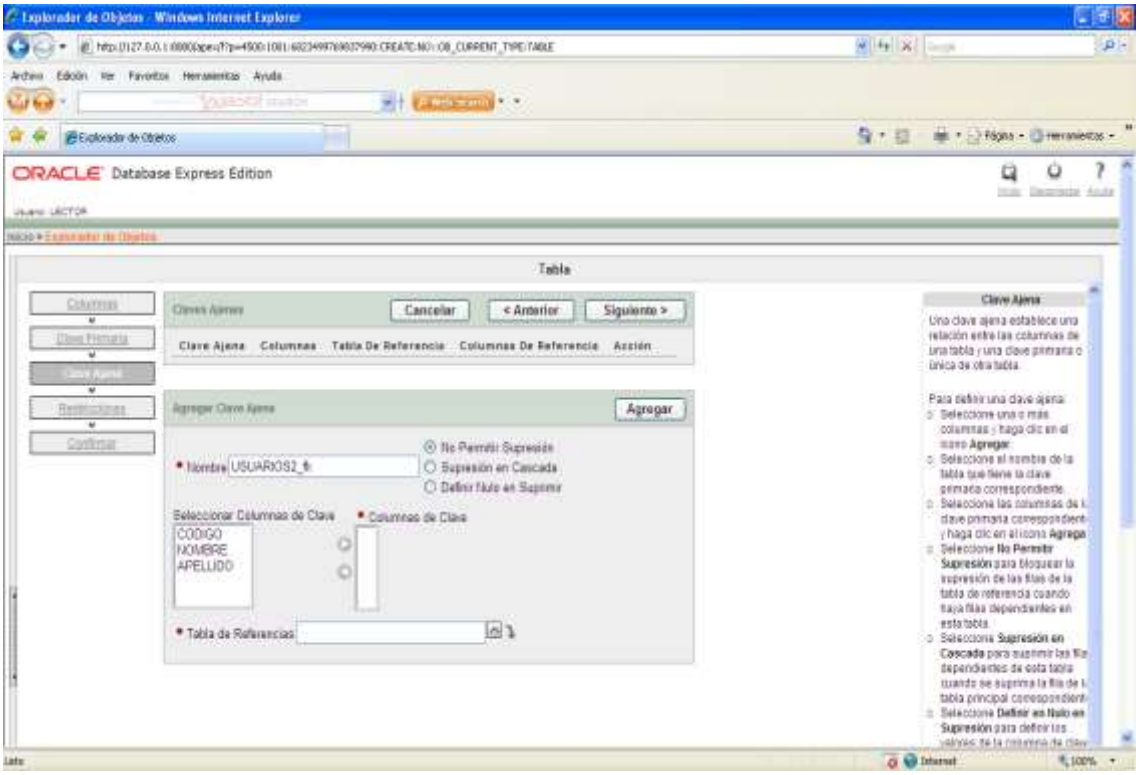
Figura No.40: Creación y montaje de la Base de Datos 13.



Fuente: Diseño Grupo Investigador

12. Despues de creada la llave primaria se entra a clave ajena donde no se modifica ningun campo y se da click en siguiente:

Figura No.41: Creación y montaje de la Base de Datos 14.

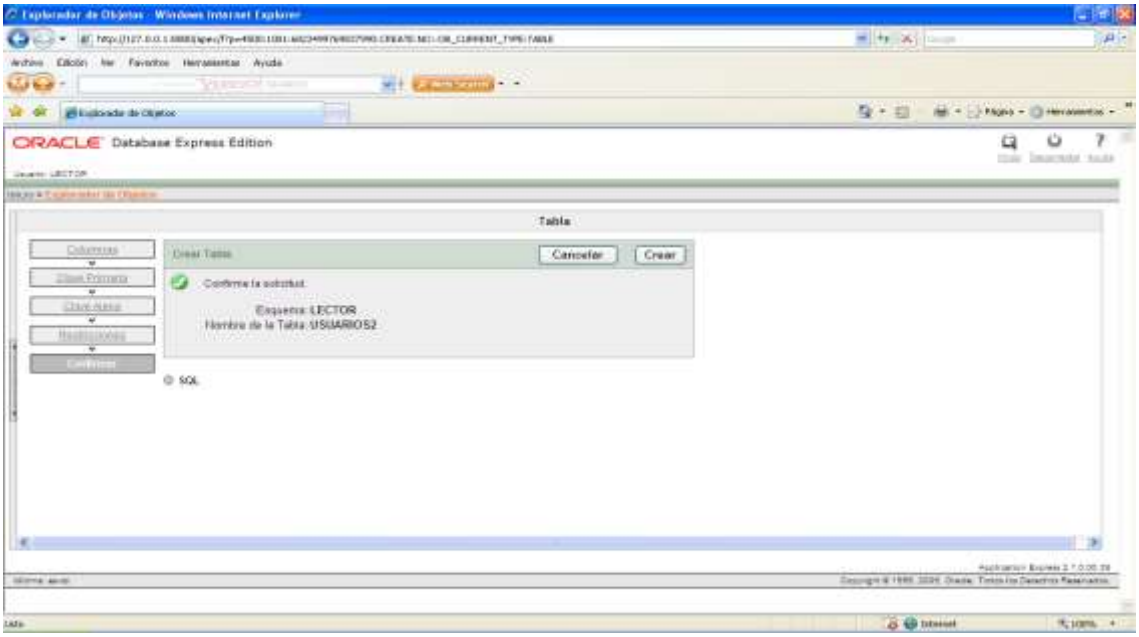


Fuente: Diseño Grupo Investigador

13. Aparecera la pantalla de restricciones donde tampoco se modifica ningun itemy se da click en terminar:

14. Una hechos los anteriores pasos, se llega a la ultima pantalla de la creacion, donde se confirman los aspectos de la tabla y se da click en crear:

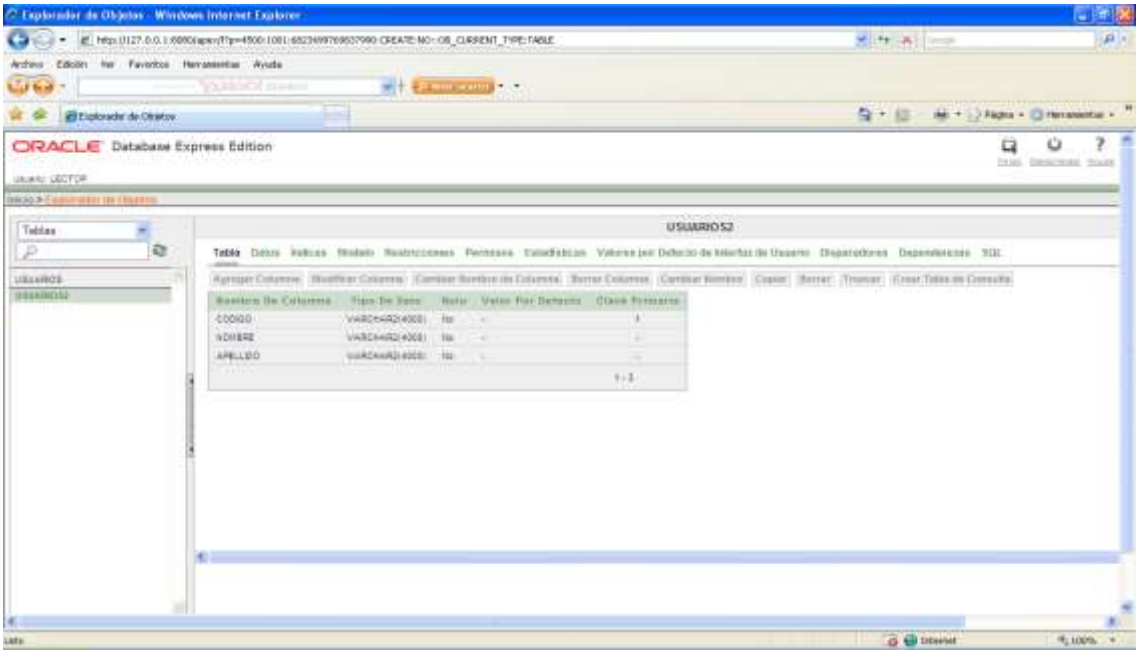
Figura No.42: Creación y montaje de la Base de Datos 15.



Fuente: Diseño Grupo Investigador

15. Este es el resultado de los pasos anteriores:

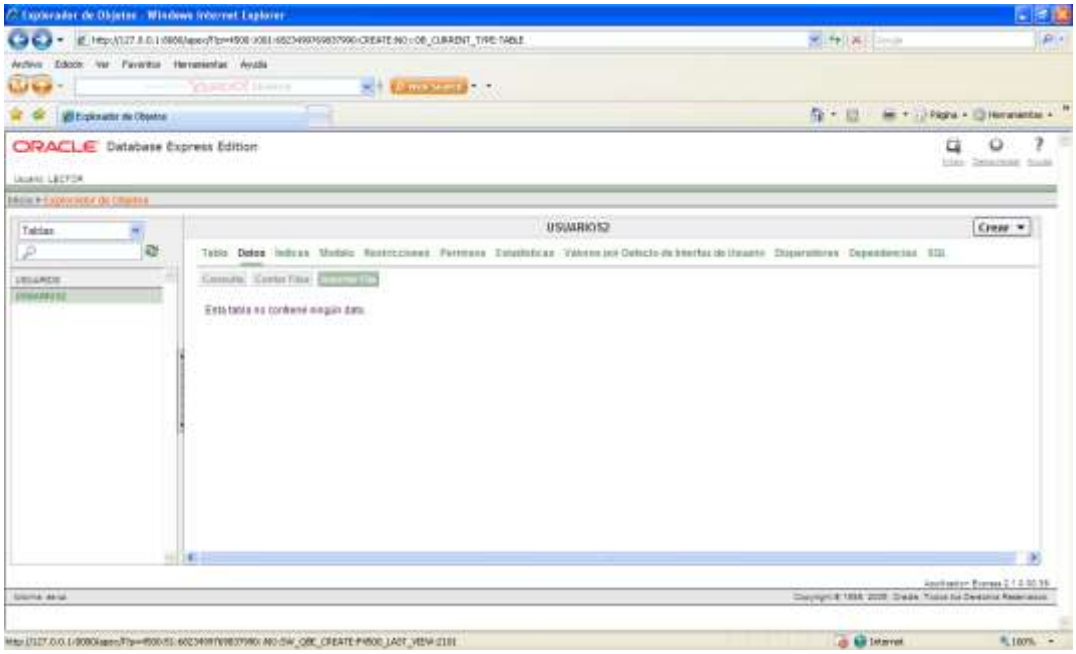
Figura No.43: Creación y montaje de la Base de Datos 16.



Fuente: Diseño Grupo Investigador

16. Ahora, para agregar los datos a la tabla se da click en la pestaña datos y luego en insertar fila:

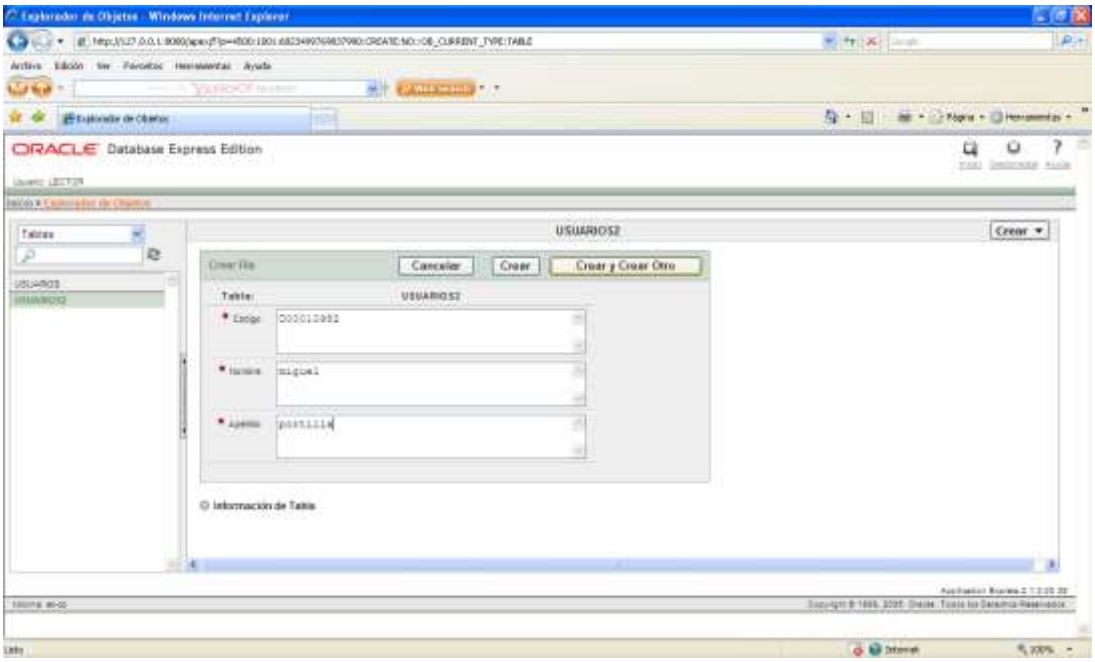
Figura No.44: Creación y montaje de la Base de Datos 17.



Fuente: Diseño Grupo Investigador

17. Una vez dentro de insertar fila se procede a llenar los campos de la tabla:

Figura No.45: Creación y montaje de la Base de Datos 18.



Fuente: Diseño Grupo Investigador

Estos son los pasos a seguir para el montaje y la creacion de la Base de Datos necesaria para el funcionamiento del dispositivo.

5.1.3 Diseño del Software El proceso de diseño seleccionado para la creación del software fue el Diagrama de Flujo de Datos (DFD), el cual utiliza una interacción en el sistema del tipo: entrada-proceso-salida. El funcionamiento de esta interacción se describe de la siguiente manera: existen dos tipos de objetos de datos (entrada y salida), los primeros son los que fluyen hacia el interior del software, una vez interactúan dentro de él, se transforman mediante elementos de procesamiento y se genera el segundo tipo de objetos de datos, los cuales fluyen hacia el exterior del software.

El DFD se representa en forma jerárquica, siempre buscando de lo general a lo particular, ya que el primer modelo de flujo de datos (llamado DFD de nivel 0 ó diagrama de contexto) representa el sistema como un todo; de este DFD de nivel 0 se generan diagramas de flujos de datos subsecuentes que refinan el

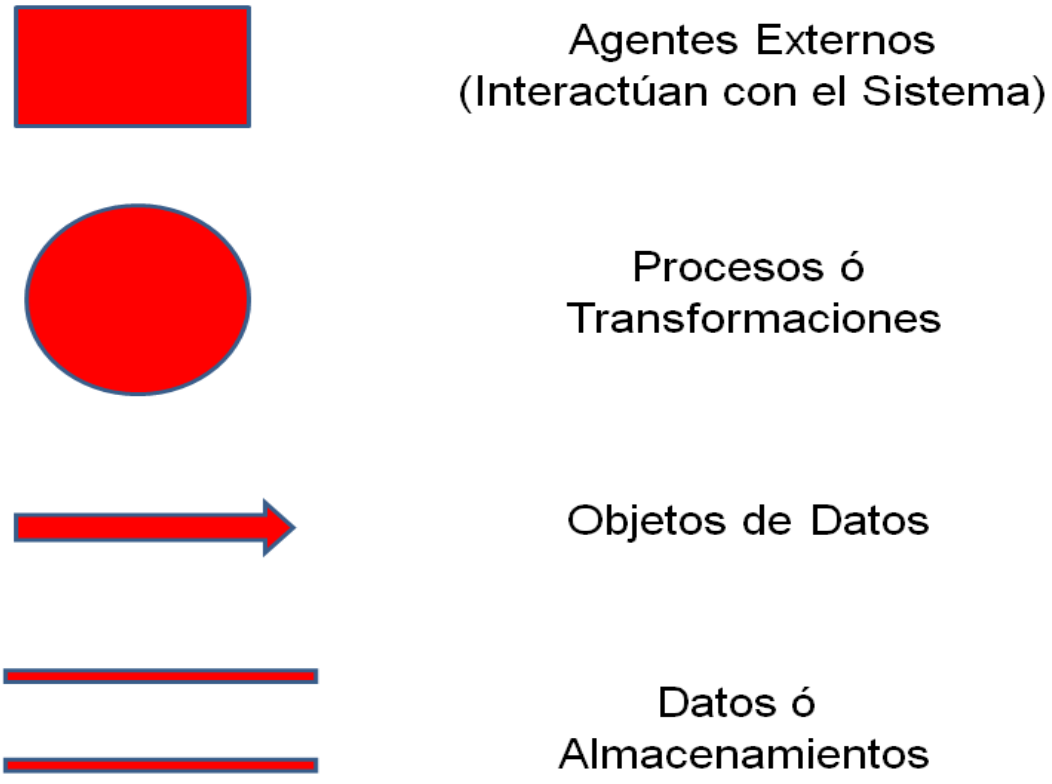
diagrama de contexto y ayudan a su entendimiento, ya que proporcionan detalles cada vez más específicos con sus niveles siguientes.

Los diferentes niveles que conforman un Diagrama de Flujo de Datos son:

- Diagrama de contexto ó Nivel 0.
- Diagrama de nivel superior ó Nivel 1.
- Diagrama de detalle, diagrama de expansión ó Nivel 2.

Los componentes usados en la elaboración de un DFD son los siguientes:

Figura No.46: Componentes de Diagramas de Flujo de Datos



Fuente: Diseño Grupo Investigador

Los Diagramas de Flujo de Datos correspondientes a cada software del proyecto, son los siguientes:

5.1.3.1 Diagramas de Flujos de Datos Software Usuario.
VER ANEXO 1

5.1.3.2 Diagramas de Flujos de Datos Software Administrador.
VER ANEXO 2

5.1.4 Diccionario de Datos El diccionario de datos es un aspecto de mucha importancia en todo trabajo investigativo que contenga Diagramas de Flujos de Datos, ya que nos permite identificar, organizar y guardar los diferentes componentes y detalles de un DFD, para esta investigación que contiene dos implementaciones software, se tienen los siguientes elementos:

5.1.4.1 Flujos de Datos En todo sistema existen flujos de datos, también llamados streams, estos datos fluyen dentro del sistema, siempre desde una entrada especifica que a su vez contiene una salida que reporta el resultado de la acción realizada, los flujos de datos elaborados para este sistema son:

- **Flujos de Datos Software Usuario**

VER ANEXO 3

- **Flujos de Datos Software Administrador**

VER ANEXO 4

5.1.4.2 Almacenes de Datos Para este sistema fue necesario la creación de ocho tablas, las cuales conforman la Base de Datos que simula a la que funciona en la Universidad Autónoma de Bucaramanga, estas tablas nos permiten ver las diferentes características de los usuarios del dispositivo, como por ejemplo su nombre, sus materias, código, horarios, etc.

Pero el sistema de lector solamente interactúa directamente con tres de estas tablas, ya que solo realiza consultas en las de usuario, docentes y salones, aunque para ayudar a su comprensión se expondrán todas las tablas:

- **Almacenes de Datos Software Usuario**

VER ANEXO 5

- **Almacenes de Datos Software Administrador**

VER ANEXO 6

5.1.4.3 Procesos Son los encargados de ejecutar diferentes operaciones dentro del sistema para que el funcionamiento de este se lleve a cabo, para nuestro sistema conformado por dos programas se tienen los siguientes procesos:

- **Procesos Software Usuario**

VER ANEXO 7

- **Procesos Software Administrador**

VER ANEXO 8

5.1.4.4 Agentes Externos Son los actores que interactúan de manera directa con el sistema e influyen en el funcionamiento de este, y a su vez pueden enviar o recibir información que comparten con el sistema, para este sistema de control de acceso se tienen los siguientes agentes externos:

- **Agentes Externos Software Usuario**

VER ANEXO 9

- **Agentes Externos Software Administrador**

VER ANEXO 10

5.1.5 Modelo Entidad – Relación Para el funcionamiento del sistema de Control de Acceso se cuenta con ocho tablas de almacenamiento de datos de los usuarios, las cuales se relacionan de manera simultánea para obtener cualquier dato que requiera el sistema y además se cuenta con otras dos tablas de almacenamiento de datos del sistema (LEC_ARCHIVOS y LEC_COMANDOS) que no hacen parte del diagrama Entidad-Relación.

Cabe resaltar que los nombres de todas las tablas poseen la sigla (LEC) en su inicio, esto se hace solamente como un identificador usado por el Grupo Investigador para relacionarlo con el Lector y no posee mayor importancia para el sistema.

Las tablas que conforman la base de datos del software de control de acceso son las siguientes:

Figura No.47: Tabla LEC_ALUMNOS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
CODIGO	VARCHAR2(20)	No	-	1
NOMBRES	VARCHAR2(50)	No	-	-
APELLIDOS	VARCHAR2(50)	No	-	-
TIPO_DOCUMENTO	VARCHAR2(2)	No	-	-
NRO_DOCUMENTO	VARCHAR2(20)	No	-	-
SEMESTRE	VARCHAR2(10)	No	-	-
				1 - 6

Fuente: Diseño Grupo Investigador

Tabla que contiene todos los datos referentes a las características de los Alumnos, como por ejemplo su ID, semestre, etc.

Figura No.48: Tabla LEC_ALUMNOS_MATERIAS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_ALUM_MATERIA	NUMBER	No	-	1
CODIGO	VARCHAR2(20)	No	-	-
ID_MATERIA_CARRERA	NUMBER	No	-	-
NOTA	NUMBER(3,2)	Yes	-	-
				1 - 4

Fuente: Diseño Grupo Investigador

Tabla que guarda las materias que tiene matriculadas cada alumno.

Figura No.49: Tabla LEC_ARCHIVOS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
TIPO	VARCHAR2(20)	No	-	1
HEXADECIMAL	VARCHAR2(20)	Yes	-	-
				1 - 2

Fuente: Diseño Grupo Investigador

Archivos referentes al lector que necesita el sistema para trabajar.

Figura No.50: Tabla LEC_COMANDOS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
COMANDO	VARCHAR2(20)	No	-	1
HEXADECIMAL	VARCHAR2(20)	No	-	-
				1 - 2

Fuente: Diseño Grupo Investigador

Datos que el sistema utiliza para convertir ATR del lector.

Figura No.51: Tabla LEC_DOCENTES

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
NRO_DOCUMENTO	VARCHAR2(20)	No	-	1
TIPO_DOCUMENTO	VARCHAR2(2)	No	-	-
NOMBRES	VARCHAR2(50)	No	-	-
APELLIDOS	VARCHAR2(50)	No	-	-
				1 - 4

Fuente: Diseño Grupo Investigador

Tabla que almacena las características de los docentes, por ejemplo su cedula.

Figura No.52: Tabla LEC_FACULTAD_CARRERAS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_CARRERA	NUMBER	No	-	1
ID_FACULTAD	NUMBER	No	-	-
NOMBRE_CARRERA	VARCHAR2(100)	No	-	-
				1 - 3

Fuente: Diseño Grupo Investigador

En esta tabla se guardan las carreras que pertenecen a cada facultad, como por ejemplo Ing. De Sistemas pertenece a la facultad de Ciencias Naturales e Ingeniería.

Figura No.53: Tabla LEC_FACULTADES

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_FACULTAD	NUMBER	No	-	1
NOMBRE_FACULTAD	VARCHAR2(50)	No	-	-
				1 - 2

Fuente: Diseño Grupo Investigador

Tabla que contiene todas las facultades que conforman la Universidad Autónoma de Bucaramanga, por ejemplo: Facultad de Ciencias de la Salud, Facultad de Ingenierías, etc.

Figura No.54: Tabla LEC_MATERIAS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_MATERIA	NUMBER	No	-	1
NOMBRE_MATERIA	VARCHAR2(100)	No	-	-
				1 - 2

Fuente: Diseño Grupo Investigador

Aquí se guardan todas las materias que conforman cada pensum de la Universidad, sin importar facultad o semestre.

Figura No.55: Tabla LEC_MATERIAS_CARRERAS

Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_MATERIA_CARRERA	NUMBER	No	-	1
SEMESTRE	VARCHAR2(20)	No	-	-
ID_MATERIA	NUMBER	No	-	-
ID_CARRERA	NUMBER	No	-	-
ID_SALON	NUMBER	No	-	-
GRUPO	VARCHAR2(20)	No	-	-
DIA	VARCHAR2(10)	No	-	-
HORA_INICIO	NUMBER	No	-	-
HORA_FINAL	NUMBER	No	-	-
NRO_DOCUMENTO	VARCHAR2(20)	No	-	-
				1 - 10

Fuente: Diseño Grupo Investigador

Esta tabla es la más importante de la Base de Datos, ya que en esta se relacionan todas las otras tablas y además contiene la información detallada de cada usuario que usa el dispositivo, por ejemplo el ID (estudiante), Cedula (docente), horas de la clase, salón, etc.

Figura No.56: Tabla LEC_SALONES

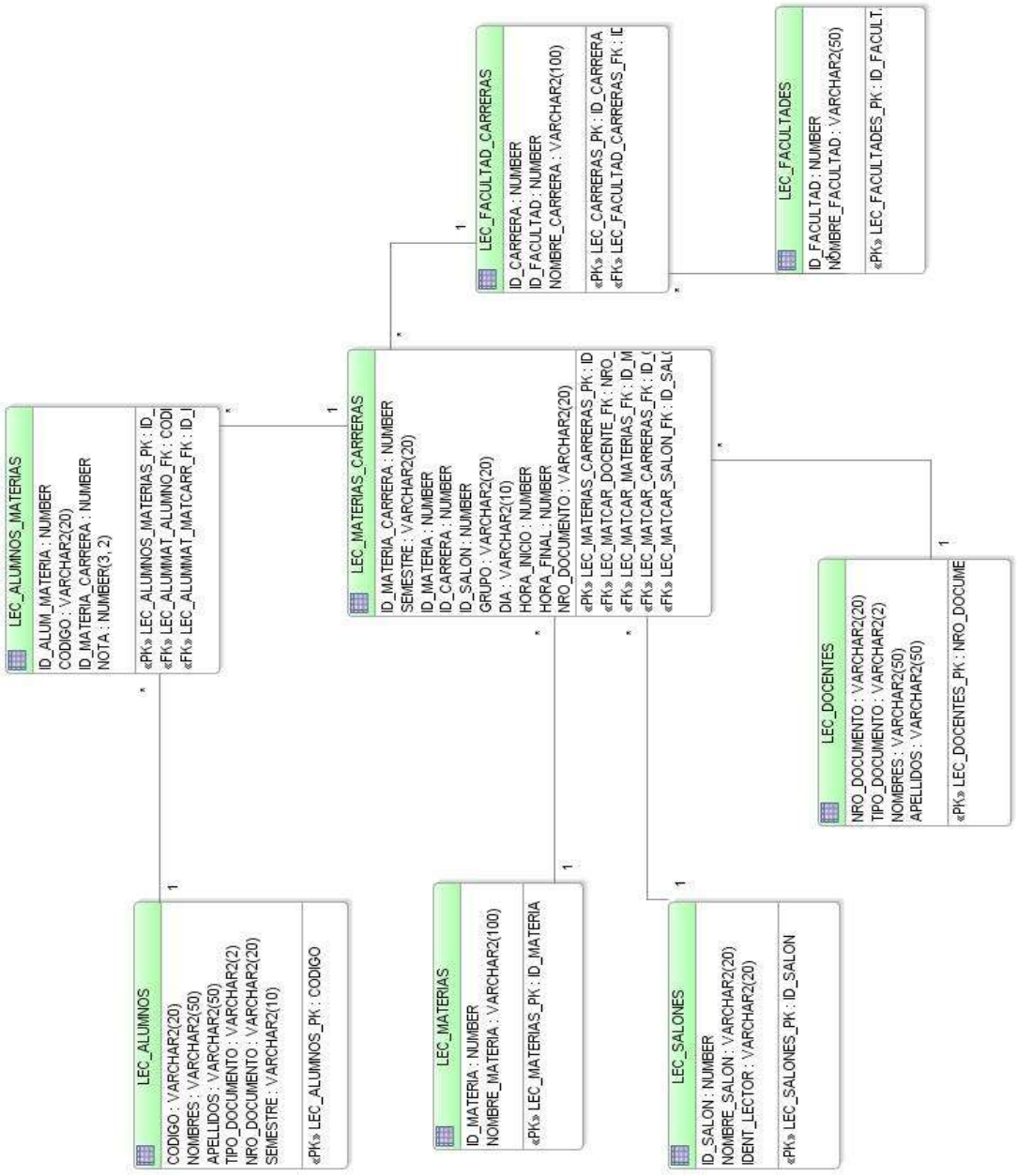
Nombre De Columna	Tipo De Dato	Nulo	Valor Por Defecto	Clave Primaria
ID_SALON	NUMBER	No	-	1
NOMBRE_SALON	VARCHAR2(20)	No	-	-
IDENT_LECTOR	VARCHAR2(20)	Yes	-	-
				1 - 3

Fuente: Diseño Grupo Investigador

Tabla que contiene la información de los salones y el identificador del lector que allí se esté utilizando.

Para presentar de una manera más especifica el sistema de tablas, se tienen dos tipos de conexión entre ellas, las cuales son: 1-1 (representada por el número 1), 1-muchos (representada por un asterisco):

Figura No.57: Diagrama Entidad Relación



Fuente: Diseño Grupo Investigador

Del anterior esquema se puede ver que las relaciones entre las tablas son expresamente de 1-muchos y la tabla principal es: LEC_MATERIAS_CARRERAS, ya que este almacén de datos relaciona las demás y entrega una información puntual del usuario que utiliza el dispositivo.

5.1.6 Descripcion del Software Para el desarrollo del proyecto, se cuenta con dos programas desarrollados en java usando la librería de java: javax.smartcardio. El primer software, es el referente al administrador, el cual es el que va a ser el encargado de grabar y eliminar la información de las tarjetas para poder tener acceso a las aulas, para hacer esto, se necesita que en algún momento, el código guardado en el chip de la tarjeta, este guardado en la base de datos a usar. Este software nos ayuda a controlar la comunicación, si la tarjeta está presente o no en el lector y mostrar al personal encargado como manejar el software y mostrar el lector a usar para la comunicación.

El segundo software que se implementará, será un software de acceso automático, es decir este software se iniciara pero las funciones principales no se ejecutaran sino hasta que la tarjeta se encuentre presente en el lector. Este software hará automáticamente la lectura del archivo creado en la tarjeta y su contenido, por lo que no necesita que una persona esté constantemente sentada en el computador mirando si está el usuario en la base de datos o no, o estar inscribiéndolo en un log nombre y hora de entrada.

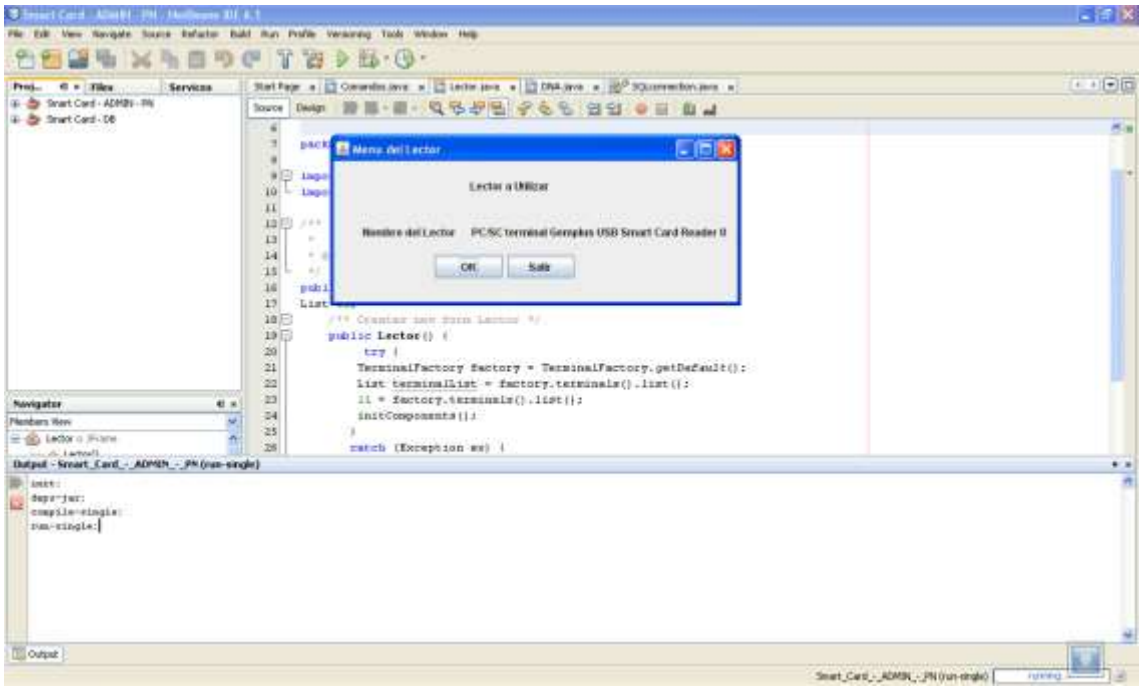
Además, al software se le añadirá la función de servir con un micro controlador y un relay, ya que el software al comprobar que existe el usuario en la base de datos, mandara una señal por un pin del puerto de impresora conocido como el puerto paralelo a un micro controlador el cual comprobara la entrada si es un 1 lógico, enviara este uno lógico por un puerto de salida, el cual será recibido por un relay, el cual le enviara una señal para dejar activa la puerta de entrada al aula, pero si el micro controlador recibe un 0, este enviara un cero al relay, cortándole la señal a la puerta.

5.1.7 Funcionamiento Prototipo El software desarrollado para esta tecnologia (Tarjetas Inteligentes), fue implementado en JAVA con la herramiento NetBeans IDE 6.1, cabe resaltar que este software no se pudo

terminar, debido a que se tuvo un problema con el proveedor de las tarjetas, ya que estas estan protegidas con contraseñas y nunca se pudo resolver este inconveniente. El funcionamiento de la aplicación que se logro desarrollar es el siguiente:

Al ejecutar el programa aparece una primera ventana, que nos muestra el tipo de lector que se esta utilizando, que para este caso es: PC/SC Terminal Gemplus USB Smart Card Reader (GEM PC TWIN), el lector que se muestra en la pantalla lo detecta el programa antes de ejecutarse:

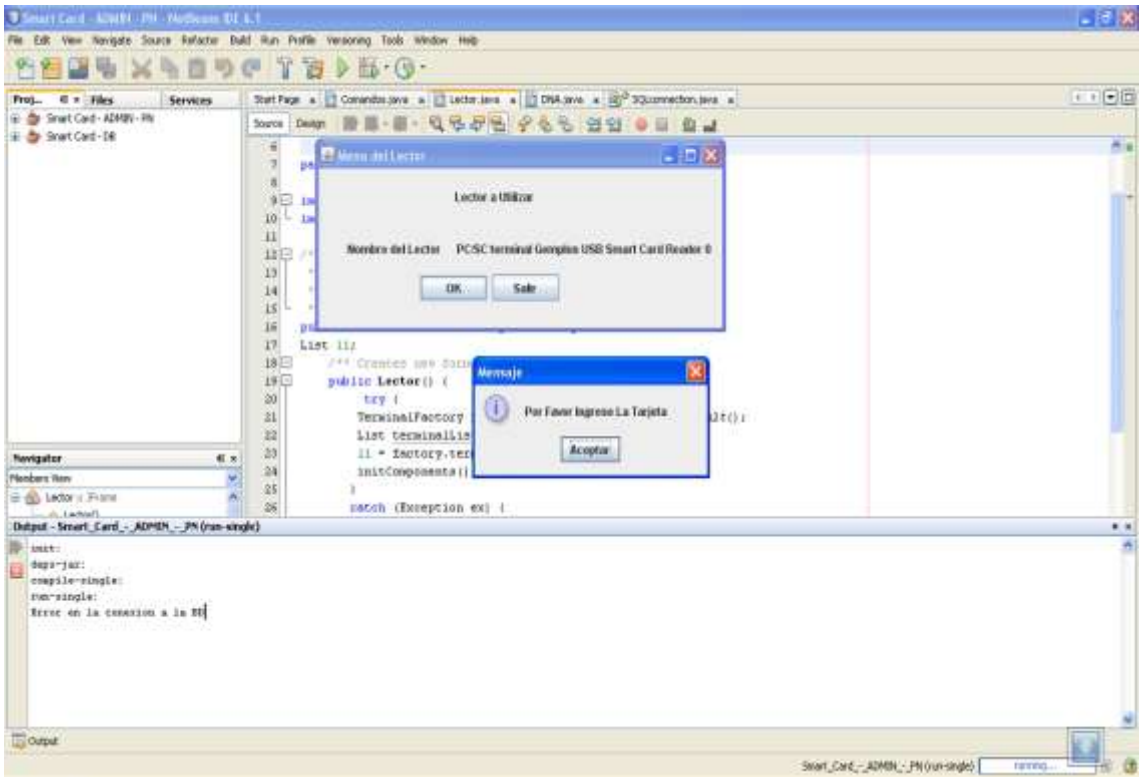
Figura No.58: Funcionamiento Prototipo Tarjeta Chip Ejecución del programa



Fuente: Diseño Grupo Investigador

Una vez ejecutado el programa se da click en el boton OK y el programa verificara que exista una tarjeta dentro del lector, de no ser asi, emitira una advertencia como se ve a continuación:

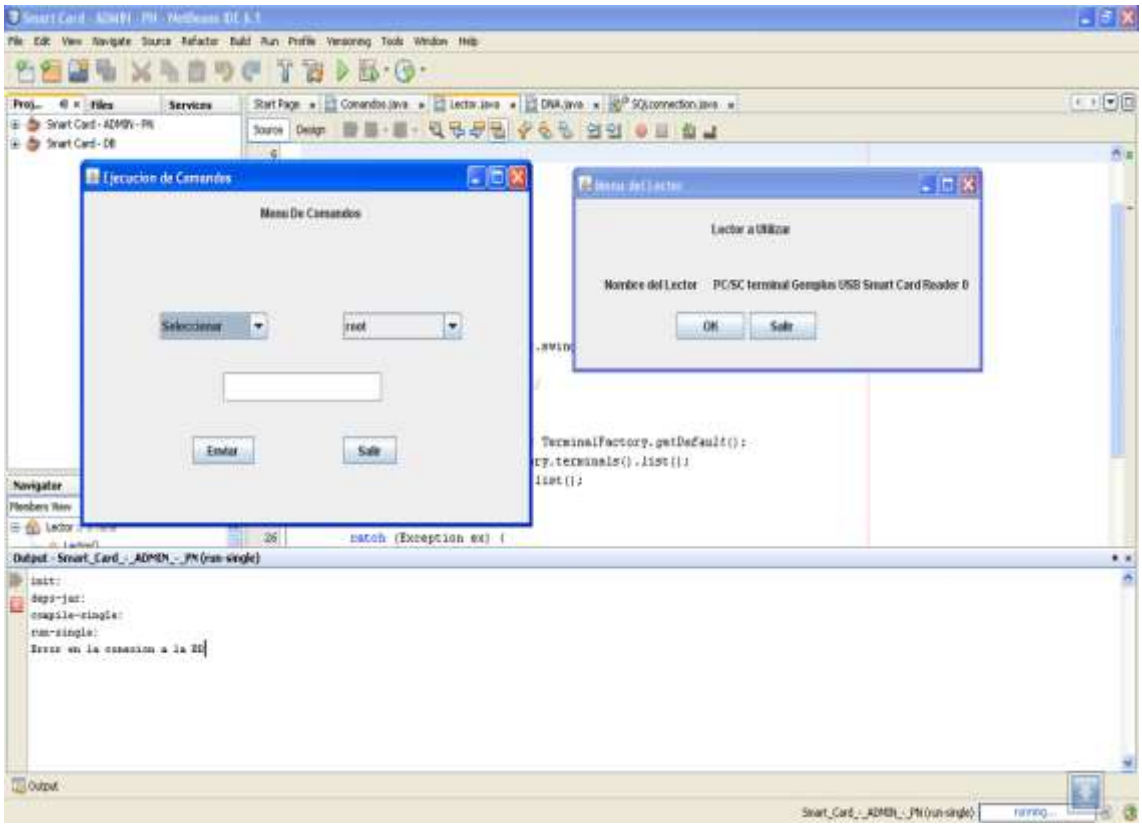
Figura No.59: Funcionamiento Prototipo Tarjeta Chip- Error de Tarjeta



Fuente: Diseño Grupo Investigador

Despues de tener la tarjeta en el lector, se abrira una nueva ventana que representa el menú principal de las funciones del lector, desafortunadamente solo le logro implementar la función de leer el root de la tarjeta, ya que como se explico anteriormente surgieron problemas con el proveedor que llevo a que este software no pudiera terminarse, el menú principal es el siguiente (ventana izquierda):

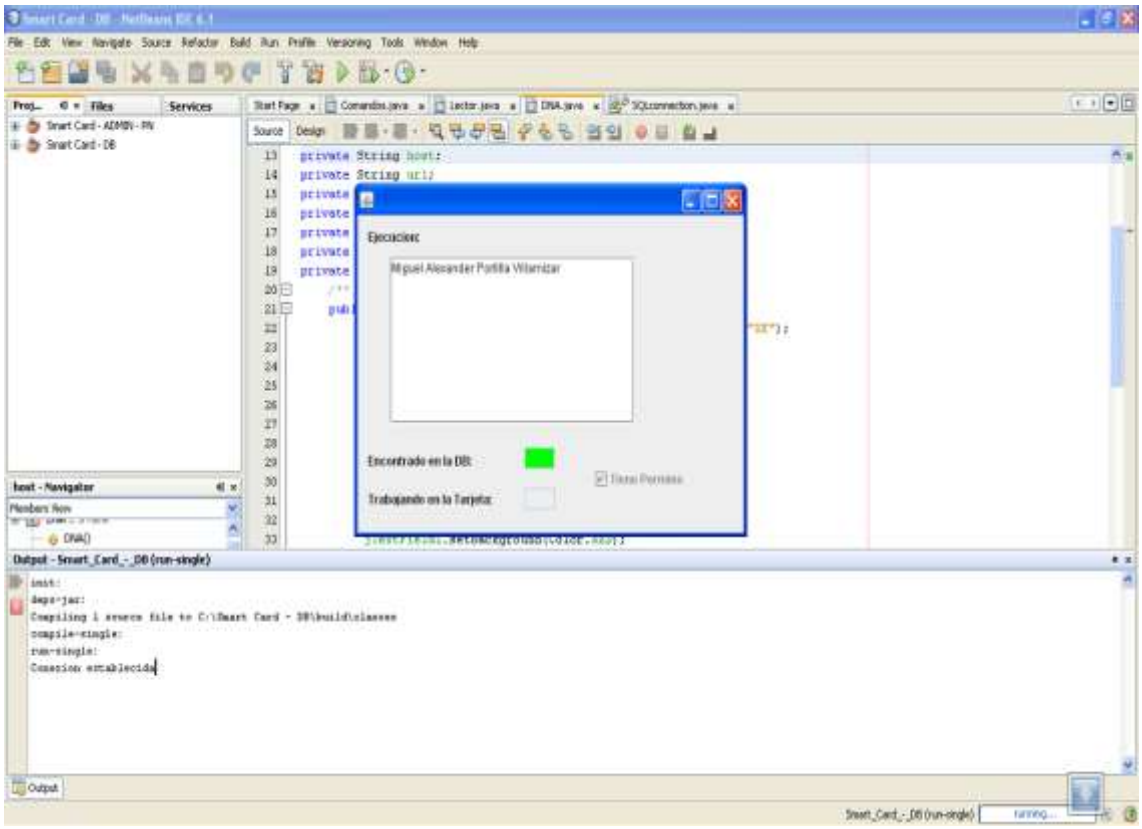
Figura No.60: Funcionamiento Prototipo Tarjeta Chip - Menú principal



Fuente: Diseño Grupo Investigador

Finalmente se creo otra aplicación que nos permite realizar la consulta con la base de datos, para verificar el control de acceso a las aulas, para este caso se ejecuto la busqueda del estudiante Miguel Portilla, es importante resaltar que cuando el acceso es permitido la pantalla mostrara un cuadro verde, de lo contrario el cuadro sera de color rojo:

Figura No.61: Funcionamiento Prototipo Tarjeta Chip - Comparación Base de Datos



Fuente: Diseño Grupo Investigador

6. CONCEPTUALIZACIÓN DE LA PROPUESTA

6.1 CONVOCATORIA

Basado en las experiencias e investigaciones realizadas por el grupo Investigador en cuanto al proyecto PROTOTIPO DE AUTENTICACIÓN PARA SEGURIDAD Y CONTROL DE ACCESO EN LAS AULAS DE LA UNIVERSIDAD AUTONOMA DE BUCARAMANGA, el Ing. Eduardo Carrillo en representacion de la Universidad cito a las empresas Grupo Condor, IONIX y al grupo investigador para hacer un análisis científico y técnico sobre los temas de seguridad y control de acceso.

6.2 REUNIÓN UNIVERSIDAD, EMPRESAS Y GRUPO INVESTIGADOR

El grupo investigador interesado en seguir la exploración de todos los procedimientos y en adquirir otras nuevas metodologias, que permitan el desarrollo de las tareas concernientes al control de acceso, atendio la propuesta del Ing. Eduardo Carrillo junto con el Grupo Condor, de exponer los avances y las experiencias vividas durante el trascurso del proyecto con las tarjetas inteligentes, donde se realizo una presentación de los lectores, la tarjetas, la base de datos y el programa, con el fin de comunicarles las debilidades y problemas encontrados.

Una vez terminada la presentación, se realizo un debate donde se expresaron varios puntos de vista en cuanto a la tecnologia trabajada y el Grupo Condor representado por su Gerente (Ing. Nestor Santos), comento una nueva

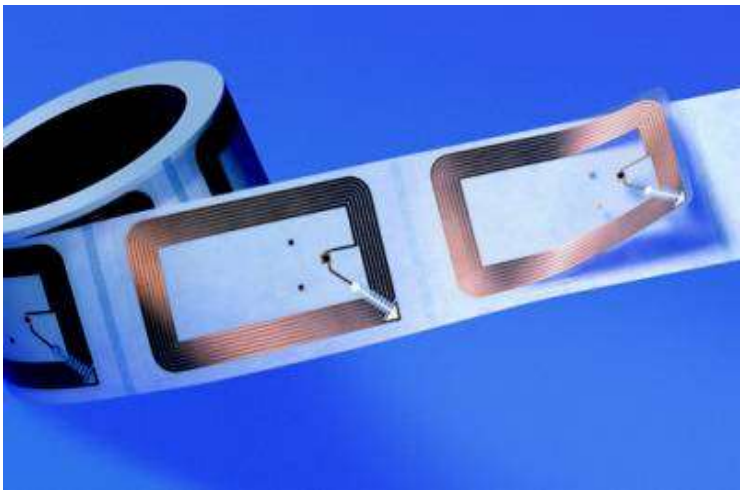
tecnologia (RFID), donde expresaba su interes en que el grupo investigador a traves de sus experiencias adquiridas, trabajara esta nueva tecnologia.

6.3 CONVENIO

Durante la reunión se llegó a la conclusión de que el grupo investigador en representacion de la UNAB, continuara trabajando con la nueva tecnologia expuesta, pero con la condicion de que esta experiencia se deberia realizar en las instalaciones de la empresa y fue asi como se celebro un contrato entre las partes para desarrollar las diferentes actividaes durante las dos semanas siguientes al convenio. VER ANEXO 11: CONVENIO, una vez iniciada la practica en las instalaciones de la empresa, se firmo una carta entre las partes (Grupo Investigador y Grupo Condor) de privacidad y exclusividad de informacion para la tecnologia RFID.

7. IMPLEMENTACIÓN PROTOTIPO RFID

Figura No.62: Tarjeta RFID



Fuente: http://www.frascatilivinglab.org/images/A_rfid.jpg

La identificación por radiofrecuencia (RFID), es un sistema que trabaja en medio inalámbrico y es utilizado principalmente para identificar etiquetas o tags, esta tecnología desde hace años ha estado constituyéndose como la evolución del código de barras, ya que en ella se ha podido agregar más información (datos). Una de sus características más relevantes, es que puede ser captada por medios de comunicación masivos como es Internet.

Los tags pueden ser incorporados a diferentes entes como por ejemplo: tarjetas, relojes, llaveros, llaves, celulares, etc. Además por su pequeño tamaño pueden ser introducidos debajo de la piel de las personas como de animales, esto se utiliza principalmente como rastreadores.

La tecnología con la que trabajan los tags RFID, son de proximidad y de no línea de vista, esto quiere decir que entre el tag y el lector no necesariamente debe haber contacto pero si una distancia mínima de 10cm, esto se logra

gracias a que estos tags (trasnpondedores) poseen unas antenas que permiten enviar y recibir datos (peticiones) por medio de ondas de radio hacia el lector (transceptor), el cual a su vez está emitiendo estas mismas ondas permanentemente para interactuar con algún ente cercano a su rango de influencia [5].

Las etiquetas de RFID se dividen en tres tipos de memoria las cuales son:

- Solo lectura: el codigo de identificacion del tag es puesto en su elaboracion y no puede ser modificado.

- Lectura y escritura: la informacion de estos tags si puede ser modificada por los lectores.

- Anticolisión: son etiquetas que pueden ser leidas al mismo tiempo por un solo lector.

Los lectores que utiliza esta tecnologia estan compuestos principalmente por: una antena, un decodificador y un trasnceptor, estos lectores desde el momento en que empiezan a trabajar envian ondas radiales (13.56Mz – frecuencia RFID) constantemente para interactuar con algún tag que este dentro de su rango de influencia y al encontrarlo empiezan la decodificacion de datos para interactuar con el.

7.1 PROTOCOLOS

La tecnologia RFID trabaja con 2 tipos de protocolo para sus tags, estos son:

7.1.1 Protocolo 15693 ISO 15693 es un estándar ISO para "Tarjetas de Vecindad" (Vicinity Cards), como por ejemplo las tarjetas que pueden ser leídas desde una mayor distancia que las tarjetas de proximidad.

El sistema ISO 15693 opera en la frecuencia 13.56MHz, y ofrece una distancia máxima de lectura de entre 1 y 1,5 metros.

7.1.2 Protocolo 14443 ISO 14443 es un estándar internacional para tarjetas de identificación electrónicas, como por ejemplo tarjetas inteligentes, y que trabaja conjuntamente con la Organización Internacional De Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).

Este estándar consta de cuatro partes y se describen dos tipos de tarjetas: “A” y “B”. Las principales diferencias entre estos tipos son:
Parte 1. Preocupación de los métodos de modulación.
Parte 2. Codificación de los planes.
Parte 3. El protocolo de inicialización de los procedimientos.
Parte 4. Las tarjetas de ambos tipos (A y B) utilizan el mismo protocolo de alto nivel (llamado T = CL). El protocolo T = CL especifica los bloques de datos y los mecanismos de intercambio:

1. Bloque de datos de encadenamiento
2. Tiempo de espera de extensión
3. Múltiple activación

La tarjeta Calypso cumple con la norma ISO/IEC 14443 parte 1, 2, 3 y 4 de tipo B. Las tarjetas Mifare cumplen con las partes 1, 2 y 3 de tipo A de la especificación ISO/IEC 14443.

Numeral 7.1 Tomado de wikipedia.

7.2 IMPLEMENTACIÓN BASE DE DATOS (JDVELOPER 11)

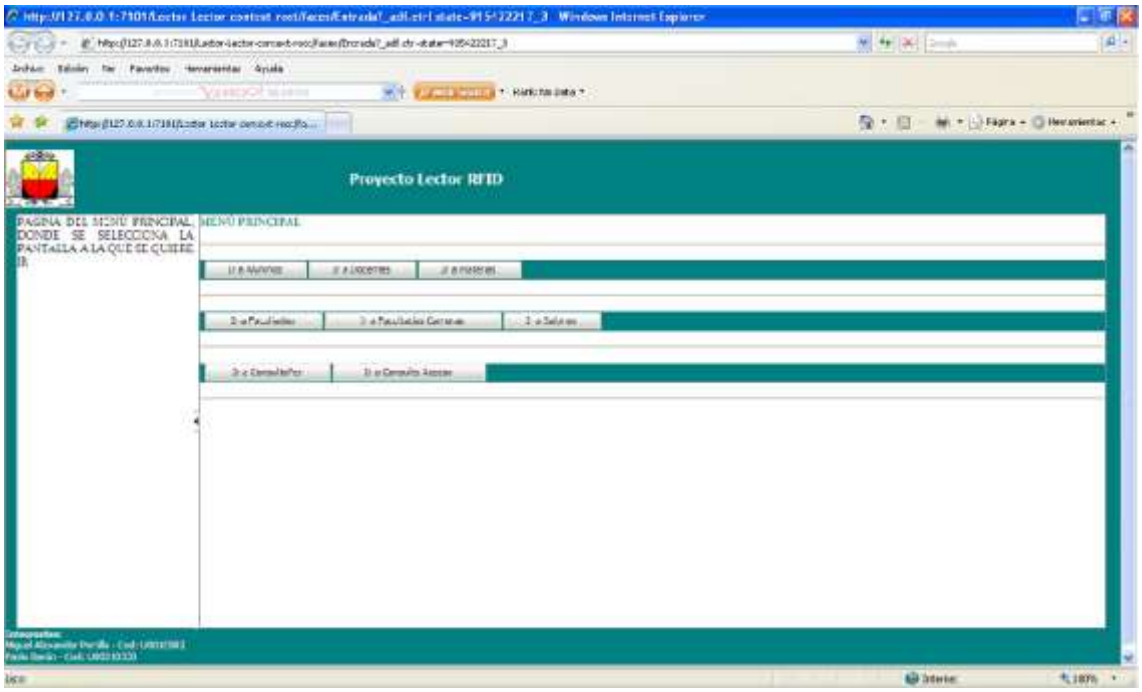
La base de datos usada para la implementacion del prototipo RFID es la misma que fue creada en el numeral 5.1.2, la cual se utilizo para el prototipo de Tarjetas Inteligentes y esta implementada en Oracle.

Para la construcción del software de esta nueva tecnologia se crearon unas paginas en el programa (JDeveloper 11) que permiten al usuario trabajar con la información de las tablas que conforman la base de datos principal y asi realizar consultas, agregar nueva información o eliminar datos si lo desea, tambien en las paginas se incorporaron unas ayudas situadas al lado izquierdo de estas que funcionan como ventanas desplegables, para ayudar al usuario a identificar los datos con los que esta trabajando y facilitarle su labor en el manejo de la información.

Además las paginas creadas para manipular la información de la base de datos funcionan en web, lo que hace que este proyecto pueda implementarse de manera total en la Universidad, debido a que las aplicaciones de la UNAB trabajan en la misma plataforma.

Las paginas elaboradas para la manipulación de datos son las siguientes:

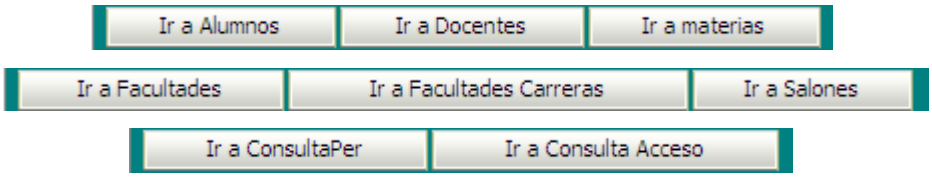
Figura No.63: Paginas JDeveloper 11 - Página de Menú Principal



Fuente: Diseño Grupo Investigador

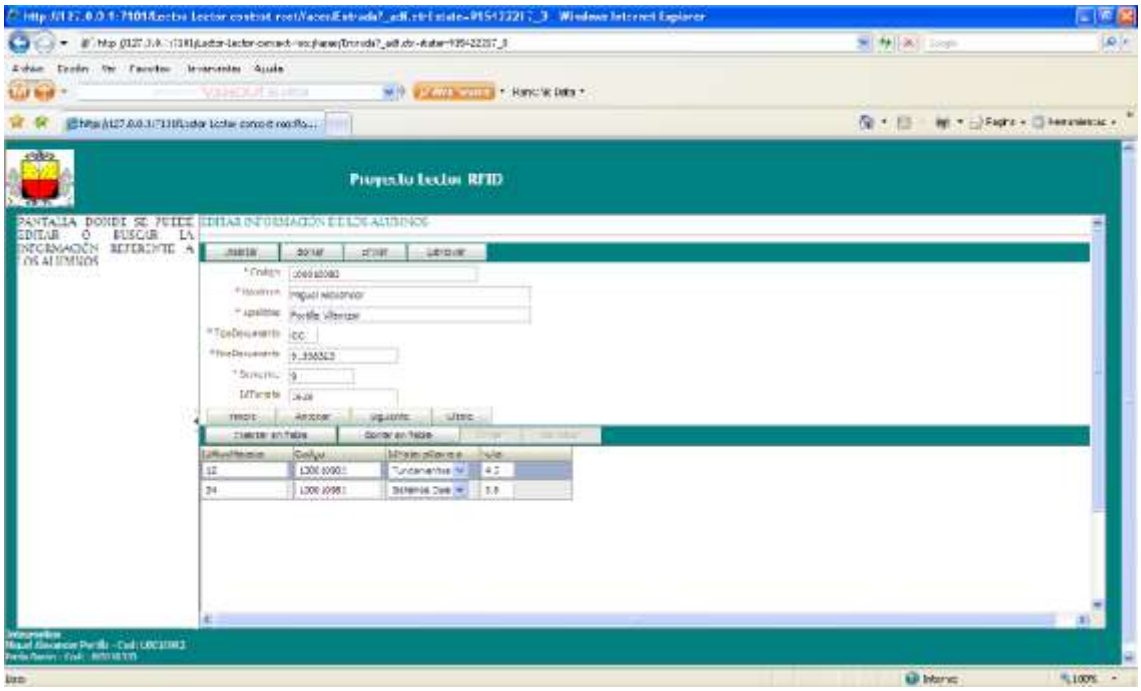
La página de menú principal como su nombre lo indica es la pagina principal de la aplicación, ya que desde ella se puede acceder a cualquier otra página que se desee; el menú principal esta compuesto por 8 botones los cuales son:

Figura No.64: Paginas JDeveloper 11 - Botones Menú Principal



Fuente: Diseño Grupo Investigador

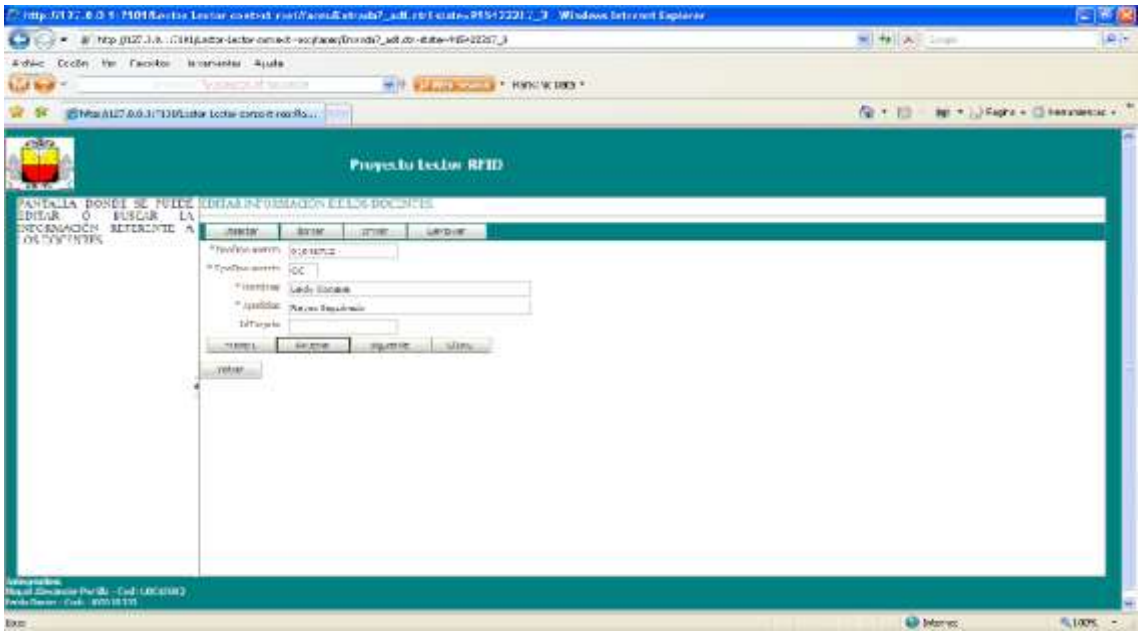
Figura No.65: Paginas JDeveloper 11- Página Alumnos



Fuente: Diseño Grupo Investigador

En esta página se puede observar, consultar o modificar la información referente a los alumnos.

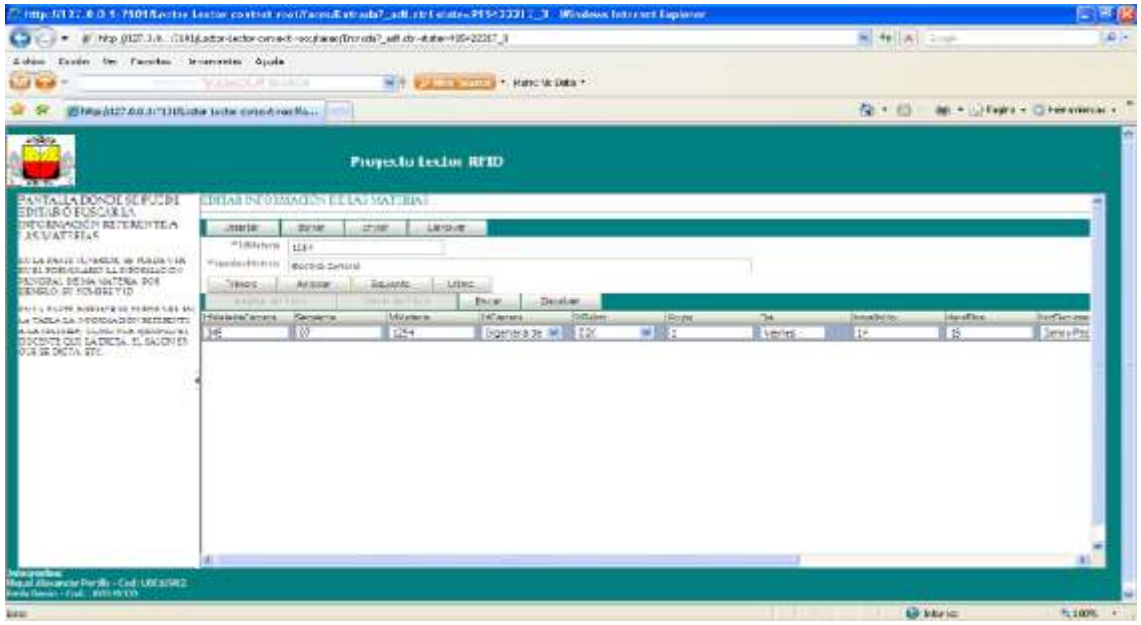
Figura No.66: Paginas JDeveloper 11 - Página Docentes



Fuente: Diseño Grupo Investigador

En esta página se puede observar, consultar o modificar la información referente a los docentes.

Figura No.67: Paginas JDeveloper 11 - Página Materias

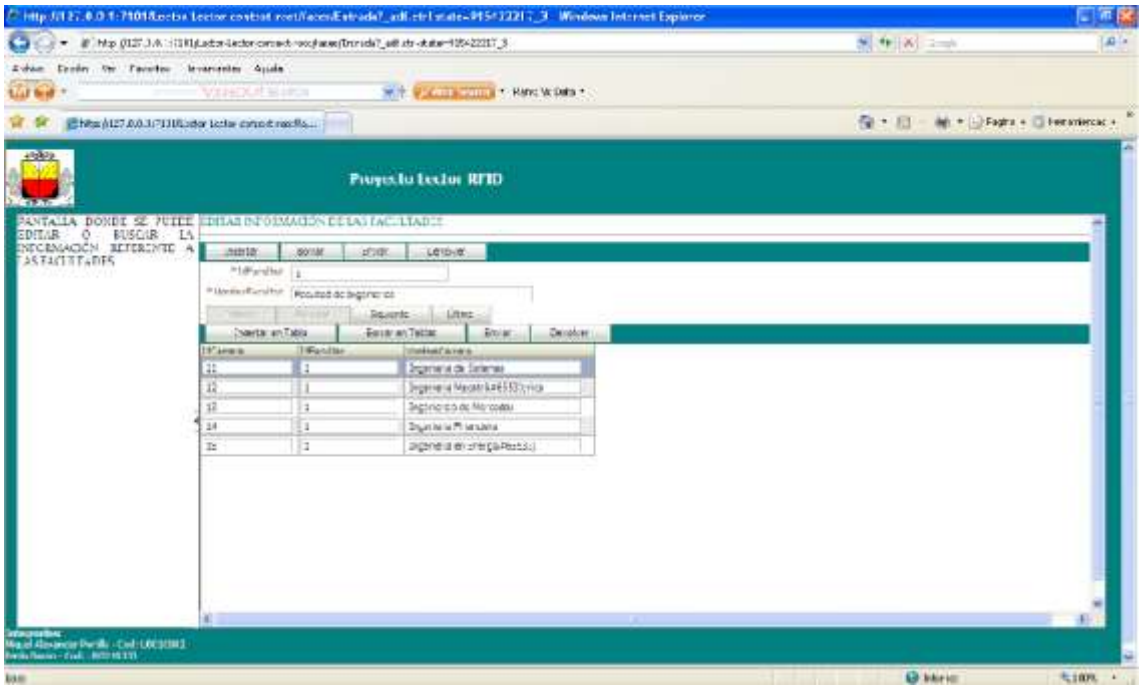


Fuente: Diseño Grupo Investigador

Página donde se puede editar ó buscar información referente a las materias.

En la parte superior, se puede ver en el formulario la información principal de la materia, por ejemplo: su nombre y ID. Mientras que en la parte inferior se puede ver en la tabla, la información referente a la materia, como por ejemplo: el docente que la dicta, el salón donde se dicta, etc.

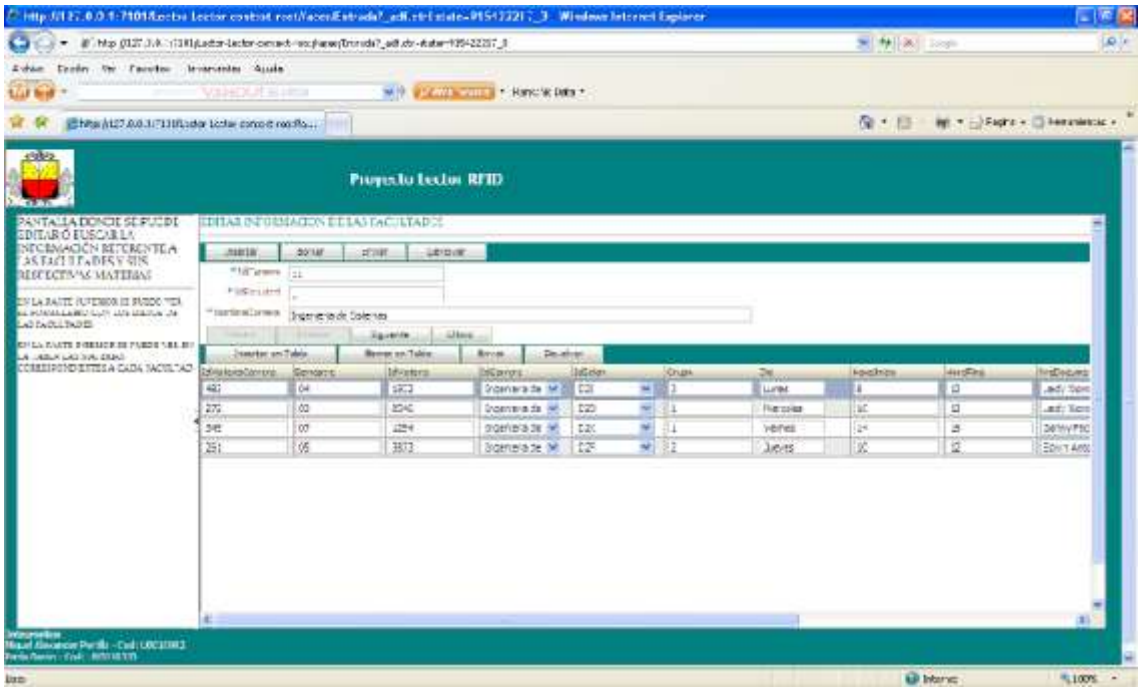
Figura No.68: Paginas JDeveloper 11 - Página Facultades



Fuente: Diseño Grupo Investigador

En esta página se puede observar, consultar o modificar la información referente a las facultades que conforman la Universidad.

Figura No.69: Paginas JDeveloper 11 - Página Facultades Carreras

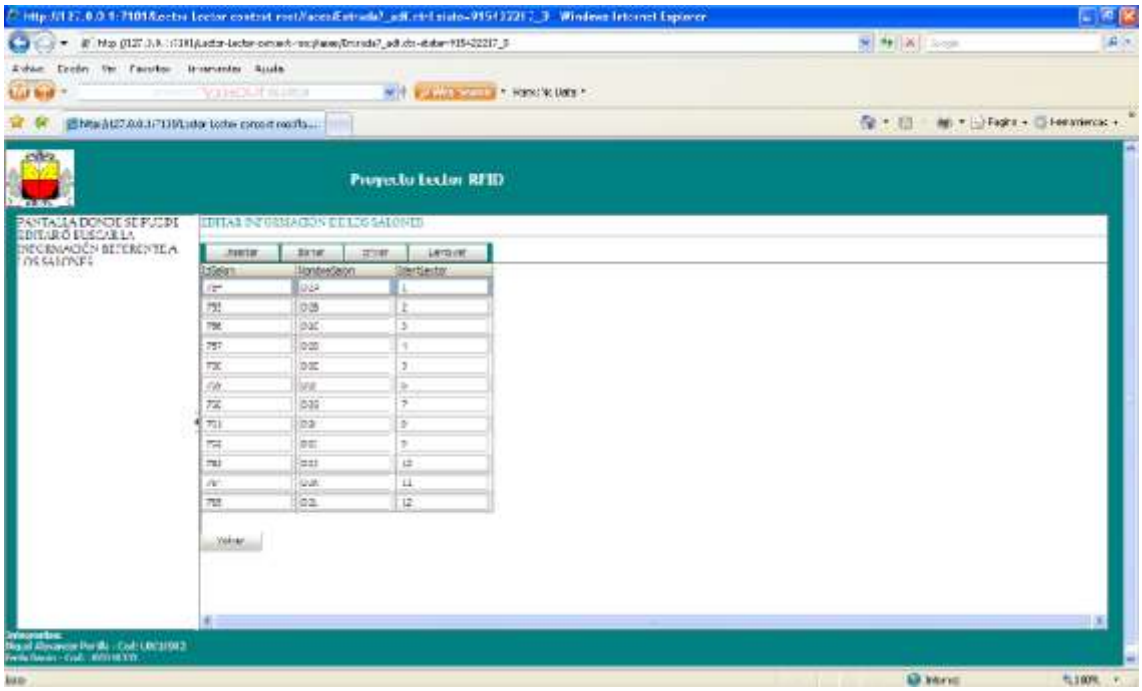


Fuente: Diseño Grupo Investigador

Página donde se puede editar ó buscar información referente a las carreras de cada facultad.

En la parte superior, se puede ver en el formulario los datos de las facultades. Mientras que en la parte inferior se puede ver en la tabla, las materias correspondientes a cada facultad.

Figura No.70: Paginas JDeveloper 11 - Página Salones



Fuente: Diseño Grupo Investigador

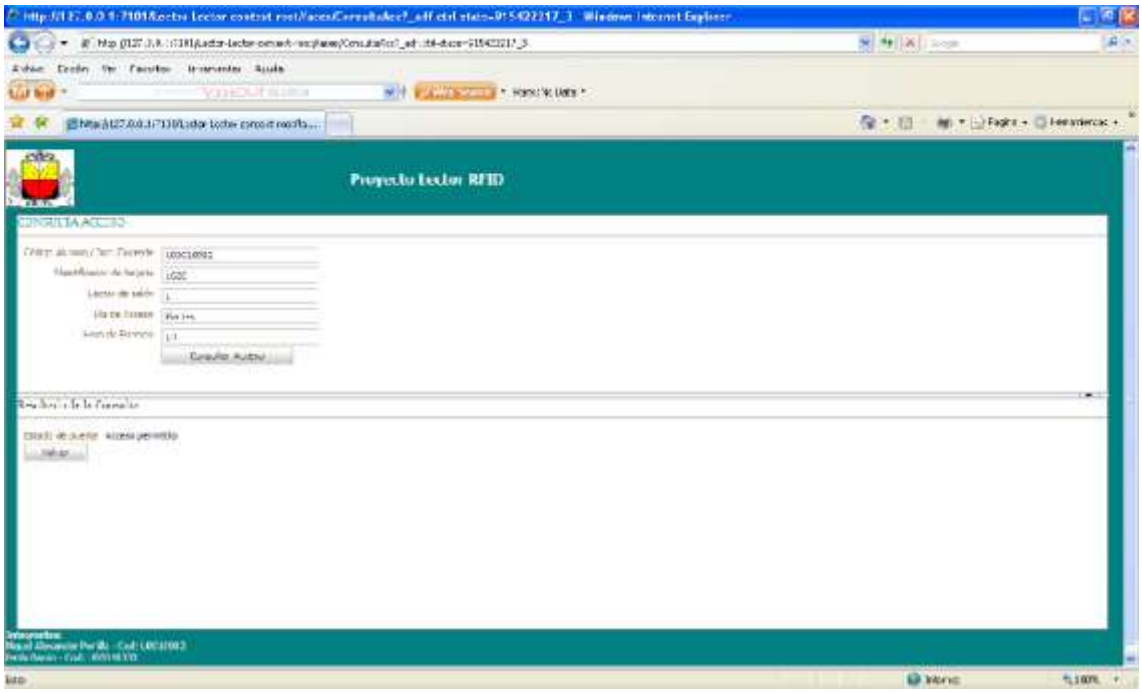
En esta página se puede observar, consultar o modificar la información referente los diferentes salones de la Universidad, para este caso se utilizaron los salones del bloque D.

Figura No.71: Paginas JDeveloper 11 - Página ConsultaPer

Fuente: Diseño Grupo Investigador

Esta Página es la mas importante de todas, ya que en esta pagina se consulta la informacion de los usuarios, una vez encontrado el usuario esperado,se da click en el boton “enviar codigo” e inmediatamente se ejecutan los programas en Java y C++ que guardan el codigo (Alumno) o cedula (Docente) en la tarjeta que se quiera.

Figura No.72: Paginas JDeveloper 11 - Consulta Acceso



Fuente: Diseño Grupo Investigador

Esta página de consulta acceso es la segunda mas importante de nuestro modelo, ya que con esta, se puede verificar el acceso de los usuarios a los salones, permitiendo o negando la entrada por medio de la comparación entre el codigo, identificador de la tarjeta, el dia y la hora de la clase con los datos de las tablas de Oracle.

7.3 DESCRIPCION DEL SOFTWARE

Para la implementación del prototipo RFID, se elaboraron 3 programas para el funcionamiento de los lectores, 1 de las aplicaciones se elaboro en C++ y las otras dos trabajan conjuntamente Java y C++.

El software elaborado es el siguiente:

7.3.1 Software Administrador Este programa consta de tres funciones (Inventario, leer, escribir) cada una de ellas complementa las otras dos, el funcionamiento de este primer programa es el siguiente: al ejecutarlo, lo primero que se hace es leer el inventario de la tarjeta, en el cual se nos mostrara el UID de cada tarjeta leida, despues de esto se ejecuta la función leer, en la cual ya podemos ver los datos almacenados en la tarjeta, esto lo podemos ver leyendo los bloques que se quieran, y por ultimo se tiene la función de escribir, en la cual se le grabaran los datos que se quieran en la tarjeta, que para nuestro caso es el código del alumno o la cedula del docente. En el numeral 7.4.1 se explicara de una manera mas detallada este programa.

7.3.2 Software Grabar Este segundo programa se ejecuta desde la página de "ConsultaPer", explicada en el numeral 7.2, principalmente lo que hace este programa es que al encontrar el usuario deseado, se selecciona el puerto por el cual esta conectado el lector y se da click en el boton "Enviar Codigo", lo que hara que el programa en Java llame una aplicación en C++ que guardara el codigo del alumno en la tarjeta y a su vez extraera de la misma la tarjeta el UID que sera el asigando al alumno dueño de esta tarjeta. En el numeral 7.4.2 se explicara de manera mas detallada este programa.

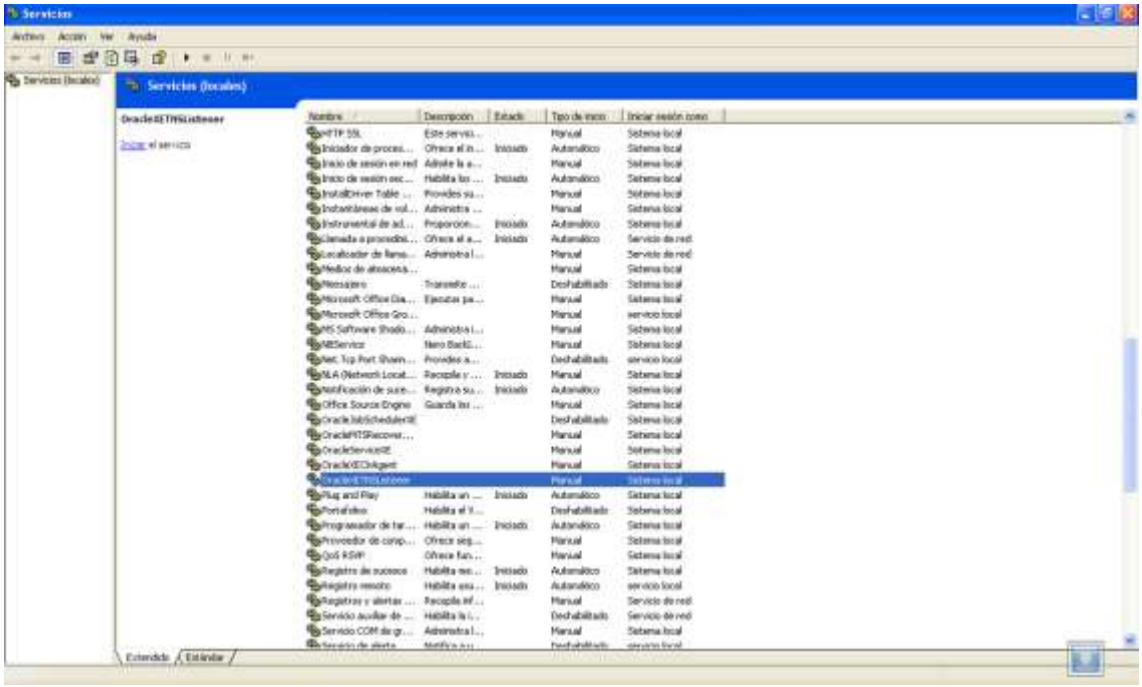
7.3.3 Software Leer Este tercer programa tambien combina las aplicaciones de Java y C++, ya que al ejecutarse desde C++ leera los datos de la tarjeta y los enviara al programa en Java por medio de un .txt para que sean comparados con los de la base de datos y asi permitir o negar el acceso del usuario. Al igual que los anteriores dos programas en el numeral 7.4.3 se explicara de manera mas detallada este programa.

7.4 FUNCIONAMIENTO PROTOTIPO

Una vez implementados los difrerentes sistemas y la base de datos, se procede a la ejecución de estos, la cual se realiza siguiendo los siguientes pasos:

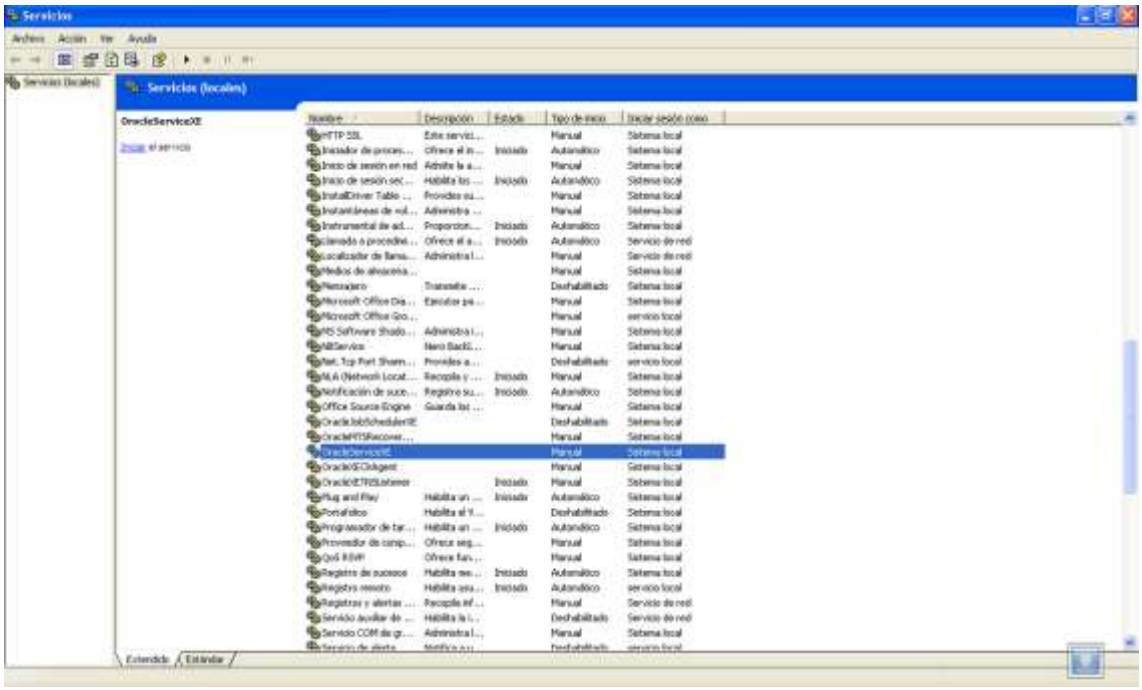
- Primero se procede a iniciar los servicios que nos permitiran trabajar con la base de datos, estos servicios son: OracleXENTSListener y OracleServiceXE.

Figura No.73: Iniciar servicio OracleXENTSListener



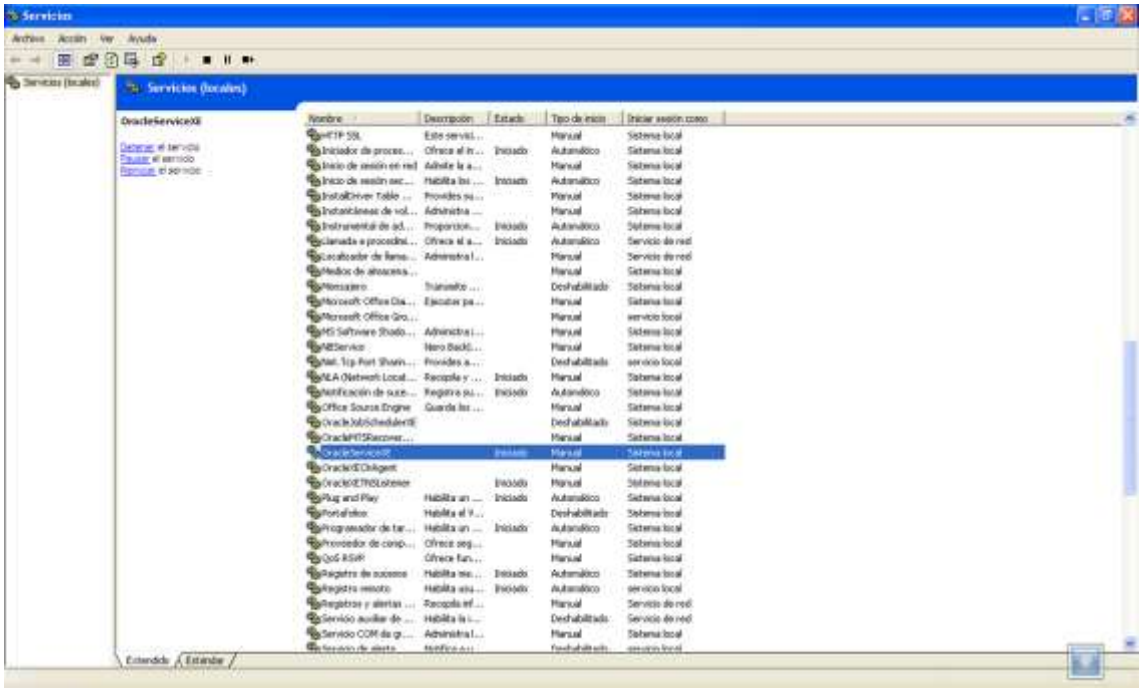
Fuente: Diseño Grupo Investigador

Figura No.74: Iniciar servicio OracleServiceXE



Fuente: Diseño Grupo Investigador

Figura No.75: Servicios Iniciados



Fuente: Diseño Grupo Investigador

En esta tercera imagen se puede observar los servicios ya iniciados, despues de esto se procede a la conexión de la base de datos, la cual se realiza escribiendo los siguientes comandos en la Línea de Comandos SQL:

Figura No.76: Establecer Conexión a Base de Datos

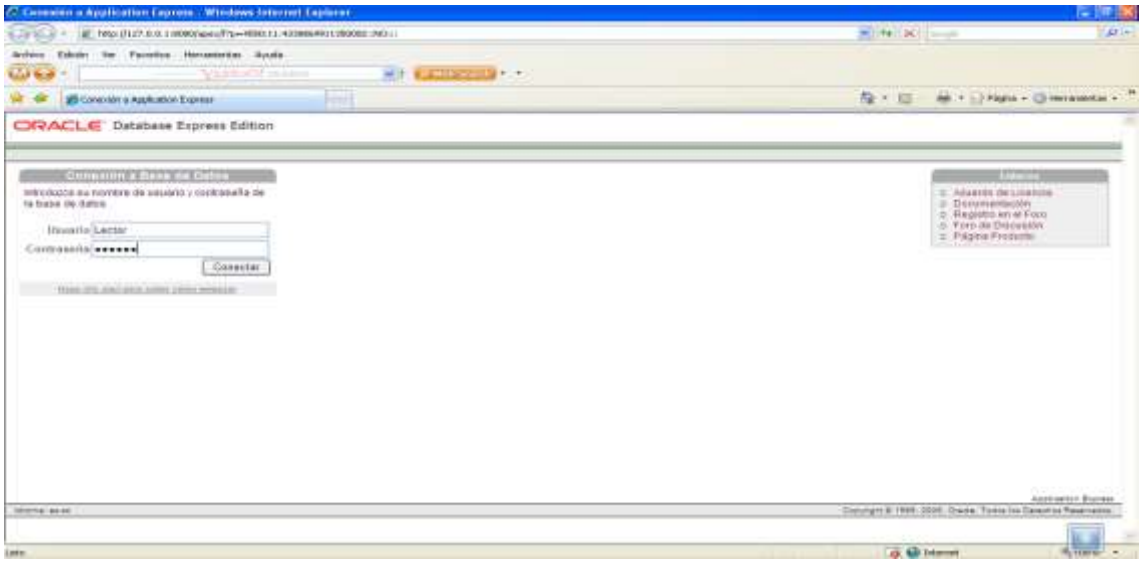
Fuente: Diseño Grupo Investigador

Las tres líneas que se deben escribir son:
Connect
System (usuario)
Root (contraseña)

Una vez conectado vamos a la pagina principal de Oracle, donde podremos observar las tablas, en esta pagina tambien se debe identificar el usuario y la contraseña, que para nuestro trabajo son:

Lector (usuario)
Lector (contraseña)

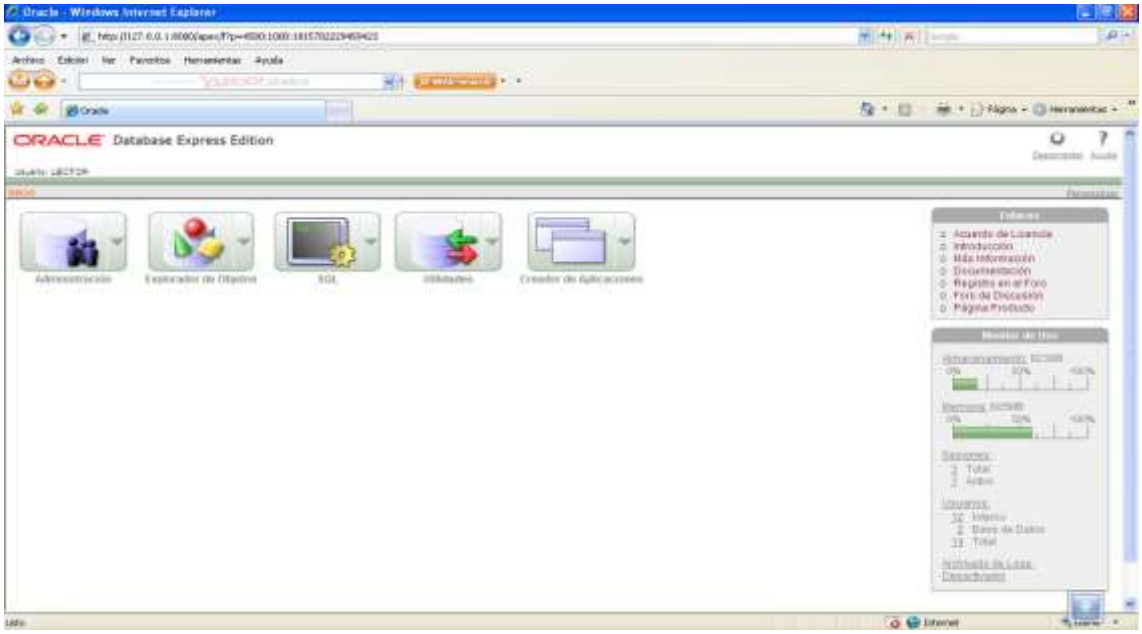
Figura No.77: Menú entrada Base de Datos Oracle



Fuente: Diseño Grupo Investigador

Una vez se halla ingresado al menu principal, se selecciona la opcion: Explorador de Objetos que es donde se encuentran las tablas de nuestra base de datos.

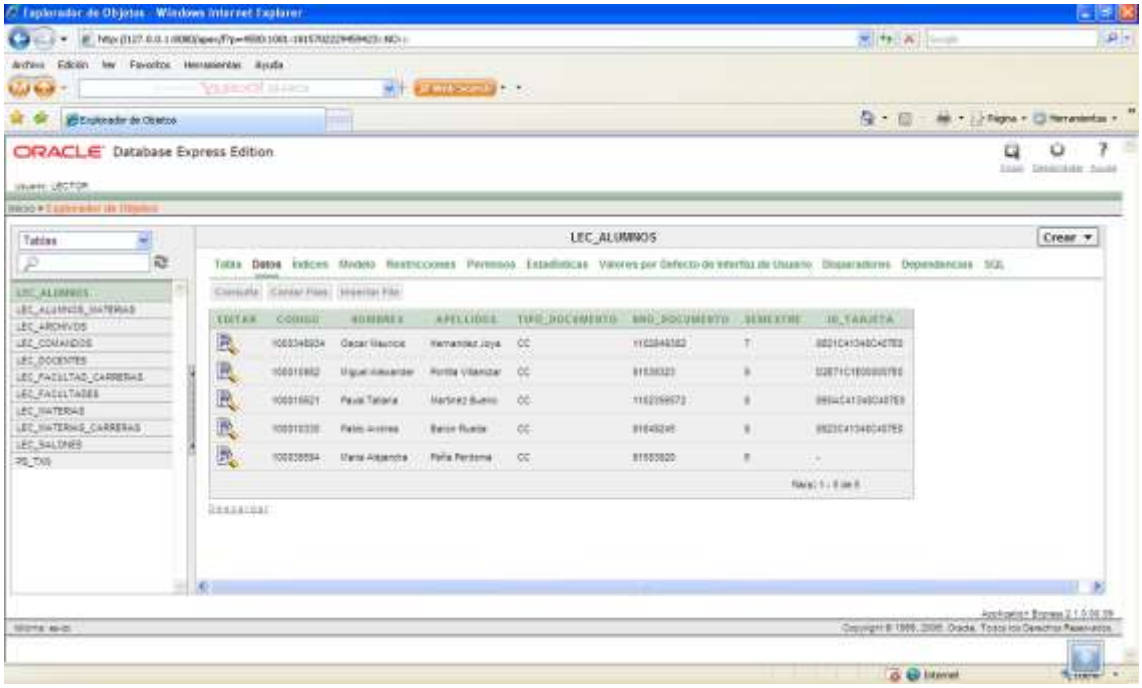
Figura No.78: Menú Principal Base de Datos Oracle



Fuente: Diseño Grupo Investigador

Esta imagen nos muestra una tabla (LEC_USUARIOS) de las que conforman la base de datos:

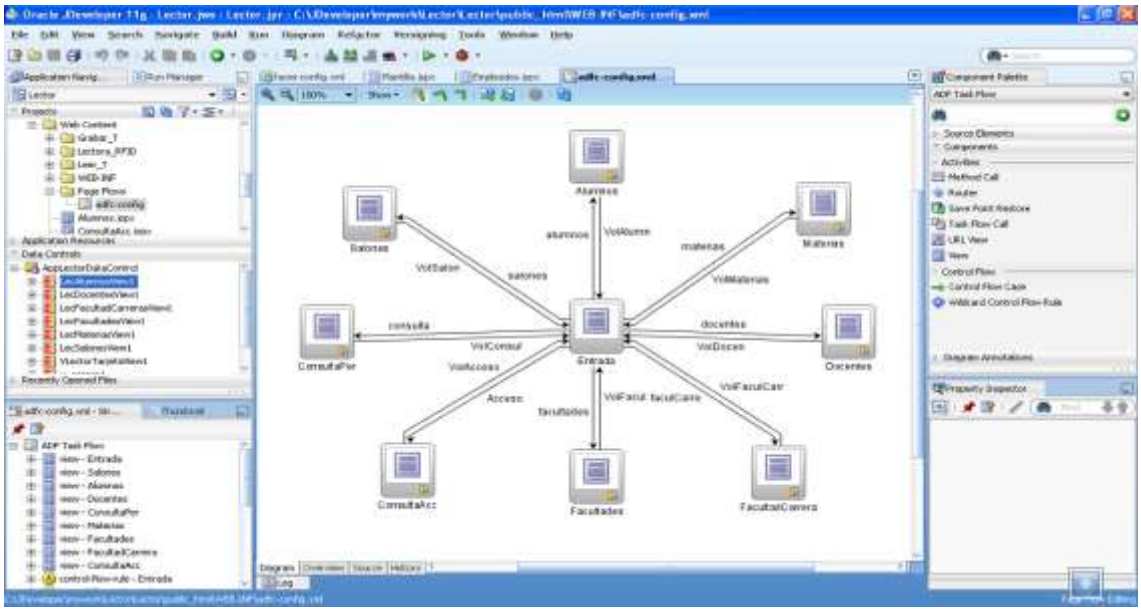
Figura No.79: Tabla LEC_ALUMNOS desde Base de Datos Oracle



Fuente: Diseño Grupo Investigador

Una vez iniciados los servicios y conectada la base de datos, procedemos a ejecutar las paginas de consulta y modificación de datos de los usuarios, creadas en JDeveloper 11, el modelo de paginas es el siguiente:

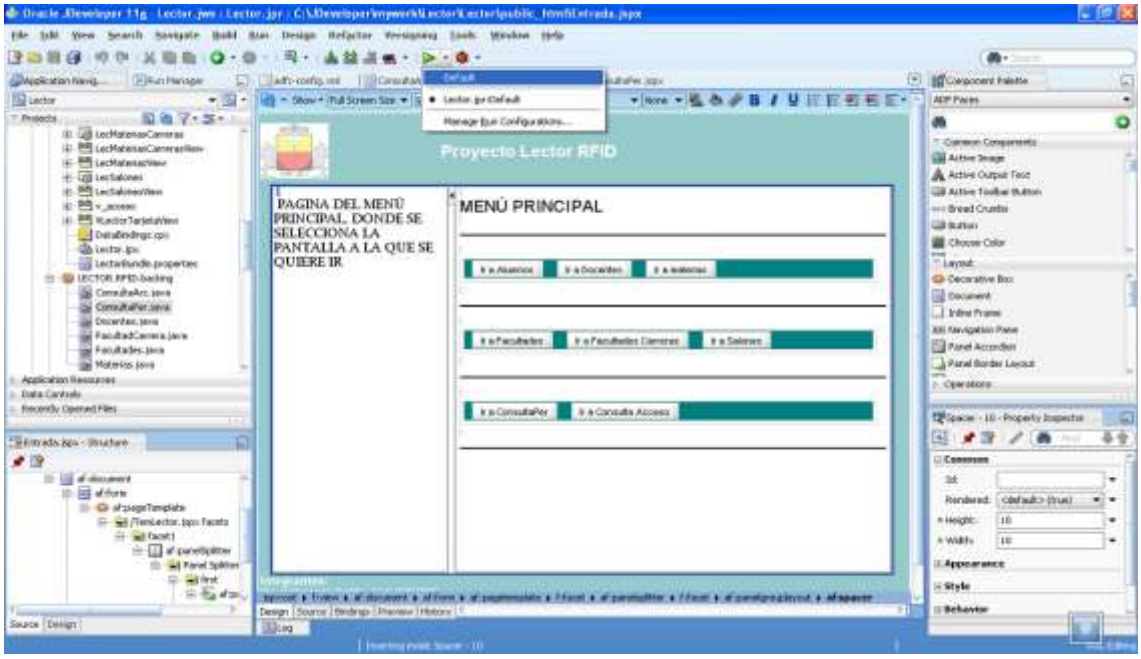
Figura No.80: Modelo de Paginas JDeveloper 11



Fuente: Diseño Grupo Investigador

Ahora se procede a iniciar el montaje de las paginas, para que nuestro sistema trabaje en red:

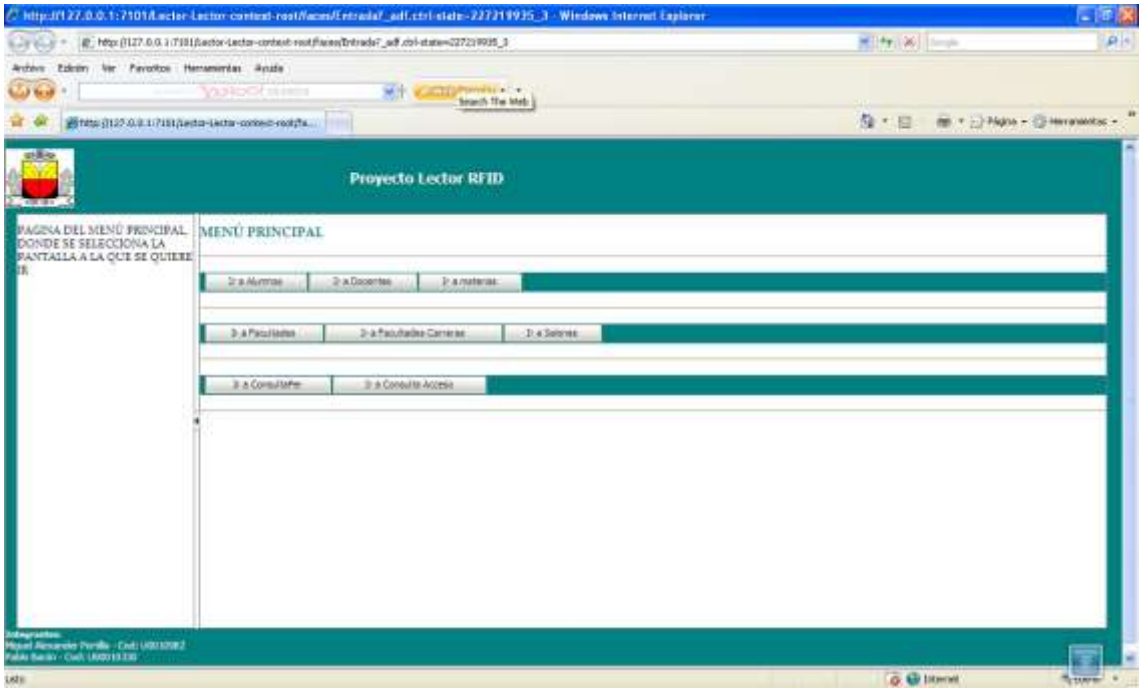
Figura No.81: Iniciar Montaje de Paginas



Fuente: Diseño Grupo Investigador

Despues de iniciadas las paginas se tiene este menú principal, en el cual podemos escoger la opción que queramos:

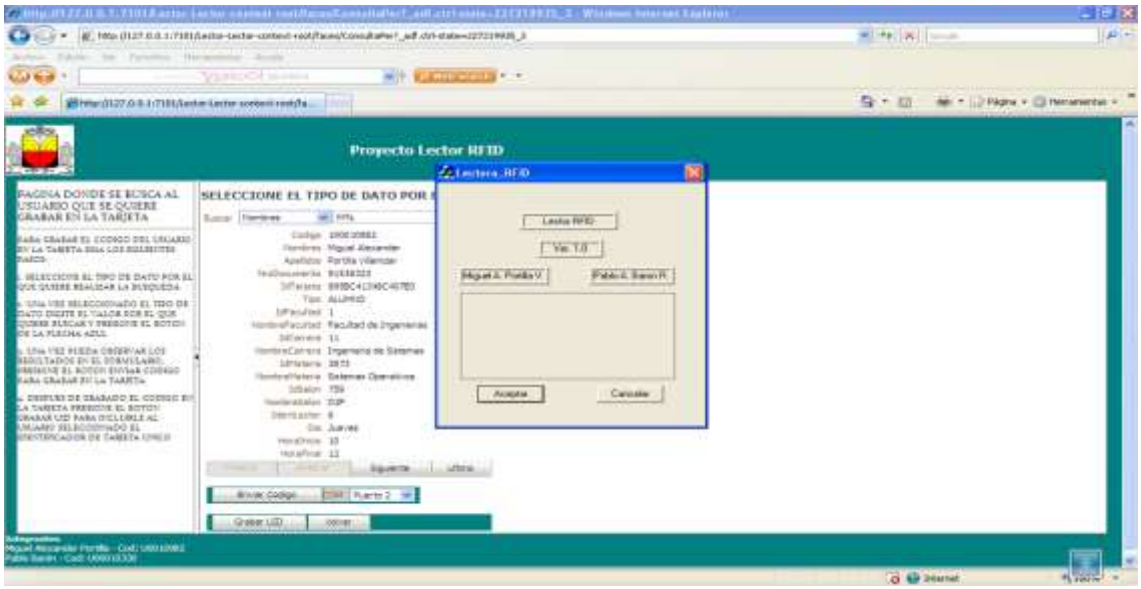
Figura No.82: Menú principal paginas JDeveloper 11



Fuente: Diseño Grupo Investigador

7.4.1 Software Administrador Este software fue el primero en desarrollarse y fue diseñado principalmente para un personal experto en el manejo de estas tarjetas, ya que todas sus opciones tienen que realizarse manualmente. Al iniciar este programa se tiene una primera pantalla que tiene como nombre Lectora_RFID:

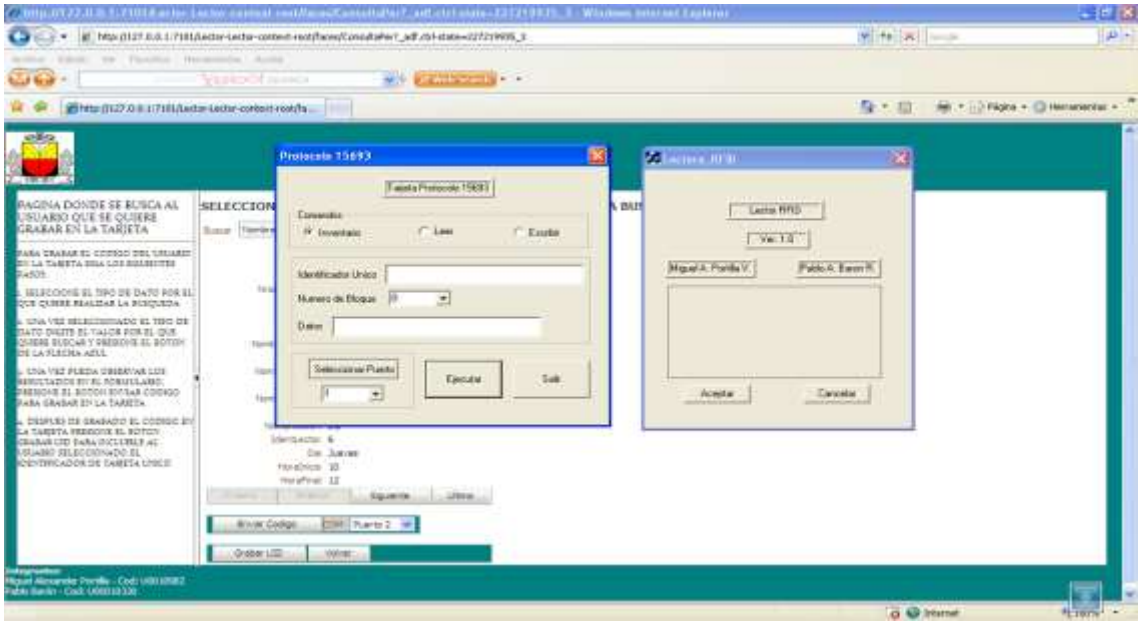
Figura No.83: Funcionamiento Software Administrador Tarjeta RFID - Ejecución del Programa



Fuente: Diseño Grupo Investigador

Al dar click en el boton aceptar se abre una nueva pantalla llamada protocolo 15693, donde aparecen las tres funciones que conforman este programa, las cuales son: Inventario, Leer y Escribir.

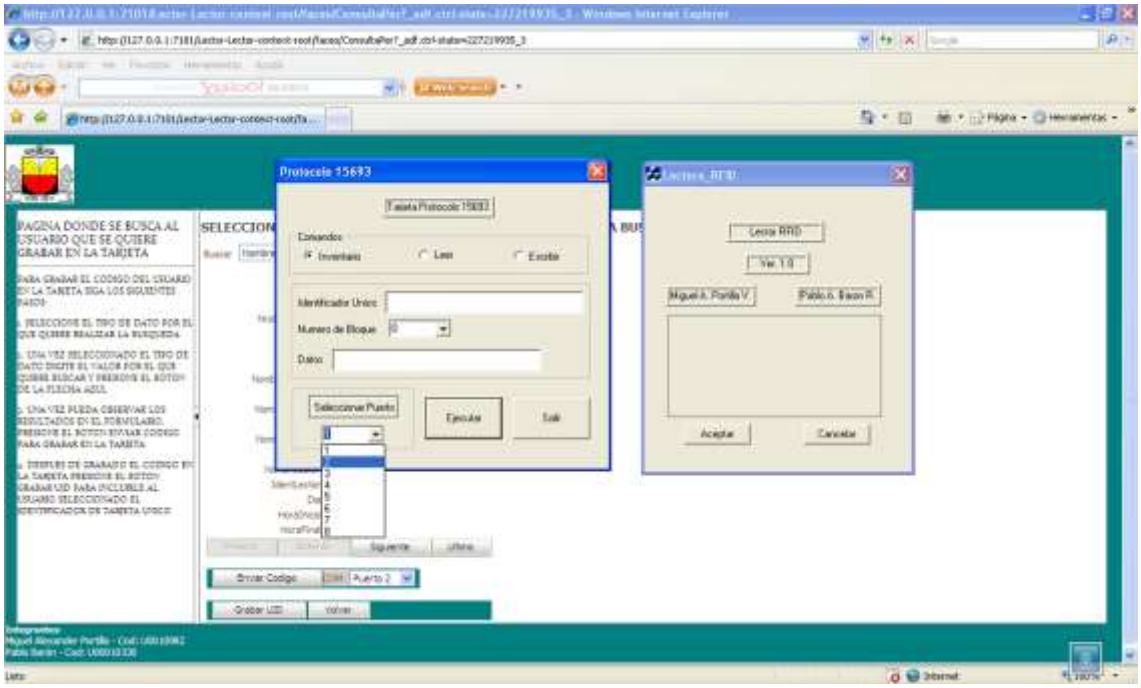
Figura No.84: Funcionamiento Software Administrador Tarjeta RFID Menú principal



Fuente: Diseño Grupo Investigador

Para la ejecucion de este programa, primero debemos seleccionar el puerto al cual esta conectado nuestro lector, que para este caso es el puerto 2:

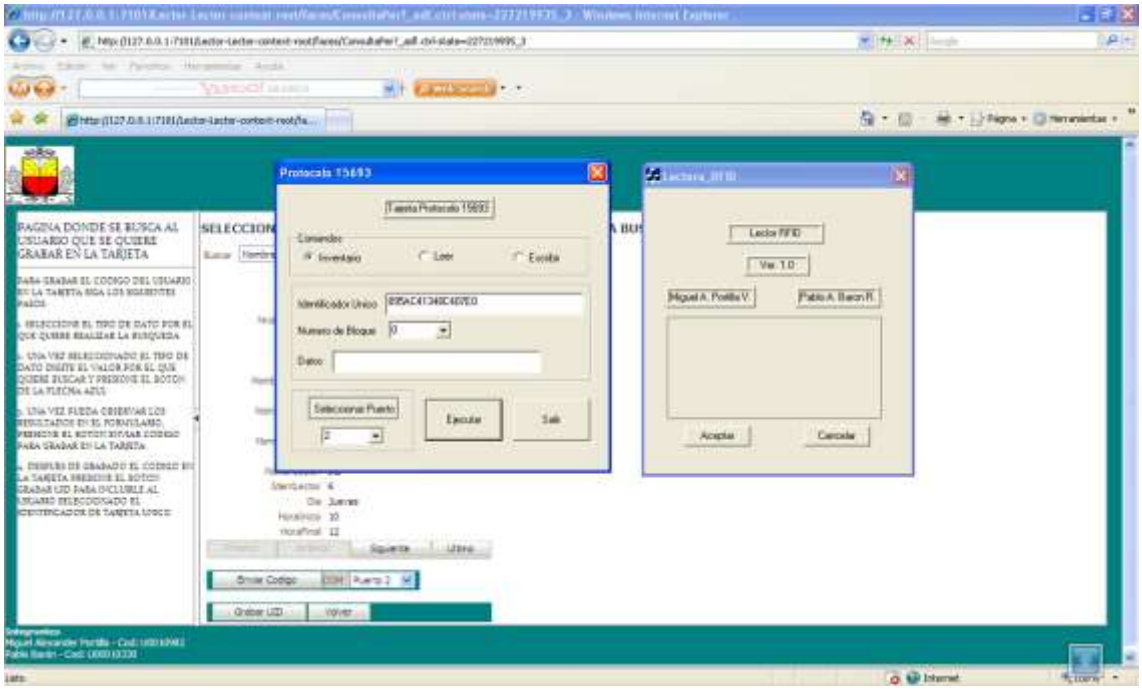
Figura No.85: Funcionamiento Software Administrador Tarjeta RFID - Selección de puerto



Fuente: Diseño Grupo Investigador

Despues de seleccionado el puerto y teniendo el lector junto a la tarjeta se procede a ejecutar la primera funcion que es Inventario, la cual nos sirve para leer el UID (identificador unico de la tarjeta):

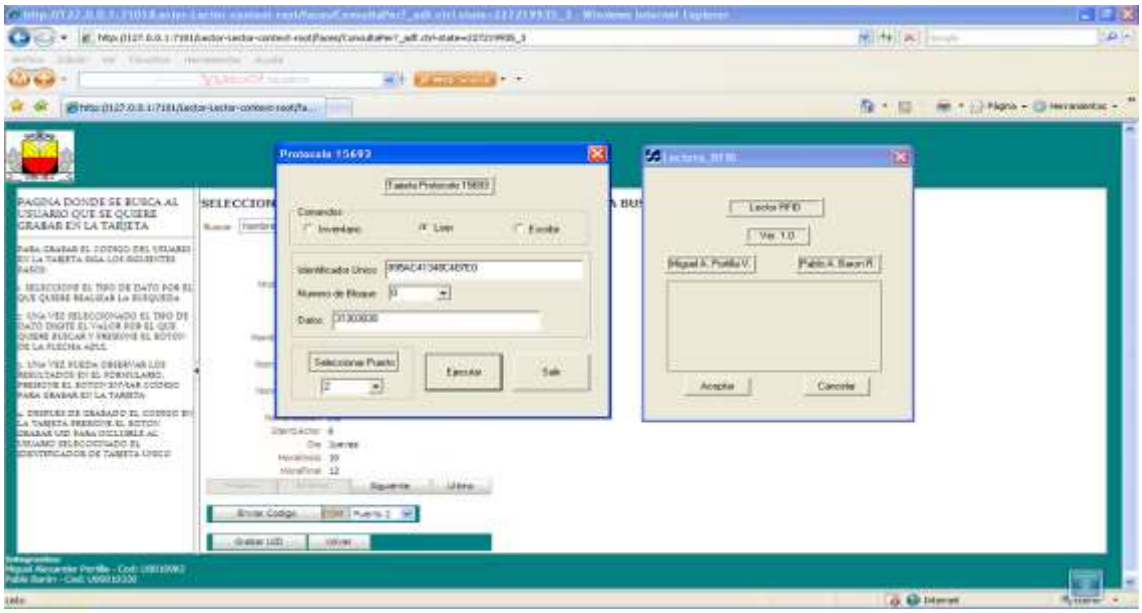
Figura No.86: Funcionamiento Software Administrador Tarjeta RFID - Ejecución función Inventario



Fuente: Diseño Grupo Investigador

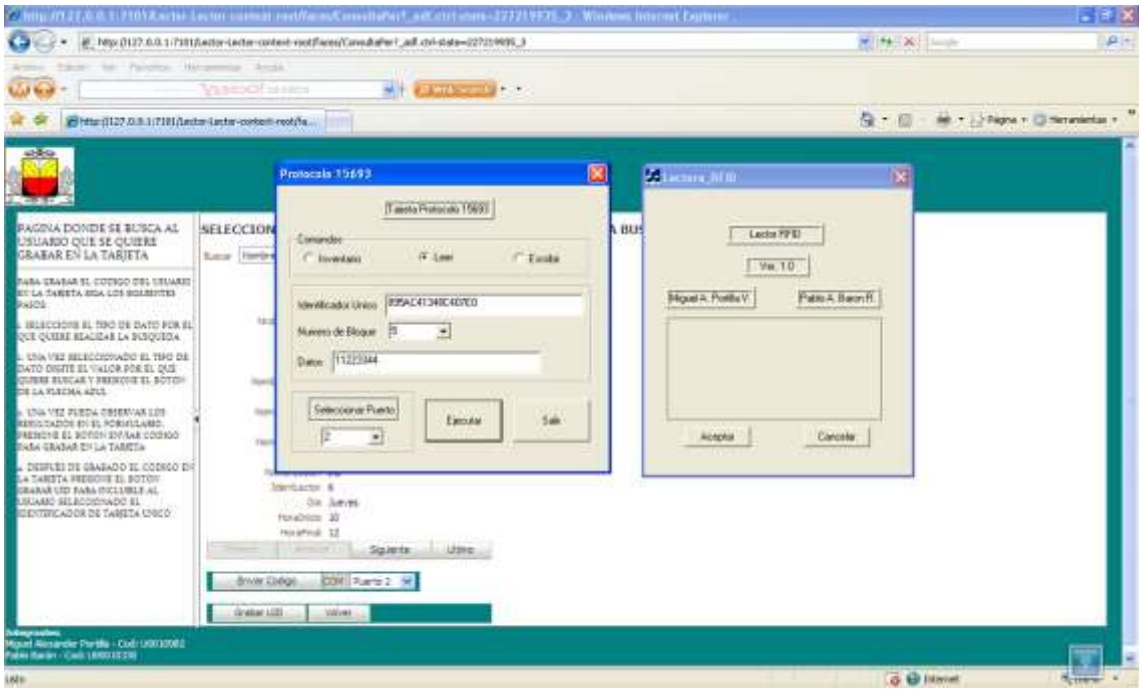
La segunda opción es la concerniente a leer, la cual nos sirve para leer cualquier bloque de la tarjeta, cabe resaltar que todos los datos con los que trabaja este programa estan en formato hexadecimal, a continuación se muestra la lectura de los bloques 0 y 5:

Figura No.87: Funcionamiento Software Administrador Tarjeta RFID Ejecución función Leer



Fuente: Diseño Grupo Investigador

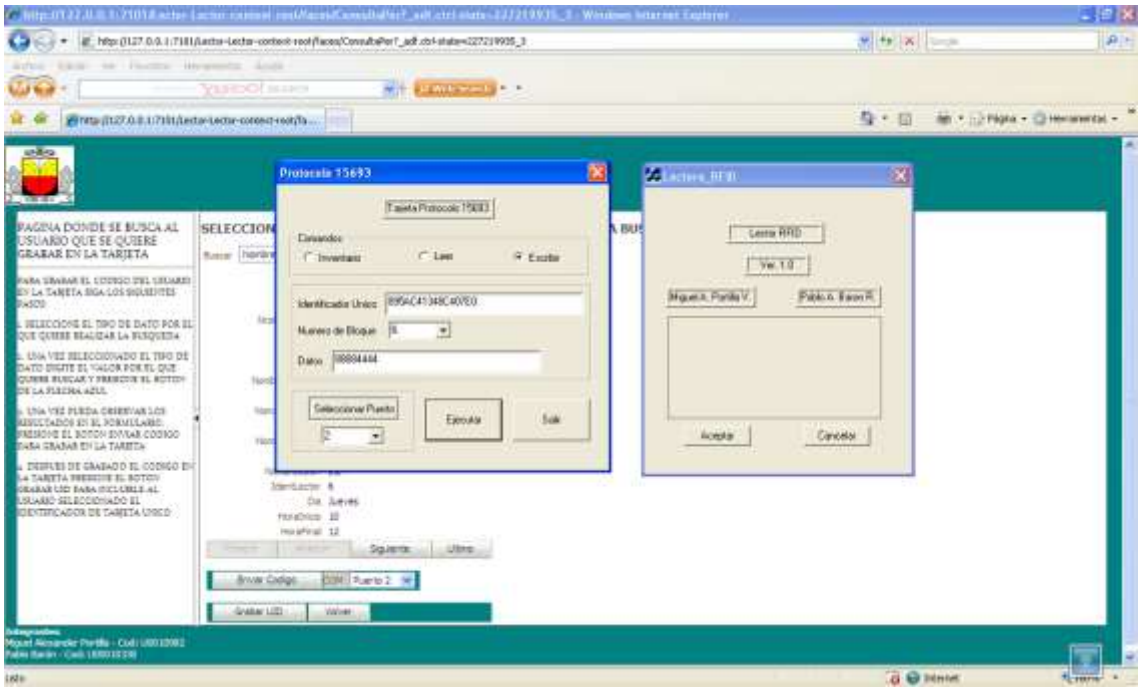
Figura No.88: Funcionamiento Software Administrador Tarjeta RFID Ejecución función Leer



Fuente: Diseño Grupo Investigador

Por ultimo, se tiene la opción de escribir, en la cual podremos escribir cualquier dato en el bloque que se quiera, para este caso se escribieron en el bloque 6 los datos 88884444:

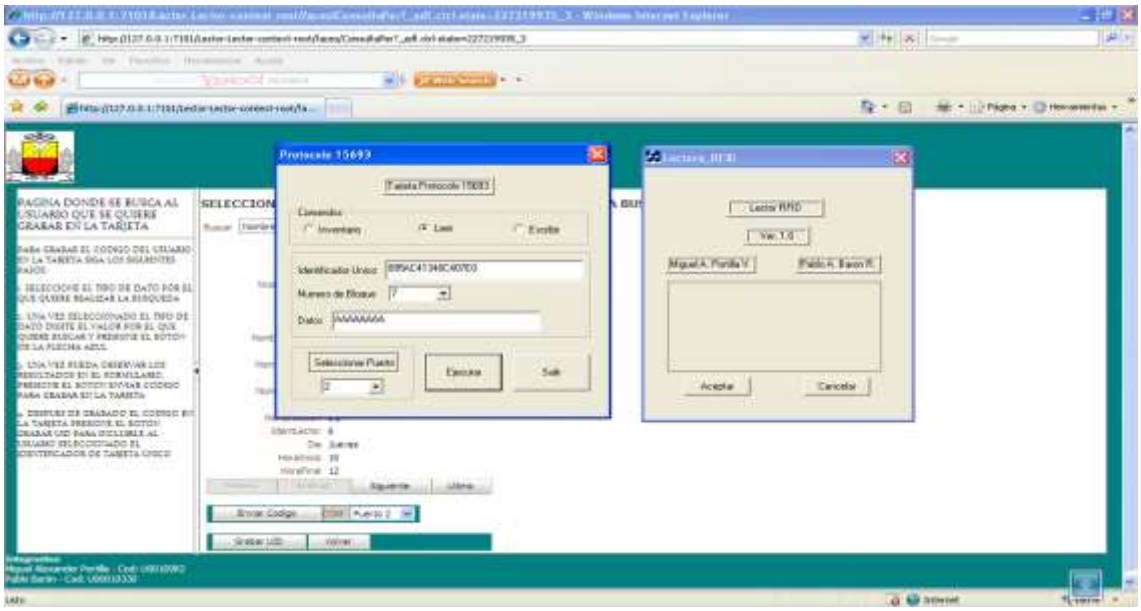
Figura No.89: Funcionamiento Software Administrador Tarjeta RFID Ejecución función Escribir



Fuente: Diseño Grupo Investigador

Despues se procede a leer cualquier otro bloque, por ejemplo el 7 que nos imprime AAAAAAA:

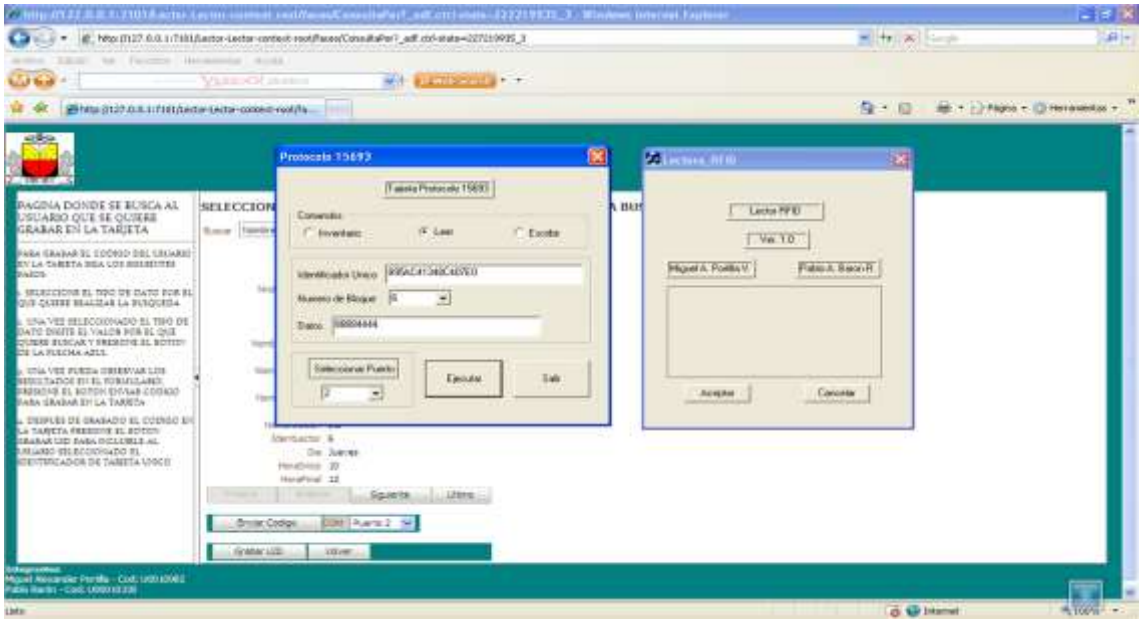
Figura No.90: Funcionamiento Software Administrador Tarjeta RFID Prueba lectura



Fuente: Diseño Grupo Investigador

Y para comfirmar la escritura de los datos en la tarjeta leemos el bloque 6 en el cual fue el que se escribio 88884444:

Figura No.91: Funcionamiento Software Administrador Tarjeta RFID Prueba lectura



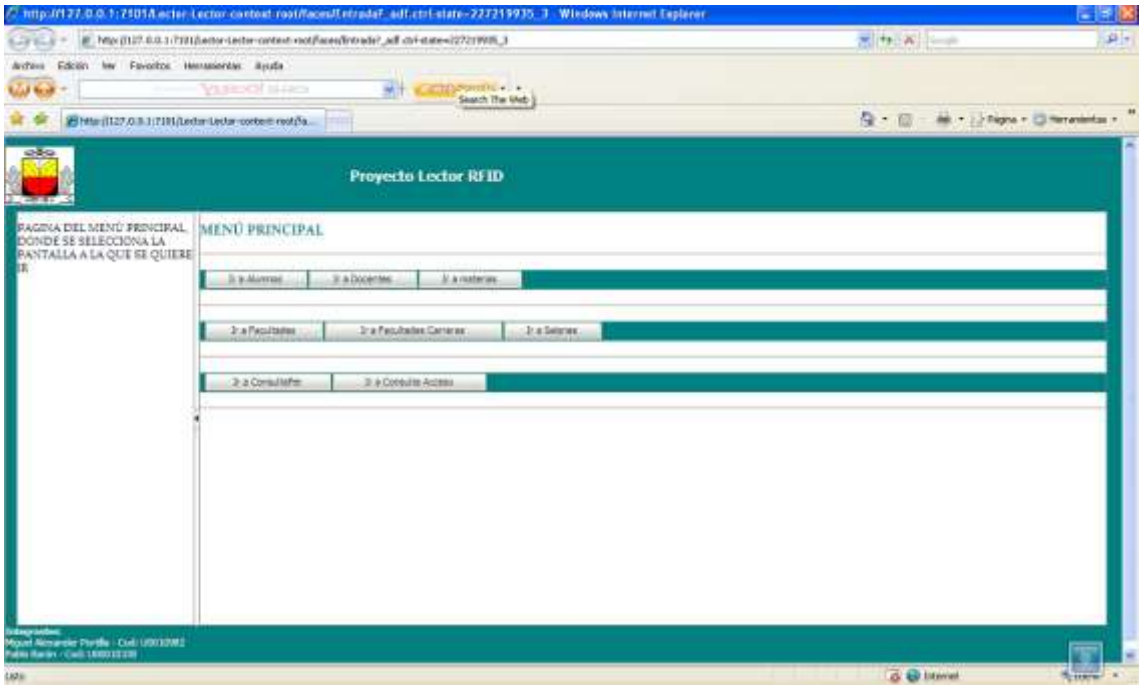
Fuente: Diseño Grupo Investigador

Esta es la manera en que trabaja este software de administrador, el cual debe ser operado solamente por un experto debido a la complejidad de sus funciones.

7.4.2 software Grabar Este software es el que permite realizar la grabación de datos en los carnets de manera automatica, ya que el usuario solo ejecuta dos botones, ademas para su funcionamiento se tienen dos programas que trabajan conjuntamente, uno se desarrollo en C++ y el otro es implementado en JAVA.

Para ejecutar la grabación de los datos, primero se debe acceder a las paginas creadas en JDeveloper 11:

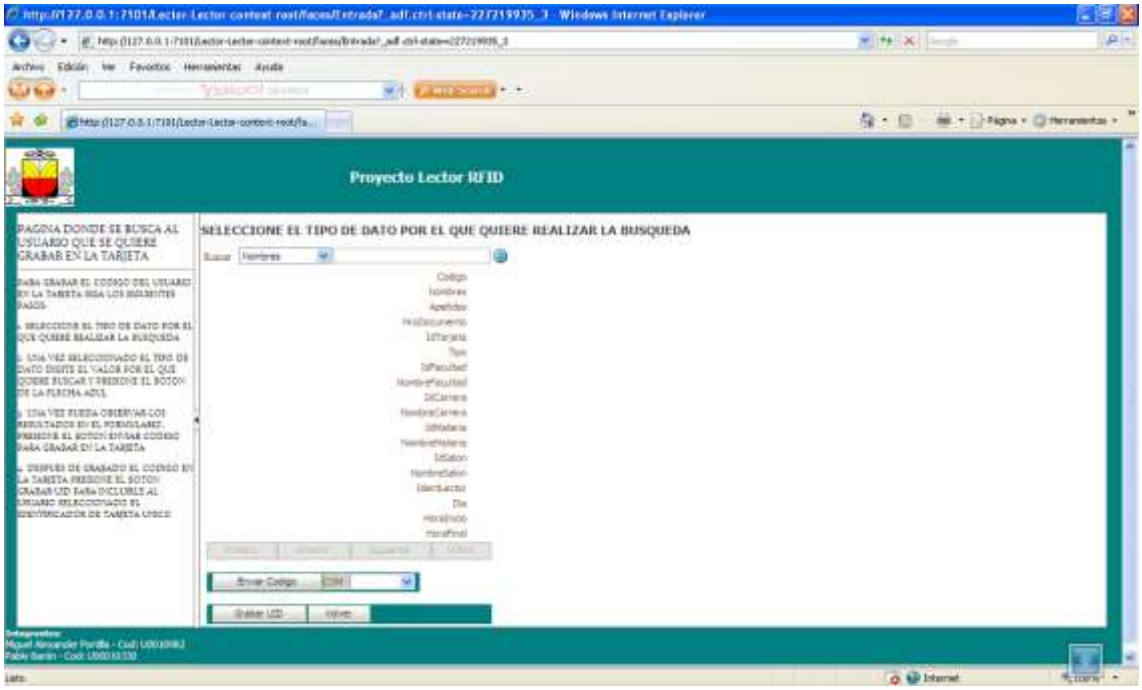
Figura No.92: Funcionamiento Software Grabar Tarjeta RFID Menú principal



Fuente: Diseño Grupo Investigador

Una vez alli, se selecciona la opcion Ir a ConsultaPer, que es donde se pueden observar los datos de todos los usuarios que conforman la base de datos:

Figura No.93: Funcionamiento Software Grabar Tarjeta RFID Búsqueda usuario



Fuente: Diseño Grupo Investigador

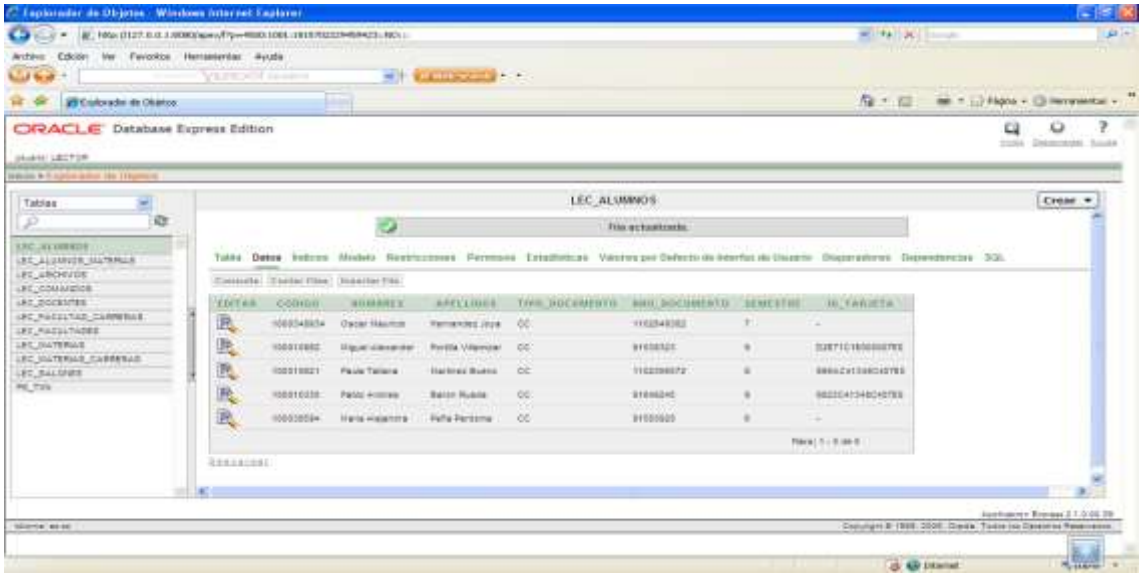
Para este ejemplo se buscaran los datos del alumno Oscar Hernandez, como se ve en la imagen siguiente, es importante resaltar que el campo de IdTarjeta se encuantra vacio, ya que al momento de la grabación este campo se le asignara de manera automatica el UID de la tarjeta que este presente en el lector:

Figura No.94: Funcionamiento Software Grabar Tarjeta RFID Confirmación campo IdTarjeta JDeveloper

Fuente: Diseño Grupo Investigador

En esta imagen se puede apreciar que en la base de datos el campo IdTarjeta al igual que en la página se encuentra vacio:

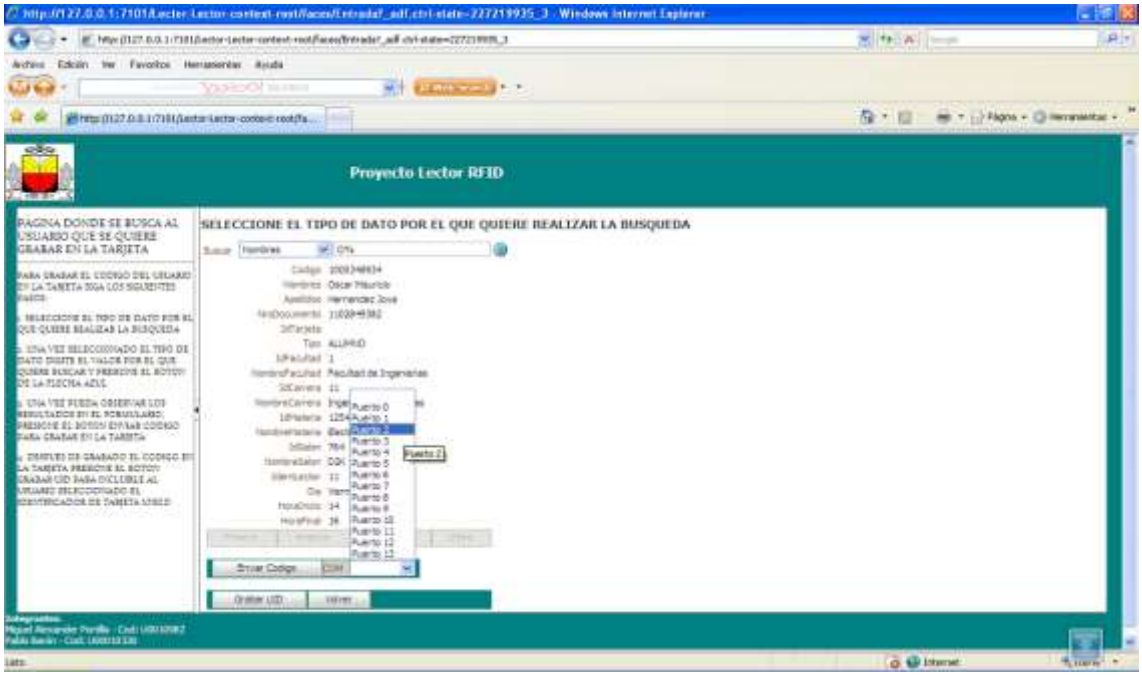
Figura No.95: Funcionamiento Software Grabar Tarjeta RFID Confirmación campo IdTarjeta Oracle



Fuente: Diseño Grupo Investigador

Ahora se procedera a la grabación del codigo del estudiante a la tarjeta, lo primero que se debe hacer es escoger el puerto que para este PC es el 2:

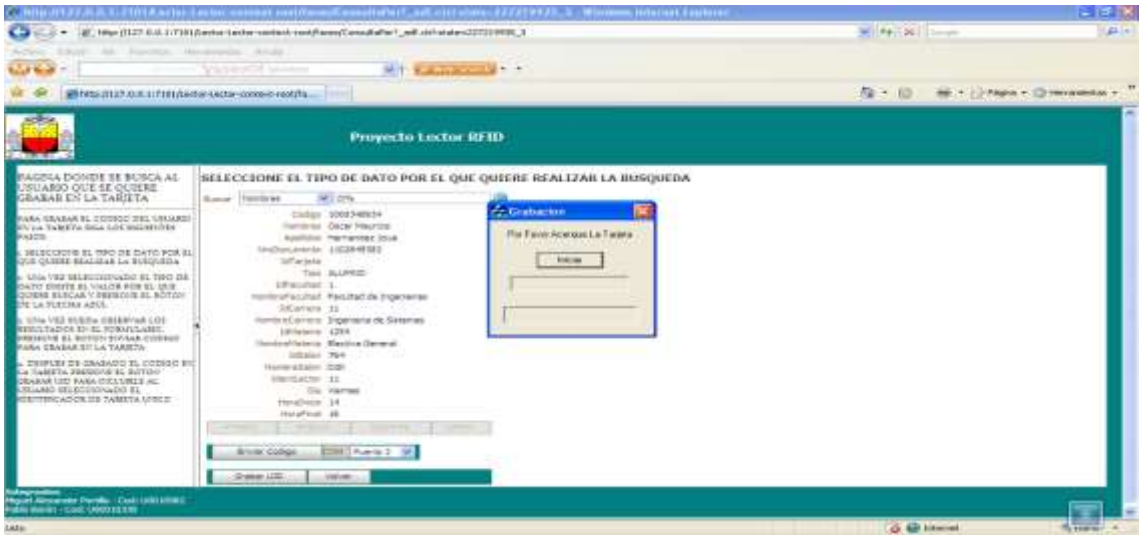
Figura No.96: Funcionamiento Software Grabar Tarjeta RFID Selección de Puerto



Fuente: Diseño Grupo Investigador

Una vez seleccionado el puerto se da click en el boton Enviar Codigo el cual llama al programa en C++ y en este se dara click en el boton Iniciar:

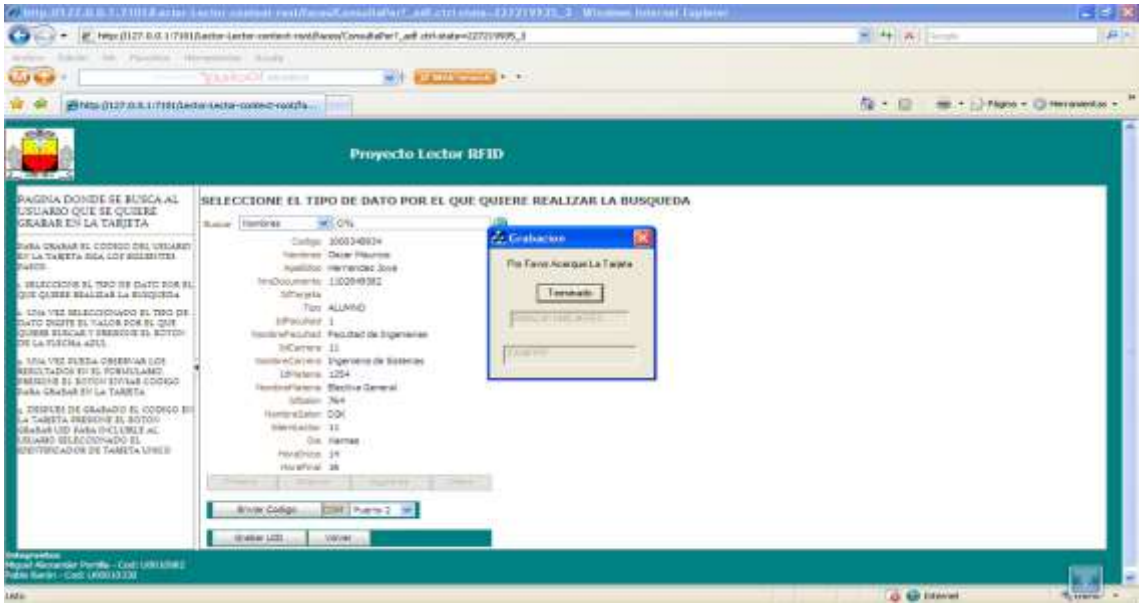
Figura No.97: Funcionamiento Software Grabar Tarjeta RFID Ejecución programa C++



Fuente: Diseño Grupo Investigador

Despues del click en el boton Iniciar, el programa en C++ grabará el codigo del usuario en la trajeta que tenga presente y mostrara en pantalla los datos que envia a la tarjeta, como tambien el boton Iniciar cambiara a Terminado lo que nos indica que el codigo fue grabado con éxito:

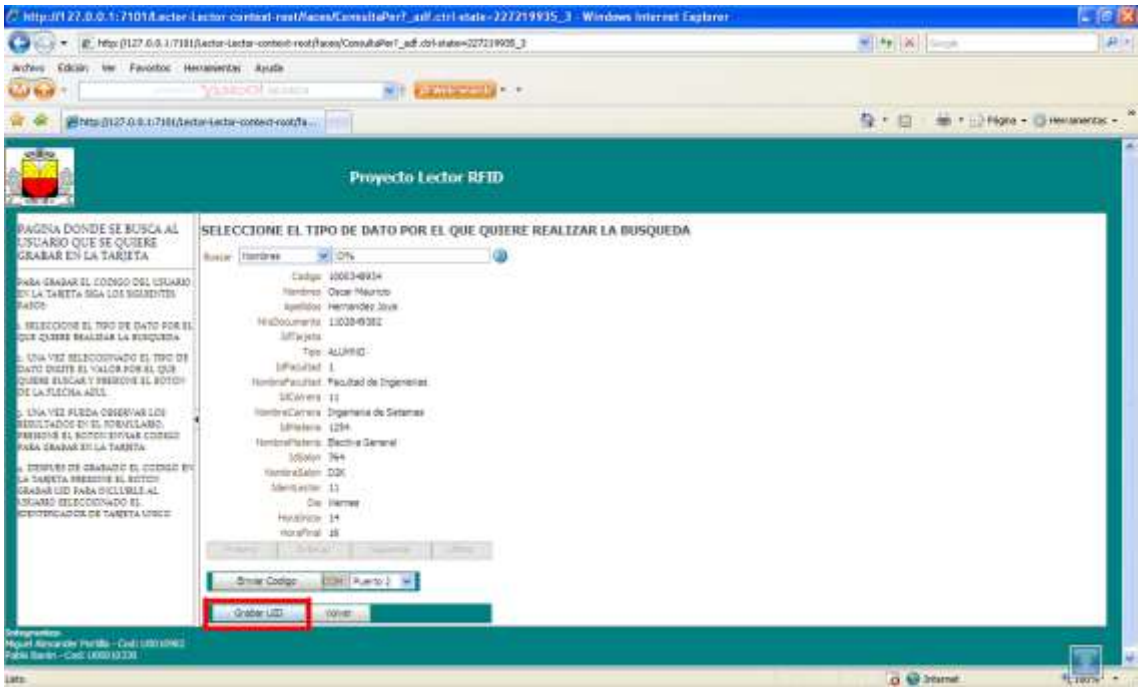
Figura No.98: Funcionamiento Software Grabar Tarjeta RFID Grabación código



Fuente: Diseño Grupo Investigador

Ahora se cierra la aplicación de C++ y volvemos a la pagina donde se da click en el boton Grabar UID, esto se hace para que el programa en JAVA grabe el identificador de la tarjeta a este usuario, esto se hace como mecanismo de protección, para que las tajetas no puedan ser clonadas:

Figura No.99: Funcionamiento Software Grabar Tarjeta RFID Grabación UID al usuario



Fuente: Diseño Grupo Investigador

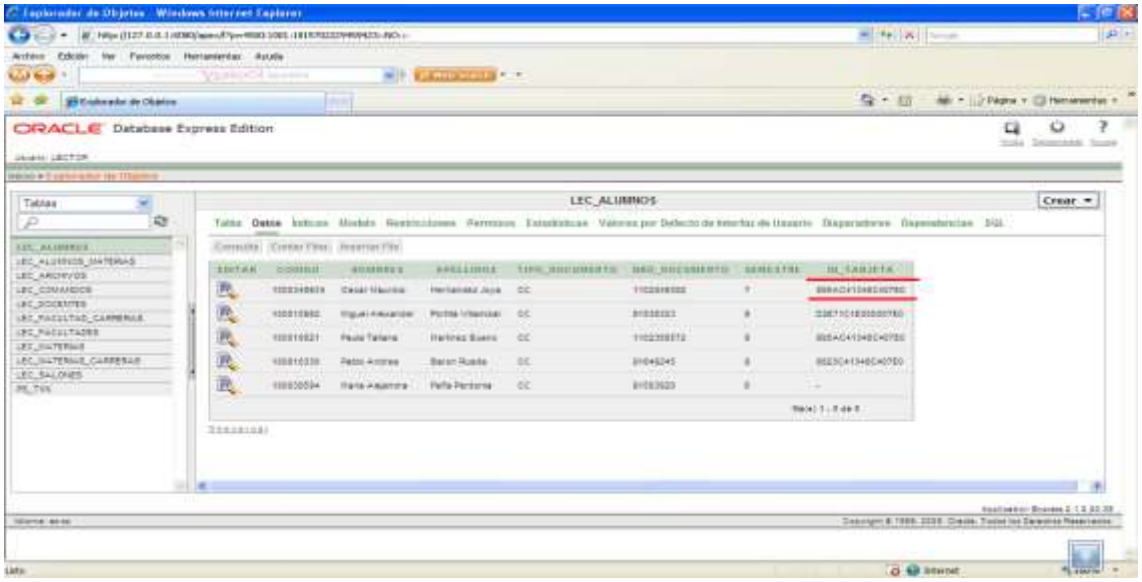
Despues de grabado el UID se procede a realizar una nueva consulta del usuario para verificar que los datos fueron grabados correctamente, como se puede observar en la imagen el UID de la tarjeta fue asignado al usuario Oscar Hernandez:

Figura No.100: Funcionamiento Software Grabar Tarjeta RFID Confirmación grabación UID JDeveloper

Fuente: Diseño Grupo Investigador

Luego vamos a confirmar la grabación de los datos en la base de datos y vemos que efectivamente el usuario Oscar Hernandez ya posee un UID:

Figura No.101: Funcionamiento Software Grabar Tarjeta RFID Confirmación grabación UID Oracle



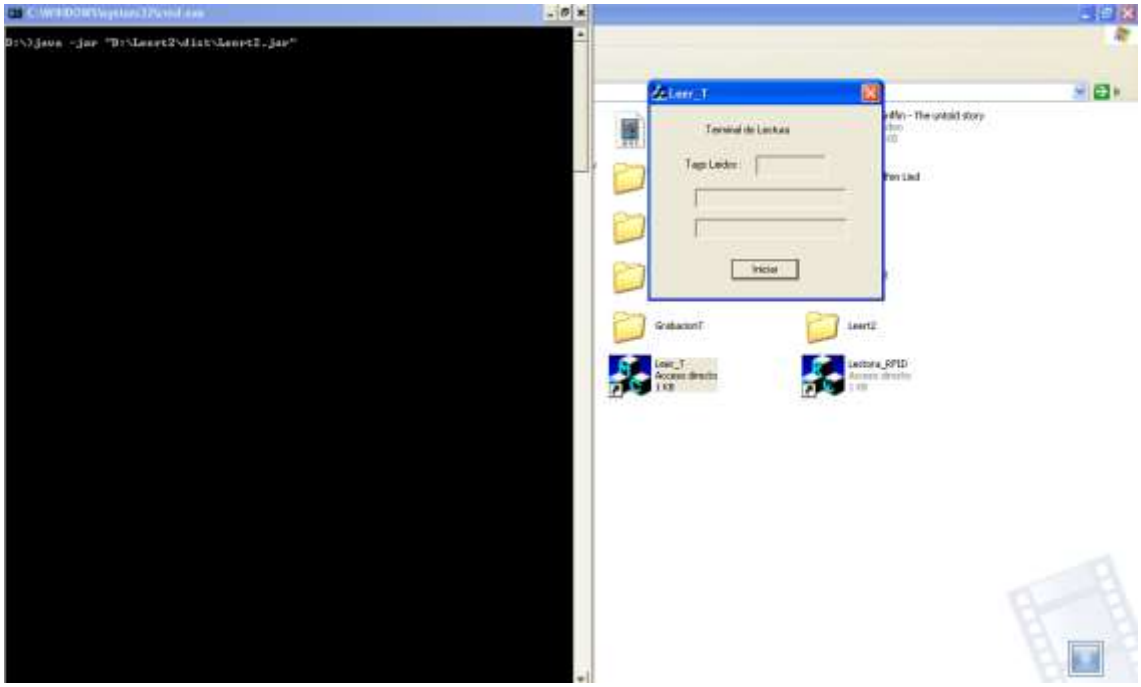
Fuente: Diseño Grupo Investigador

Estos son los pasos que se deben seguir para realizar la grabación de los datos de cualquier usuario al que se le quiera asignar una tarjeta.

7.4.3 software Leer Para la realización de esta funcion al igual que para la grabación tambien se desarrollaron dos programas (uno en C++ y otro en JAVA) que trabajan de manera conjunta y que permiten que la lectura de los tags se realice de manera automatica.

Primero se ejecuta el programa en C++, el cual sera el que leera los datos de la tarjeta y los enviara al programa en JAVA el cual los comparara con los de la base de datos y asi validar o negar la entrada del usuario, para este caso se creo un ejecutable de JAVA (pantalla negra) que nos imprimira en pantalla el estado de usuario:

Figura No.102: Funcionamiento Software Leer Tarjeta RFID Ejecución programa



Fuente: Diseño Grupo Investigador

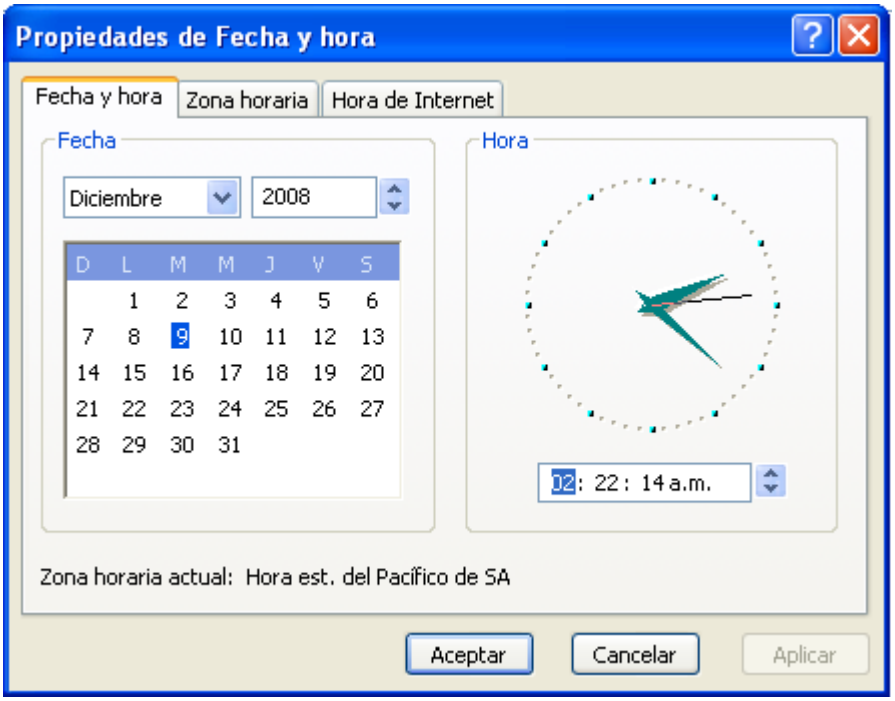
Antes de empezar con la lectura de los datos se tiene que asignar la hora y el dia en el PC, para ver si el usuario posee permiso para la clase, para el ejemplo se tienen los usuarios:

Alumno: Miguel Portilla Cód. 100010982
Horario Martes 2-4
ID Lector: Lector 1

Alumno: Oscar Hernández Cód. 1000348934
Horario: Viernes 2-4
ID Lector: Lector 11

La hora asignada al pc sera 2:22 p.m y el dia sera martes, lo que nos dira que el usuario miguel portilla tiene acceso y oscar hernandez no.

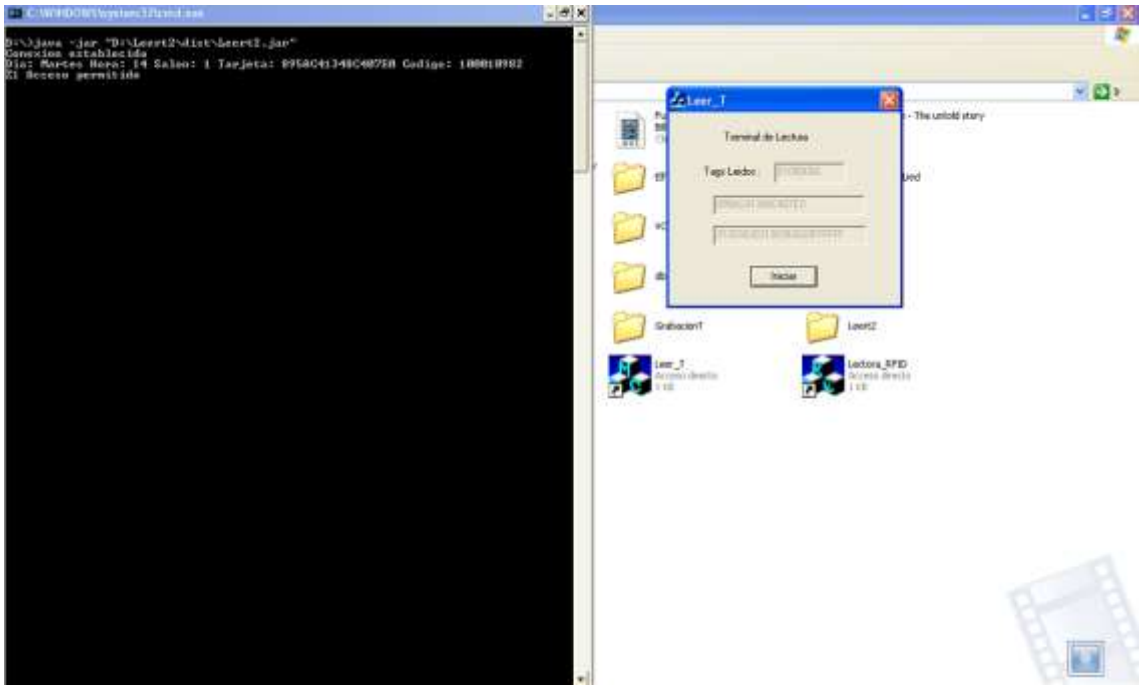
Figura No.103: Funcionamiento Software Leer Tarjeta RFID Asignar Día y Hora



Fuente: Diseño Grupo Investigador

Despues de asignada la hora y el dia se procedera a la lectura de los tags, para esto se ejecuta el boton Iniciar, despues de la comparación se mostrara en pantalla el resultado de la lectura:

Figura No.104: Funcionamiento Software Leer Tarjeta RFID Iniciar proceso grabación



Fuente: Diseño Grupo Investigador

Para el ejemplo como ya se explico anteriormente se tienen dos usuarios, que fueron leidos en el siguiente orden:

Miguel Portilla

Codigo: 100010982

UID: 895BC41348C407E0

Estado: Acceso Permitido

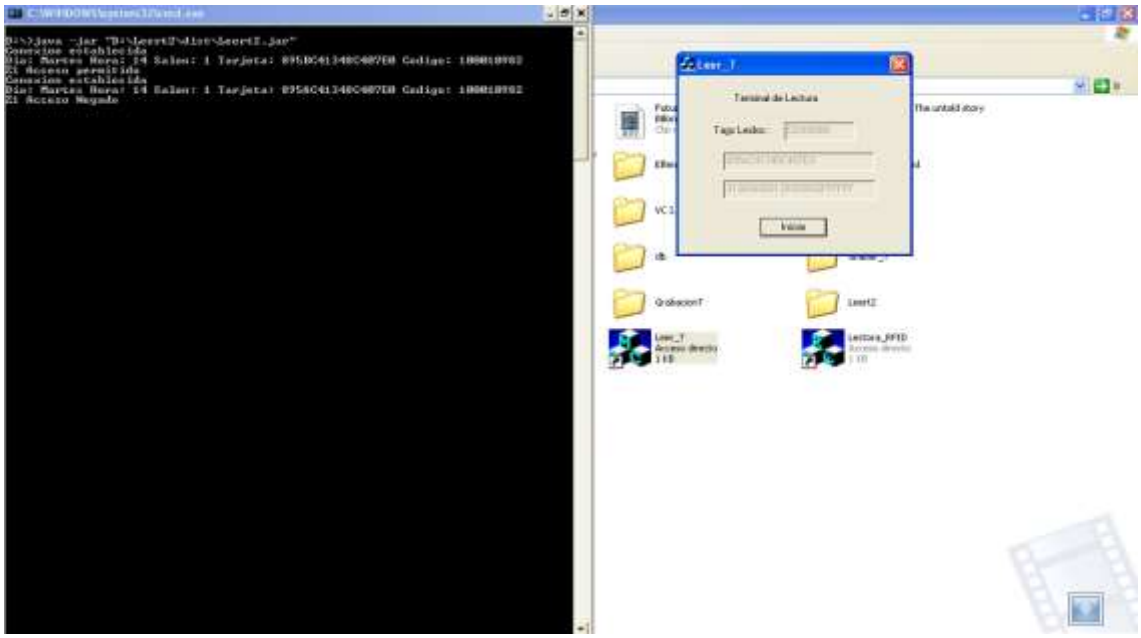
Oscar Hernadez

Codigo: 1000348934

UID: 895AC41348C407E0

Estado: Acceso Negado

Figura No.105: Funcionamiento Software Leer Tarjeta RFID Estado del acceso del usuario



Fuente: Diseño Grupo Investigador

De esta manera se realiza la lectura de tarjetas de los usuarios, para verificar el acceso a las aulas de la Universidad.

8. PROYECCIÓN FUTURA

Teniendo en cuenta la premura del tiempo y el trabajo realizado por el grupo investigador, el cual permitió que las experiencias vividas dentro del trabajo de campo se desarrollaran dos tecnologias diferentes (Tarjetas Inteligentes y RFID), pero que en la primera por la carencia de informacion y la perdida del manual de procedimientos no se pudo conseguir la clave que permitiera la lectura y escritura de las tarjetas inteligentes, pero al realizar la practica en la empresa (Grupo Cóndor) se trabajo con la segunda tecnologia (RFID), permitiendo llevar con éxito el trabajo y colocar en funcionamiento el prototipo.

Se deja en proyección para un futuro la instalación del prototipo con el fin de que los estudiantes de Ing. de Sistemas, Ing. Mecatronica de cursos inferiores, empleados de la UNAB ó alguna compañía realicen esta actividad para contrubuir con la evolución de la Universidad hacia el mejoramiento de sus instalaciones y mejorar el servicio a sus usuarios.

El software desarrollado para el funcionamiento del prototipo es de exclusividad del grupo investigador por lo tanto sugerimos a los usuarios que quieran manipularlo ó utilizarlo, comunicarse con el grupo investigador para su permiso, para el cual se dejan en disposición los correos: miguel_porty@hotmail.com y beast977@hotmal.com.

CONCLUSIONES

1. La realización de este programa que significaba establecer “un prototipo de control de acceso funcional” para la comunidad educativa “UNAB”, permitió que cada uno de los productos obtenidos se convirtieran en la base prioritaria para definir todos los procesos tecnológicos que apoyaron el desarrollo y cumplimiento de los objetivos trazados en el proyecto.

2. La transformación del proyecto, se orienta bajo los fundamentos teóricos y metodológicos diseñados con destino a la facultad de ingeniería de sistemas pero para responder a ellos, se tuvo en cuenta 4 dimensiones que permitieron la exploración y el trabajo de campo como el desarrollo definitivo de cada tarea o actividad dentro de la programación.

2.1 Dimensión Organizacional: en esta dimensión fue fundamental el apoyo del Ing. Director del proyecto, del Ing. Asesor y los Ing. Evaluadores como el interés investigativo del grupo de trabajo donde se identificaron y documentaron los diferentes ajustes requeridos en los procesos administrativos y académicos para la implementación.

2.2 Dimensión Pedagógica: en el campo curricular se revisaron y orientaron las políticas del saber hacer hacia el modelo pedagógico del programa, preparando los lineamientos para el diseño de los guiones de aprendizaje que orientan la construcción de los materiales de estudio y encontrar el verdadero modelo de diseño como fue el RFID.

2.3 Dimensión Tecnológica: partiendo de las excelentes condiciones infraestructurales con que cuenta la institución, el proyecto contribuye a la modernización técnica y de control de acceso que permite una funcionalidad rápida en el uso de las aulas porque cada usuario debe adquirir una tarjeta que le sirva de carnet o de identificación y al mismo tiempo de acceso a la aulas por lo tanto, se hace necesario continuar con la “proyección futura” donde queda a disposición todos los mecanismos de instalación y puesta en funcionamiento.

2.4 Dimensión Comunicativa: se construyeron los lineamientos de comunicación que van desde los aspectos globales de divulgación hasta lo más especifico de producción de materiales educativos digitales que facilitaron la conexión con otras empresas que fueron el pilar fundamental para la implantación del programa y el desarrollo de los diferentes accesorios que se necesitaban para su ejecución como también fue actor fundamental la biblioteca con su apoyo para producir y disponer los recursos digitales y escritos de los diferentes sistemas.

3. El ejercer y querer la Ingeniería de Sistemas es algo que dignifica al ser humano “El Ingeniero” que ha elegido en su culturización avanzada esta profesión, tanto científica como técnica con el fin de continuar profesionalmente esta noble tarea para innovar y solucionar los diferentes conflictos globalizantes de cambio que a cada instante en forma virtual se presentan dentro de este mundo contemporáneo de sistemas y tecnología

BIBLIOGRAFIA

[1] DREIFUS, Henry, Smart cards: a guide to building and managing smart card applications, 1998, John Wiley & Sons, New York.

[2] GUTHERY, Scott B, Smart card developer's kit, 1998, MacmillianTechnical Publishing, Indianapolis.

[3] RANKL, W, Smart card handbook, 1997, John Wiley & Sons, Chichester.

[4] TAPIADOR, Mateos, Marino y otro, Tecnologías Biométricas Aplicadas a la Seguridad, 2005, Alfa omega Grupo Editor, S.A de C.V, México D.F.

[5] UK Biometrics Working Group, Use of Biometric for Identification and Authentication Advice on Product Selection. Issue 2.0, Marzo 2002.

[6] Wikipedia, ISO 7816, http://es.wikipedia.org/wiki/ISO_7816, Mayo 2008.

[7] Acces Control Systems & Software, http://www.es.tensor.co.uk/docs/access-control.htm, Abril 2008

[8]Monografías, http://www.monografias.com/trabajos43/biometria/biometria2.shtml, Agosto 2008

[9] Homini, http://www.homini.com/new_page_5.htm, Mayo 2008

ANEXOS

Anexo 1: Diagramas de Flujos de Datos Software Usuario

Nivel 0: Acceso al Usuario

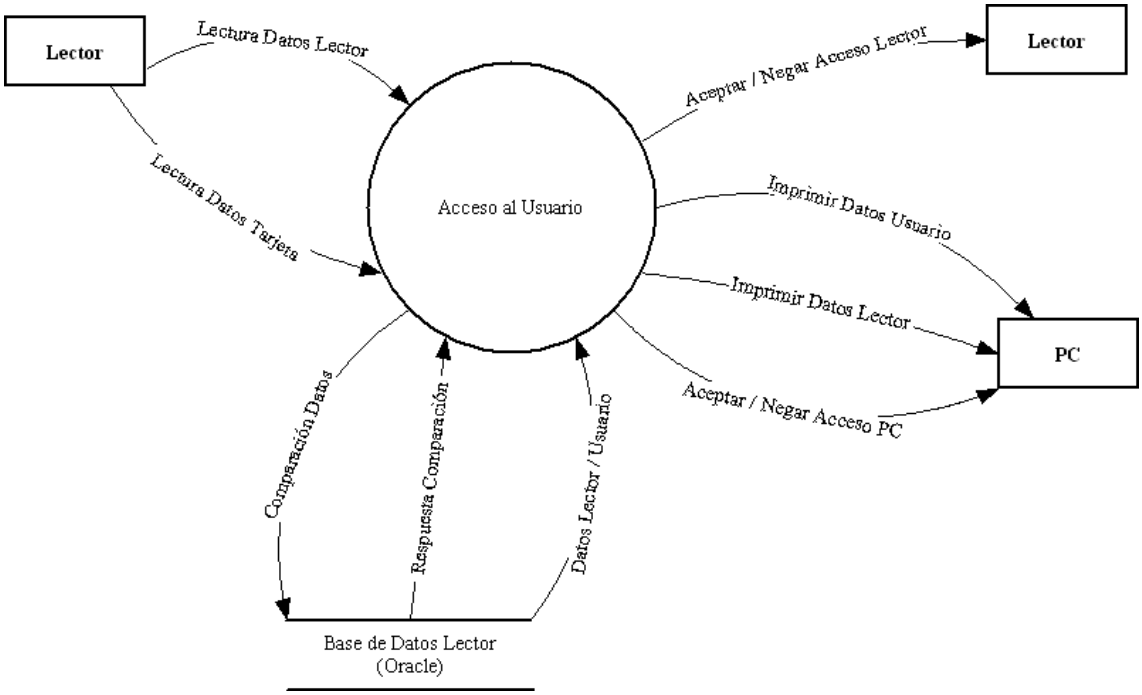


Figura No.106: DFD Tarjeta Chip Software Usuario Nivel 0

Nivel 1: 1. Lectura Datos

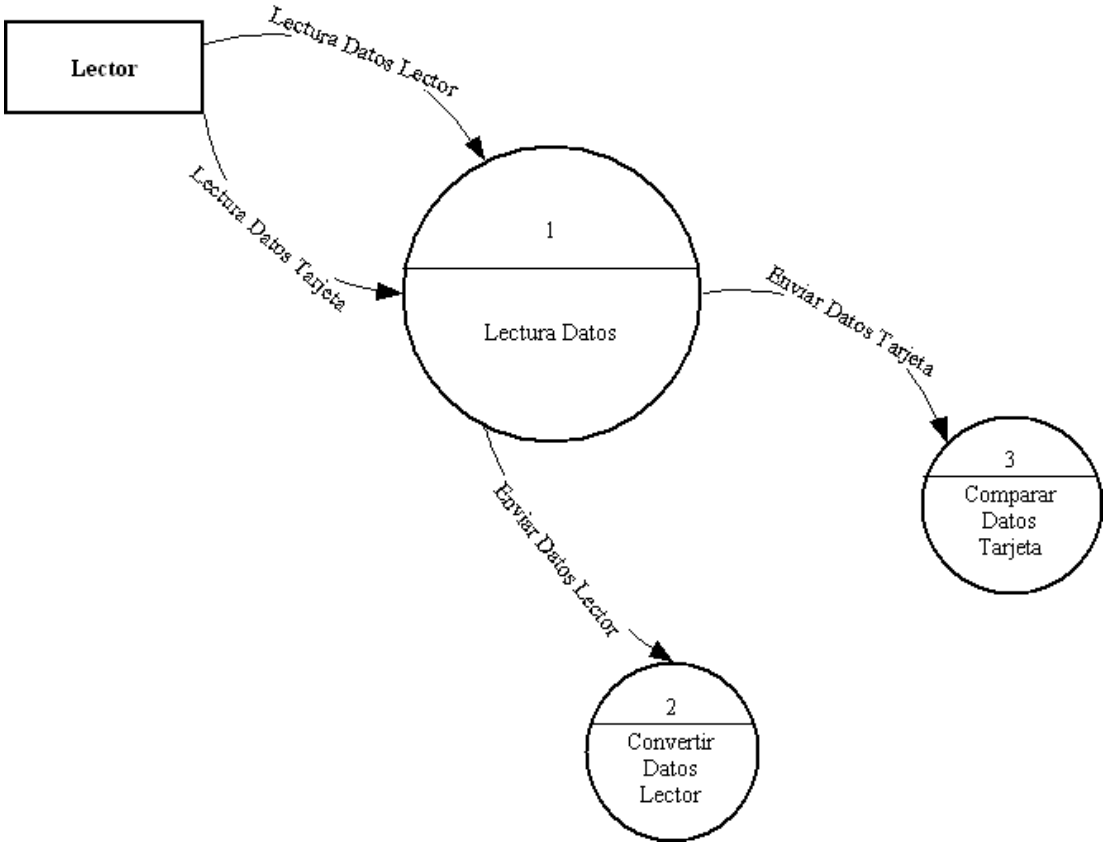


Figura No.107: DFD Tarjeta Chip Software Usuario Nivel 1 (Lectura Datos)

Nivel 1: 2. Convertir Datos Lector

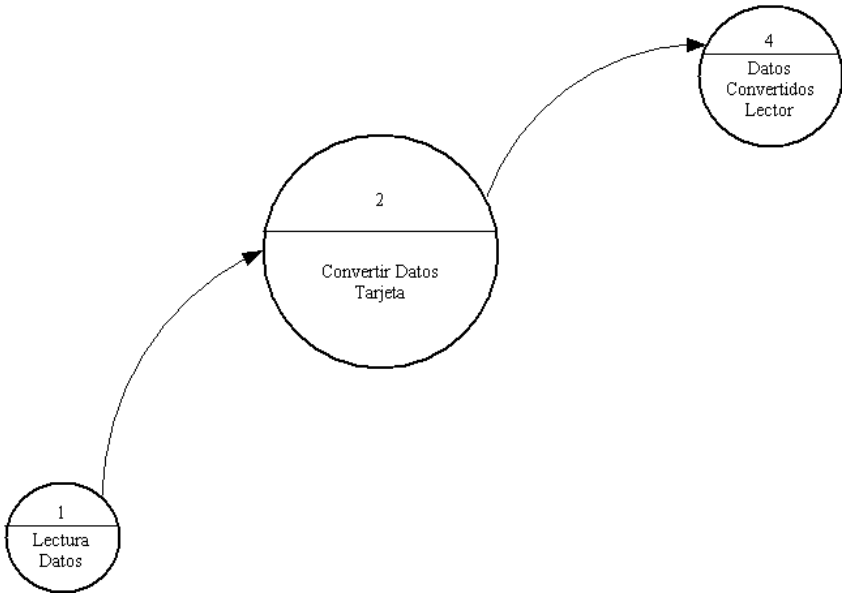


Figura No.108: DFD Tarjeta Chip Software Usuario Nivel 1 (Convertir Datos Tarjeta)

Nivel 1: 3. Comparar Datos Tarjetas

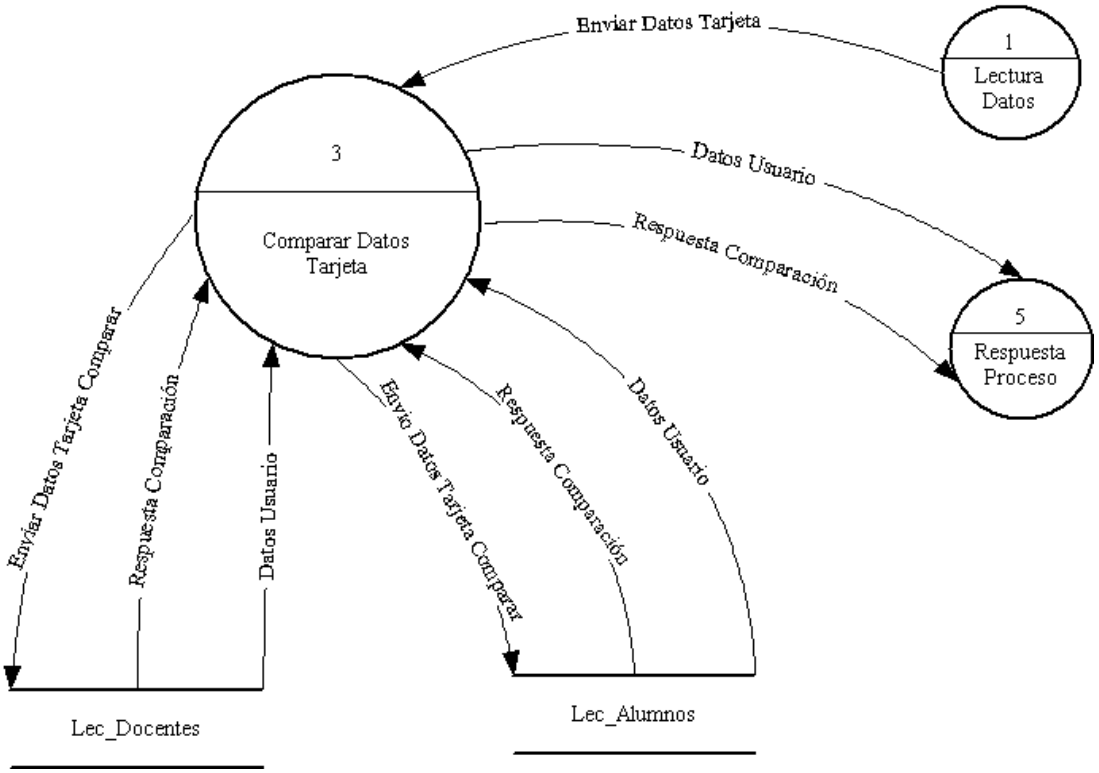


Figura No.109: DFD Tarjeta Chip Software Usuario Nivel 1 (Comparar Datos Tarjeta)

Nivel 1: 4. Datos Convertidos Lector

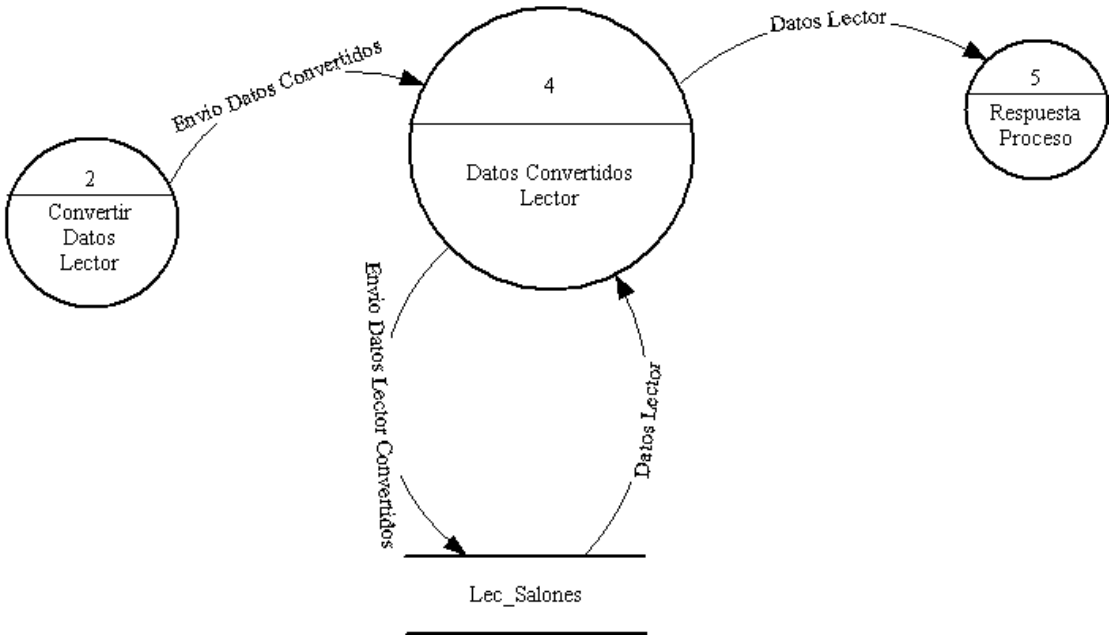


Figura No.110: DFD Tarjeta Chip Software Usuario Nivel 1 (Datos Convertidos Lector)

Nivel 1: 5. Respuesta Proceso

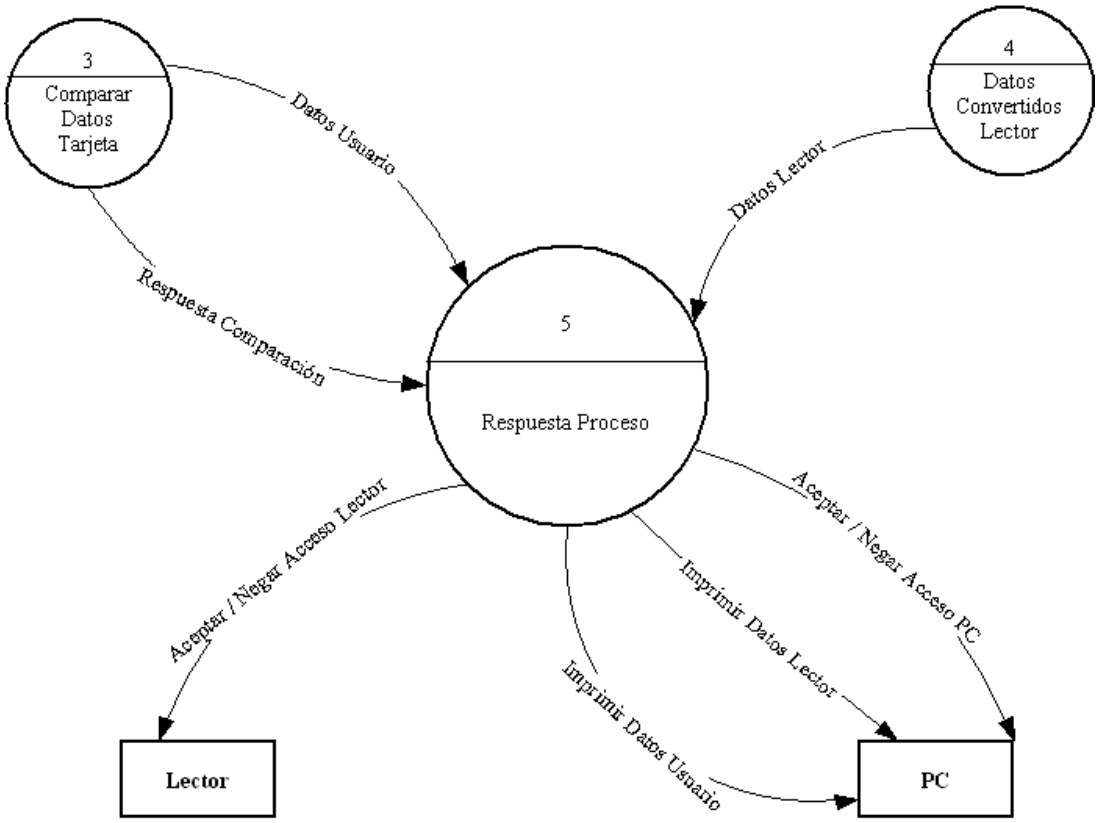


Figura No.111: DFD Tarjeta Chip Software Usuario Nivel 1 (Respuesta Proceso)

Nivel 2: 5.1 Respuesta Negativa Proceso

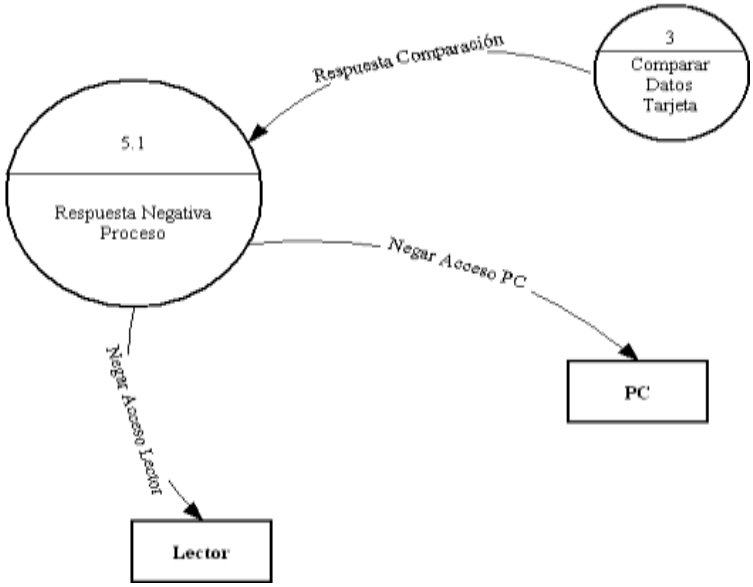


Figura No.112: DFD Tarjeta Chip Software Usuario Nivel 2 (Respuesta Negativa Proceso)

Nivel 2: 5.2 Respuesta Positiva Proceso

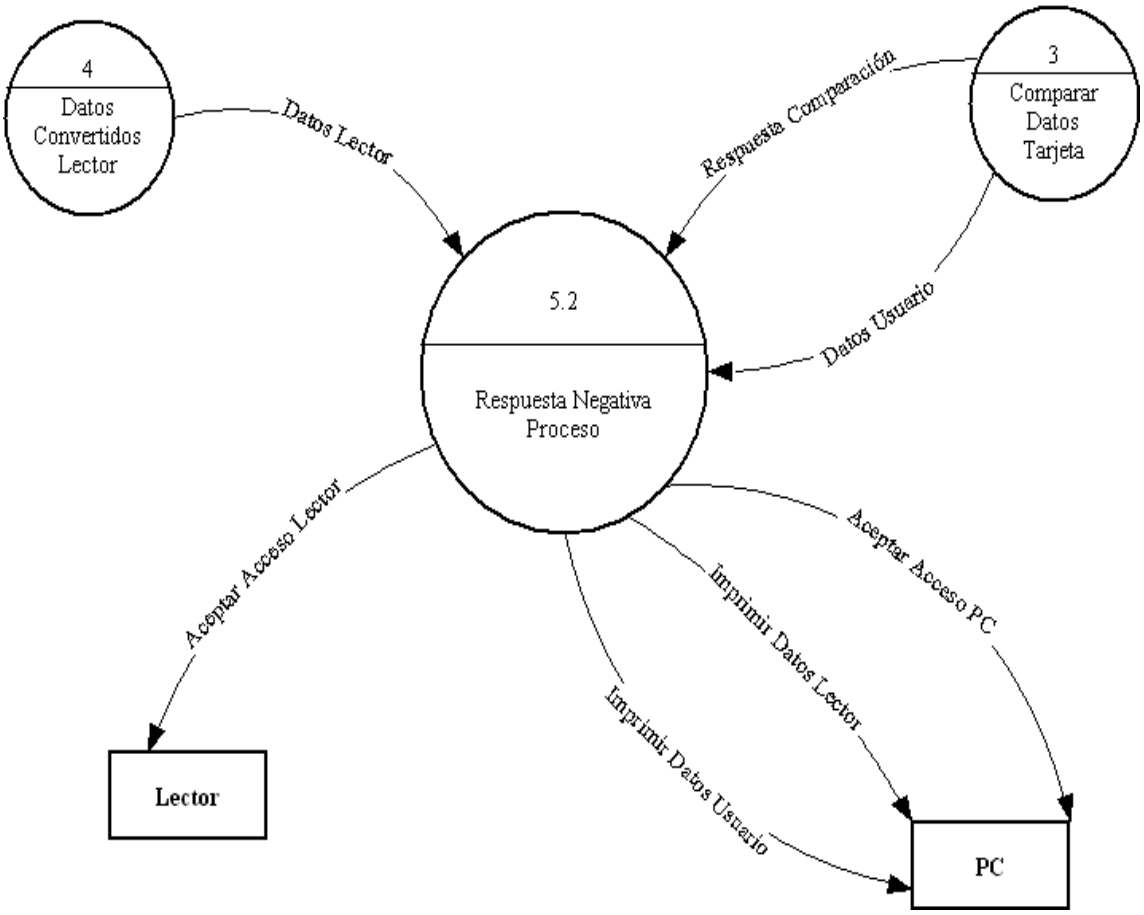


Figura No.113: DFD Tarjeta Chip Software Usuario Nivel 2 (Respuesta Positiva Proceso)

Anexo 2: Diagramas de Flujos de Datos Software Administrador

Nivel 0: Manejo de Datos Usuario

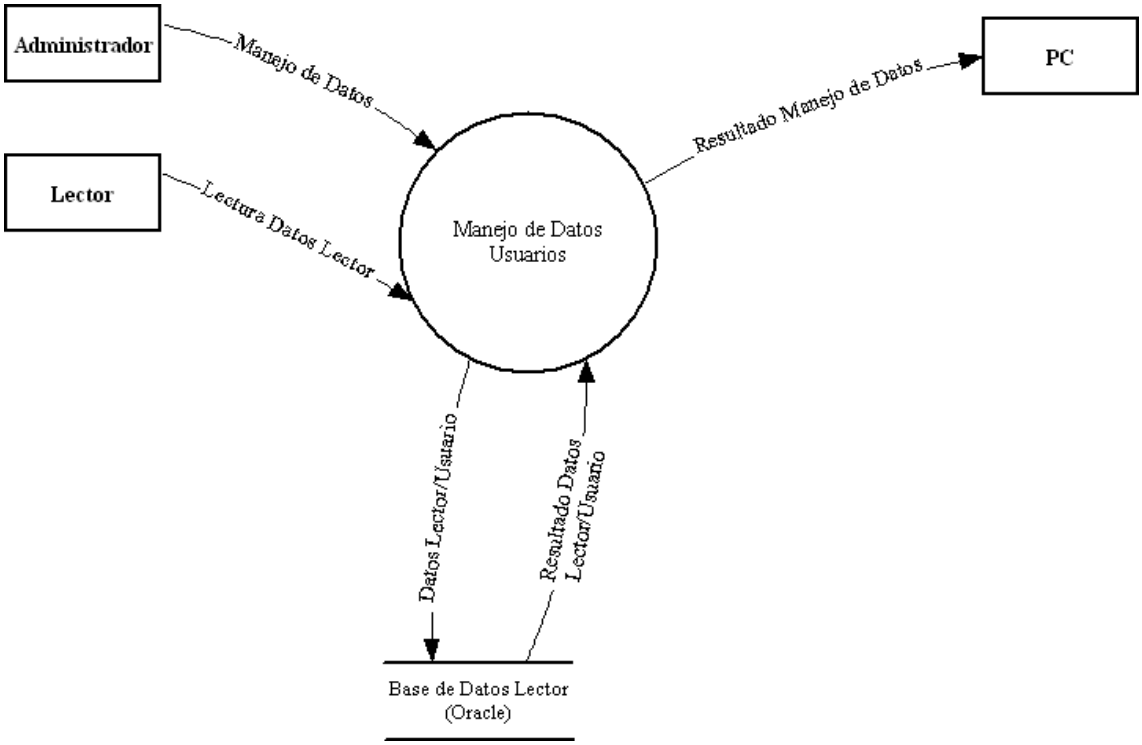


Figura No.114: DFD Tarjeta Chip Software Administrador Nivel 0

Nivel 1: 1. Leer Datos Lector

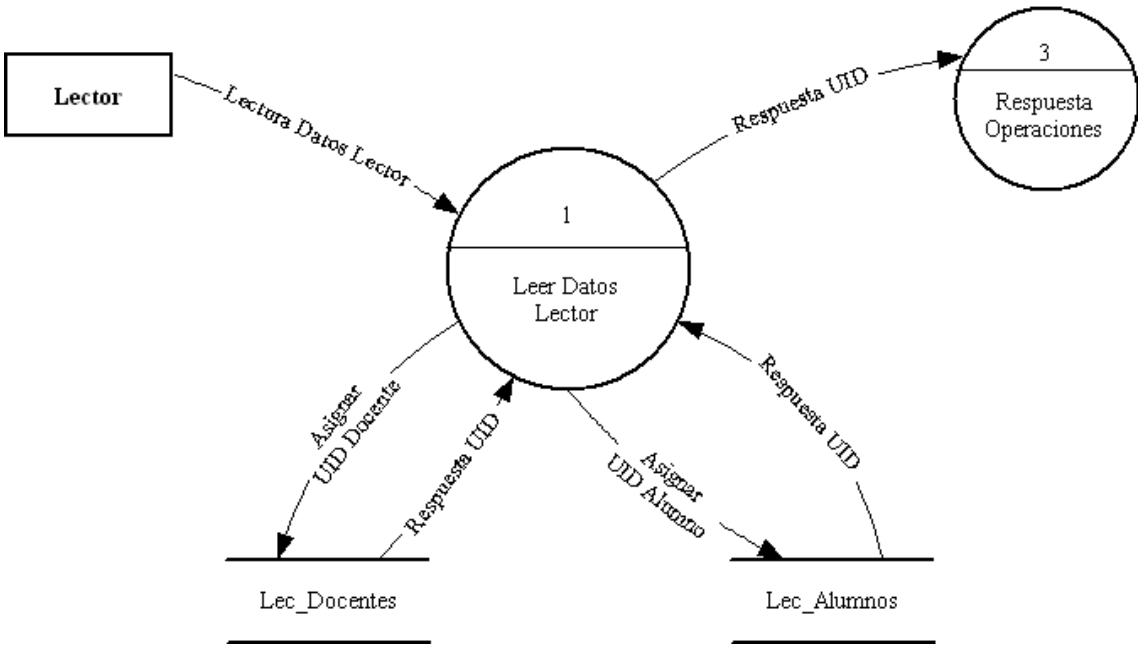


Figura No.115: DFD Tarjeta Chip Software Administrador Nivel 1 (Leer datos lector)

Nivel 1: 2. Administración Datos Usuario

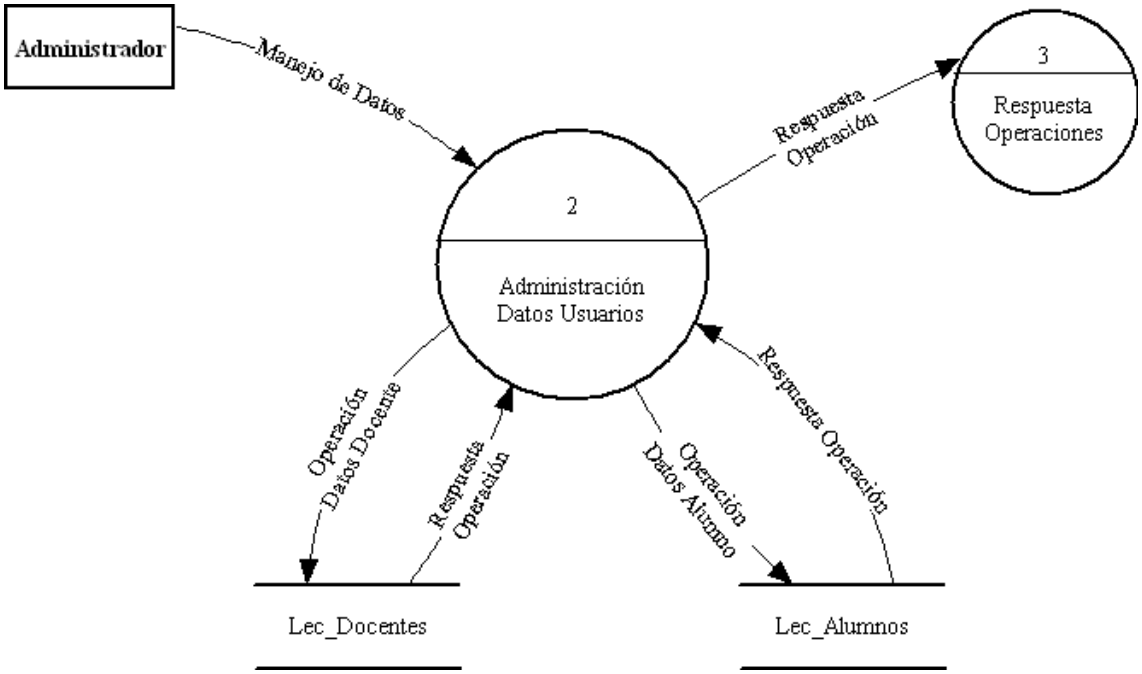


Figura No.116: DFD Tarjeta Chip Software Administrador Nivel 1 (Administración datos usuario)

Nivel 1: 3. Respuesta Operaciones

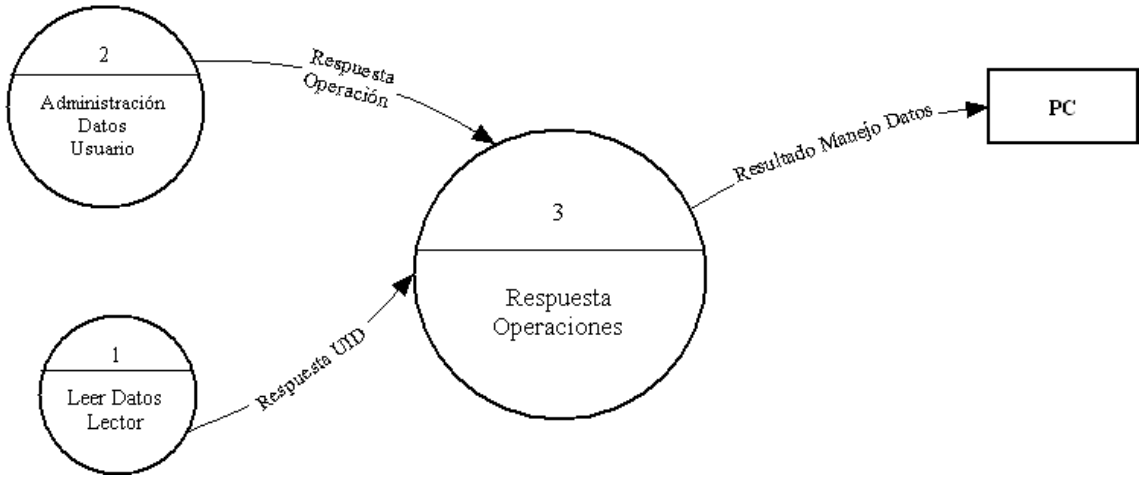


Figura No.117: DFD Tarjeta Chip Software Administrador Nivel 1 (Respuesta operaciones)

Nivel 2: 2.1 Leer, Agregar, Eliminar Datos

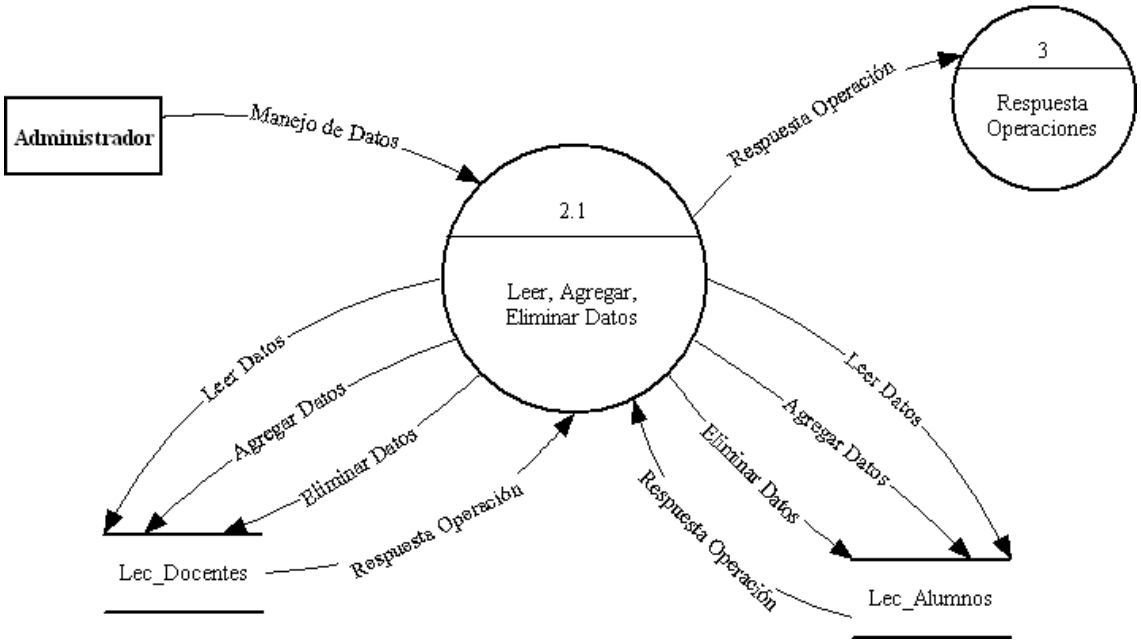


Figura No.118: DFD Tarjeta Chip Software Administrador Nivel 2 (Leer, agregar, eliminar datos)

Anexo 3: Flujos de Datos Software Usuario

NIVEL 0.

Nombre:	Lectura Datos Lector
Descripción:	Características del lector, identificador, ATR
Origen:	Agente Externo (Lector)
Destino:	Proceso (Acceso al Usuario)
Almacenamiento:	Lec_Salones

Nombre:	Lectura Datos Tarjeta
Descripción:	Datos del usuario dueño de la tarjeta (Ej. Código)
Origen:	Agente Externo (Lector)
Destino:	Proceso (Acceso al Usuario)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Nombre:	Aceptar /Negar acceso Lector
Descripción:	Permite o niega el acceso al usuario
Origen:	Proceso (Acceso al Usuario)
Destino:	Agente Externo (Lector)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Nombre:	Imprimir Datos Usuario
Descripción:	Imprime en pantalla los datos del usuario que usa el dispositivo
Origen:	Proceso (Acceso al Usuario)
Destino:	Agente Externo (PC)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Nombre:	Imprimir Datos Lector
Descripción:	Imprime las características del lector usado
Origen:	Proceso (Acceso al Usuario)
Destino:	Agente Externo (PC)
Almacenamiento:	Lec_Salones

Nombre:	Aceptar/Negar acceso PC
Descripción:	Imprime en pantalla si acepta el acceso (cuadro verde) ó si niega el acceso (cuadro rojo)
Origen:	Proceso (Acceso al Usuario)
Destino:	Agente Externo (PC)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Nombre:	Respuesta Comparación
Descripción:	Envía la respuesta de la comparación entre el Dato del usuario contenido en la tarjeta con el de la base de datos
Origen:	Lec_Docentes ó Lec_Alumnos
Destino:	Proceso (Acceso al Usuario)

Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Datos Lector
Descripción: Trae los datos del lector desde la base de datos
Origen: Lec_Salones
Destino: Proceso (Acceso al Usuario)
Almacenamiento: Lec_Salones

Nombre: Datos Usuario
Descripción: Trae los datos del usuario desde la base de datos
Origen: Lec_Alumnos ó Lec_Docentes
Destino: Proceso (Acceso al Usuario)
Almacenamiento: Lec_Alumnos ó Lec_Docentes

Nombre: Comparación Datos
Descripción: Compara los datos del usuario con los de la base de datos
Origen: Proceso (Acceso al Usuario)
Destino: Lec_Alumnos ó Lec_Docentes
Almacenamiento: Lec_Alumnos ó Lec_Docentes

NIVEL 1.

Nombre: Lectura Datos Lector
Descripción: Características del lector, identificador, ATR
Origen: Agente Externo (Lector)
Destino: Proceso (1. Lectura Datos)
Almacenamiento: Lec_Salones

Nombre: Lectura Datos Tarjeta
Descripción: Datos del usuario dueño de la tarjeta (Ej. Código)

Origen: Agente Externo (Lector)
Destino: Proceso (1. Lectura Datos)
Almacenamiento: Lec_Alumnos ó Lec_Docentes

Nombre: Envió Datos Tarjeta
Descripción: Envía los datos obtenidos de la tarjeta del usuario
Origen: Proceso (1. Lectura Datos)
Destino: Proceso (3. Comparar Datos Tarjeta)
Almacenamiento: Lec_Alumnos ó Lec_Docentes

Nombre: Envió Datos Lector
Descripción: Envía los datos obtenidos del lector
Origen: Proceso (1. Lectura Datos)
Destino: Proceso (2. Convertir Datos Lector)
Almacenamiento: Lec_Salones

Nombre: Envió Datos Convertidos
Descripción: Envía los datos del lector convertidos a hexadecimal
Origen: Proceso (2. Convertir Datos Lector)
Destino: Proceso (4. Datos Convertidos Lector)
Almacenamiento: Lec_Salones

Nombre: Envió Datos Tarjeta Comparación
Descripción: Envía los datos del usuario a la base de datos para su comparación
Origen: Proceso (3. Comparar Datos Tarjeta)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta Comparación
Descripción: Respuesta de la comparación de los datos
Origen: Lec_Docentes ó Lec_Alumnos

Destino: Proceso (3. Comparar Datos Tarjeta)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Datos Usuario
Descripción: Extrae los datos del usuario de la base de datos
Origen: Lec_Docentes ó Lec_Alumnos
Destino: Proceso (3. Comparar Datos Tarjeta)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Datos Usuario
Descripción: Envía los datos del usuario al después de la comparación con la base de datos
Origen: Proceso (3. Compara Datos Tarjeta)
Destino: Proceso (5. Respuesta Proceso)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta Comparación
Descripción: Envía la respuesta de la comparación al proceso de respuesta
Origen: Proceso (3. Comparar Datos Tarjeta)
Destino: Proceso (5. Respuesta Proceso)
Almacenamiento: Lec_Alumnos ó Lec_Docentes

Nombre: Envió Datos Lector Convertidos
Descripción: Después de transformados los datos los envía a la base de datos para compararlos
Origen: Proceso (4. Datos Convertidos Lector)
Destino: Lec_Salones
Almacenamiento: Lec_Salones

Nombre: Datos Lector

Descripción: Devuelve los datos del lector sacados de la base de datos
Origen: Lec_Salones
Destino: Proceso (4. Datos Convertidos Lector)
Almacenamiento: Lec_Salones

Nombre: Datos Lector
Descripción: Envía los datos del lector al proceso de respuesta
Origen: Proceso (4. Datos Convertidos Lector)
Destino: Proceso (5. Respuesta Proceso)
Almacenamiento: Lec_Salones

Nombre: Aceptar /Negar Acceso Lector
Descripción: Permite o niega el acceso al usuario
Origen: Proceso (5. Respuesta Proceso)
Destino: Agente Externo (Lector)
Almacenamiento: Lec_Salones

Nombre: Imprimir Datos Usuario
Descripción: Imprime en pantalla los datos del usuario que usa el dispositivo
Origen: Proceso (5. Respuesta Proceso)
Destino: Agente Externo (PC)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Imprimir Datos Lector
Descripción: Imprime las características del lector usado
Origen: Proceso (5. Respuesta Proceso)
Destino: Agente Externo (PC)
Almacenamiento: Lec_Salones

Nombre: Aceptar/Negar acceso PC

Descripción: Imprime en pantalla si acepta el acceso (cuadro verde) ó si niega el acceso (cuadro rojo)

Origen: Proceso (5. Respuesta Proceso)

Destino: Agente Externo (PC)

Almacenamiento: Lec_Docentes ó Lec_Alumnos

NIVEL 2.

Nombre: Datos Lector

Descripción: Envía los datos del lector al proceso de respuesta positivo

Origen: Proceso (4. Datos Convertidos Lector)

Destino: Proceso (5.1 Respuesta Positiva Proceso)

Almacenamiento: Lec_Salones

Nombre: Respuesta Comparación

Descripción: Envía la respuesta positiva de la comparación

Origen: Proceso (3. Comparar Datos Tarjeta)

Destino: Proceso (5.1 Respuesta Positiva Proceso)

Almacenamiento: Lec_Alumnos ó Lec_Docentes

Nombre: Datos Usuario

Descripción: Envía los datos del usuario al proceso positivo

Origen: Proceso (3. Comparar Datos Tarjeta)

Destino: Proceso (5.1 Respuesta Positiva Proceso)

Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Aceptar Acceso Lector

Descripción: Permite el acceso al usuario

Origen: Proceso (5.1 Respuesta Positiva Proceso)

Destino: Agente Externo (Lector)

Almacenamiento: Lec_Salones

Nombre: Imprimir Datos Usuario
Descripción: Imprime en pantalla los datos del usuario
Origen: Proceso (5.1 Respuesta Positiva Proceso)
Destino: Agente Externo (PC)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Imprimir Datos Lector
Descripción: Imprime en pantalla los datos del lector
Origen: Proceso (5.1 Respuesta Positiva Proceso)
Destino: Agente Externo (PC)
Almacenamiento: Lec_Salones

Nombre: Aceptar Acceso PC
Descripción: Imprime en pantalla la aceptación del acceso (cuadro verde)
Origen: Proceso (5.1 Respuesta Positiva Proceso)
Destino: Agente Externo (PC)
Almacenamiento: Lec_Salones

Nombre: Respuesta Comparación
Descripción: Envía la respuesta negativa de la comparación
Origen: Proceso (3. Comparar Datos Tarjeta)
Destino: Proceso (5.2 Respuesta Negativa Proceso)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Negar Acceso Lector
Descripción: Niega el acceso al lector
Origen: Proceso (5.2 Respuesta Negativa Proceso)
Destino: Agente Externo (Lector)
Almacenamiento: Lec_Salones

Nombre: Negar Acceso PC

Descripción: Imprime en pantalla la negación del acceso (cuadro verde)

Origen: Proceso (5.2 Respuesta Negativa Proceso)

Destino: Agente Externo (PC)

Almacenamiento: Lec_Salones

Anexo 4: Flujos de Datos Software Administrador

NIVEL 0.

Nombre: Manejo de Datos

Descripción: Administra los datos del usuario

Origen: Agente externo (Administrador)

Destino: Proceso (Manejo de Datos Usuarios)

Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Lectura Datos Lector

Descripción: Características del lector, identificador, ATR

Origen: Agente Externo (Lector)

Destino: Proceso (Manejo de Datos Usuarios)

Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Datos Lector

Descripción: Envía los datos del lector hacia la base de datos

Origen: Proceso (Manejo de Datos Usuarios)

Destino: Lec_Docentes ó Lec_Alumnos

Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Datos Usuario

Descripción: Envía los datos del usuario hacia la base de datos
Origen: Proceso (Manejo de Datos Usuarios)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta Datos Lector/Usuario
Descripción: Envía la respuesta de la acción realizada sobre el Dato del usuario contenido en la base de datos
Origen: Lec_Docentes ó Lec_Alumnos
Destino: Proceso (Manejo de Datos Usuarios)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Resultado Manejo de Datos
Descripción: Imprime en pantalla los resultados de las acciones realizadas sobre los usuarios (Ej. Insertar, borrar datos)
Origen: Proceso (Manejo de Datos Usuarios)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

NIVEL 1.

Nombre: Asignar UID Docente/Alumno
Descripción: Agregar el UID del lector al usuario con el que se está trabajando
Origen: Proceso (1. Leer Datos Lector)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta UID
Descripción: Devuelve los resultados de la grabación
Origen: Lec_Docentes ó Lec_Alumnos

Destino: Proceso (1. Leer Datos Lector)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta UID
Descripción: Devuelve los resultados de la grabación
Origen: Proceso (1. Leer Datos Lector)
Destino: Proceso (3. Respuesta Operaciones)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Operación Datos Docente/Alumno
Descripción: realiza la operación seleccionada sobre los datos del usuario (Ej. Leer, Eliminar, Insertar Datos)
Origen: Proceso (2. Administración Datos Usuario)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta Operación
Descripción: Devuelve los resultados de la operación realizada
Origen: Lec_Docentes ó Lec_Alumnos
Destino: Proceso (2. Administración Datos Usuario)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Respuesta Operación
Descripción: Devuelve los resultados de la operación realizada
Origen: Proceso (2. Administración Datos Usuario)
Destino: Proceso (3. Respuesta Operaciones)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Resultado Manejo de Datos
Descripción: Imprime en pantalla los resultados de todas las operaciones realizadas tanto de los usuarios como del lector

Origen: Proceso (3. Respuesta Operaciones)
Destino: Agente externo (PC)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

NIVEL 2.

Nombre: Manejo de Datos
Descripción: Administra los datos del usuario
Origen: Agente externo (Administrador)
Destino: Proceso (2.1 Leer, Agregar, Eliminar Datos)
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Leer Datos
Descripción: Lee los datos del usuario contenidos en la base de datos
Origen: Proceso (2.1 Leer, Agregar, Eliminar Datos)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Agregar Datos
Descripción: Adiciona nuevos datos al usuario que se desee modificar
Origen: Proceso (2.1 Leer, Agregar, Eliminar Datos)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre: Eliminar Datos
Descripción: Elimina los datos que se deseen del usuario seleccionado
Origen: Proceso (2.1 Leer, Agregar, Eliminar Datos)
Destino: Lec_Docentes ó Lec_Alumnos
Almacenamiento: Lec_Docentes ó Lec_Alumnos

Nombre:	Respuesta Operación
Descripción:	Devuelve los resultados de la operación realizada
Origen:	Lec_Docentes ó Lec_Alumnos
Destino:	Proceso (2.1 Leer, Agregar, Eliminar Datos)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Nombre:	Respuesta Operación
Descripción:	Devuelve los resultados de la operación realizada
Origen:	Proceso (2.1 Leer, Agregar, Eliminar Datos)
Destino:	Proceso (3. Respuesta Operaciones)
Almacenamiento:	Lec_Docentes ó Lec_Alumnos

Anexo 5: Almacenes de Datos Software Usuario

Nombre:	Lec_Alumnos
Descripción:	Guarda la información del alumno
Flujos que entran:	Envió datos tarjeta comparación
Flujos que salen:	Respuesta comparación
	Datos usuario
Número de Datos:	7
Datos:	Código (varchar) –> Llave primaria
	Nombres (varchar)
	Apellidos (varchar)
	Tipo_Documento (varchar)
	Nro_Documento (varchar)
	Semestre (varchar)
	ID_Tarjeta (varchar)

Nombre:	Lec_Docentes
Descripción:	Guarda información del docentes

Flujos que entran:	Envió datos tarjeta comparación
Flujos que salen:	Respuesta comparación
	Datos usuario
Número de Datos:	5
Datos:	Nro_Documento (varchar) –> Llave primaria
	Tipo_Documento (varchar)
	Nombres (varchar)
	Apellidos (varchar)
	ID_Tarjeta (varchar)

Nombre:	Lec_Salones
Descripción:	Contiene datos del salón e identificador del lector
Flujos que entran:	Envió datos lector convertidos
Flujos que salen:	Datos lector
Número de Datos:	3
Datos:	ID_Salon (number) –> Llave primaria
	Nombre_Salon (varchar)
	Ident_Lector (varchar)

Nombre:	Lec_Materias
Descripción:	Contiene datos de las materias
Número de Datos:	2
Datos:	ID_Materia (number) –> Llave primaria
	Nombre_Materia (varchar)

Nombre:	Lec_Facultades
Descripción:	Contiene las facultades de la Universidad
Número de Datos:	2
Datos:	ID_Facultad (number) –> Llave primaria
	Nombre_Facultad (varchar)

Nombre:	Lec_Facultad_Carreras

Descripción:	Contiene las carreras de cada facultad
Número de Datos:	3
Datos:	ID_Carrera (number) –> Llave primaria
	ID_Facultad (number)
	Nombre_Carrera (varchar)

Nombre:	Lec_Alumnos_Materia
Descripción:	Materias correspondientes al alumno
Número de Datos:	4
Datos:	ID_Alumno_Materia (number) –> Llave primaria
	Código (varchar)
	ID_Materia_Carrera (number)
	Nota (number)

Nombre:	Lec_Materias_Carreras
Descripción:	Contiene las materias y horarios del usuario
Número de Datos:	10
Datos:	ID_Materia_Carrera (number) –> Llave primaria
	Semestre (varchar)
	ID_Materia (number)
	ID_Carrera (number)
	ID_Salon (number)
	Grupo (varchar)
	Día (varchar)
	Hora_Inicio (number)
	Hora_Final (number)
	Nro_Documento (varchar)

Anexo 6: Almacenes de Datos Software Administrador

Nombre:	Lec_Alumnos
Descripción:	Guarda la información del alumno
Flujos que entran:	Envió datos tarjeta comparación
Flujos que salen:	Respuesta comparación
	Datos usuario
Número de Datos:	7
Datos:	Código (varchar) –> Llave primaria
	Nombres (varchar)
	Apellidos (varchar)
	Tipo_Documento (varchar)
	Nro_Documento (varchar)
	Semestre (varchar)
	ID_Tarjeta (varchar)

Nombre:	Lec_Docentes
Descripción:	Guarda información del docentes
Flujos que entran:	Envió datos tarjeta comparación
Flujos que salen:	Respuesta comparación
	Datos usuario
Número de Datos:	5
Datos:	Nro_Documento (varchar) –> Llave primaria
	Tipo_Documento (varchar)
	Nombres (varchar)
	Apellidos (varchar)
	ID_Tarjeta (varchar)

Anexo 7: Procesos Software Usuario

Nombre:	Acceso al Usuario
Propósito:	Ejecutar la comparación de acceso
Flujos que entran:	Lectura Datos Lector Lectura Datos Tarjeta Respuesta Comparación Datos Lector Datos Usuario
Flujos que salen:	Comparación Datos Aceptar/Negar Acceso Lector Imprimir Datos Usuario Imprimir Datos Lector Aceptar/Negar Acceso PC
Descripción:	Este proceso es el más general, ya que reúne todo el funcionamiento del sistema, el cual consiste en leer la información del lector y de allí compararla con la base de datos para validar o negar el acceso.

Nombre:	1. Lectura Datos
Propósito:	Leer los datos del usuario que usa el dispositivo
Flujos que entran:	Lectura Datos Lector Lectura Datos Tarjeta
Flujos que salen:	Enviar Datos Lector Enviar Datos Tarjeta
Descripción:	Lee los datos de la tarjeta que está en el lector y los envía para su comparación.

Nombre:	2. Convertir Datos Lector
Propósito:	Transformar los datos correspondientes al lector
Flujos que entran:	Enviar Datos Lector
Flujos que salen:	Envió Datos Convertidos

Descripción:	Transforma los datos del lector (identificador, ATR) en hexadecimal para poder compararlos con los de la base de datos.
Nombre:	3. Comparar Datos Tarjeta
Propósito:	Envía los datos leídos para compararlos
Flujos que entran:	Enviar Datos Tarjeta Respuesta Comparación Datos Usuario
Flujos que salen:	Envió Datos Tarjeta Comparar Datos Usuario Respuesta comparación
Descripción:	Recibe los datos del usuario leídos con el lector y los envía hasta las base de datos para verificar la información y así emitir una respuesta de acceso.
Nombre:	4. Datos Convertidos Lector
Propósito:	Compara los datos del lector en la base de datos
Flujos que entran:	Envió Datos Convertidos Datos Lector
Flujos que salen:	Envió Datos Lector Convertidos Datos Lector
Descripción:	Recibe los datos del lector convertidos y de allí los compara con los de la base de datos para responder
Nombre:	5. Respuesta Proceso
Propósito:	Envía las respuestas de las comparaciones
Flujos que entran:	Respuesta Comparación Datos Usuario Datos Lector
Flujos que salen:	Aceptar/Negar Acceso Lector Imprimir Datos Usuario

	Imprimir Datos Lector
	Aceptar/Negar Acceso PC
Descripción:	Recibe todas las comparaciones realizadas por el sistema para enviarlas al lector y al PC, validando o negando la entrada.

Nombre:	5.1 Respuesta Positiva Proceso
Propósito:	Envía respuesta positiva de la comparación
Flujos que entran:	Datos Lector
	Respuesta Comparación
	Datos Usuario
Flujos que salen:	Aceptar Acceso Lector
	Imprimir Datos Usuario
	Imprimir Datos Lector
	Aceptar Acceso PC
Descripción:	Cuando recibe la comparación positiva de datos acepta el ingreso e imprime la información del usuario que usa el dispositivo.

Nombre:	5.2 Respuesta Negativa Proceso
Propósito:	Niega el acceso del usuario
Flujos que entran:	Respuesta Comparación
Flujos que salen:	Negar Acceso Lector
	Negar Acceso PC
Descripción:	Recibe la comparación de datos y si es negativa, niega el acceso tanto en el pc como en el lector.

Anexo 8: Procesos Software Administrador

Nombre:	Manejo de Datos Usuarios
Propósito:	Manipular toda la información de los usuarios

Flujos que entran:	Lectura Datos Lector Manejo de Datos Resultado Datos Lector/Usuario
Flujos que salen:	Datos Lector Usuario Resultado Manejo de Datos
Descripción:	Este proceso es el más general de todo el sistema, ya que reúne todo el funcionamiento de este, el cual consiste en manipular toda la información de los usuarios contenidos en la base de datos y así poder validar o negar el acceso.

Nombre:	1. Leer Datos Lector
Propósito:	Leer los datos del usuario que usa el dispositivo
Flujos que entran:	Lectura Datos Lector Respuesta UID
Flujos que salen:	Asignar UID Docente Asignar UID Alumno Respuesta UID
Descripción:	Lee el UID del lector y lo asigna al usuario que va a utilizar el dispositivo

Nombre:	2. Administración Datos Usuario
Propósito:	Manipular los datos del usuario, que permita la lectura, escritura y borrado de estos
Flujos que entran:	Manejo de Datos Respuesta Operación
Flujos que salen:	Operación Datos Docente Operación Datos Alumno Respuesta Operación
Descripción:	Manipula los datos de los usuarios con el fin de realizar modificaciones y asignar datos.

Nombre:	3. Respuesta Operaciones
Propósito:	Imprimir en pantalla todos los resultados de las operaciones realizadas a los usuarios y lector
Flujos que entran:	Respuesta UID Respuesta Operación
Flujos que salen:	Resultado Manejo de Datos
Descripción:	Muestra los resultados de las operaciones realizadas

Nombre:	2.1 Leer, Agregar, Eliminar Datos
Propósito:	Realiza operaciones o modificar datos de los usuarios
Flujos que entran:	Manejo de Datos Respuesta Operación
Flujos que salen:	Leer Datos Agregar Datos Eliminar Datos Respuesta Operación
Descripción:	Realiza operaciones sobre los datos de los usuarios

Anexo 9: Agentes Externos Software Usuario

Nombre:	Lector
Descripción:	Es el dispositivo que lee la información del usuario contenida en las tarjetas y envía los datos al sistema para que puedan ser comparados con los de la base de datos y así validar o negar el acceso
Flujos que entran:	Aceptar/Negar Acceso Lector
Flujos que salen:	Lectura Datos Lector Lectura Datos Tarjeta

Nombre:	PC

Descripción: Imprime en pantalla los datos del usuario que usa el dispositivo y los datos del lector que se uso, como también imprime si acepta (cuadro verde) o niega (cuadro rojo) el acceso.

Flujos que entran: Imprimir Datos Usuario
Imprimir Datos Lector
Aceptar/Negar Acceso PC

Anexo 10: Agentes Externos Software Administrador

Nombre: Lector

Descripción: Es el dispositivo que lee la información del usuario contenida en las tarjetas y envía los datos al sistema para que puedan ser comparados con los de la base de datos y así validar o negar el acceso

Flujos que salen: Lectura Datos Lector

Nombre: PC

Descripción: Imprime en pantalla los datos del usuario que usa el dispositivo y los datos del lector que se uso, como también imprime si acepta (cuadro verde) o niega (cuadro rojo) el acceso.

Flujos que entran: Resultado Manejo de Datos

Nombre: Administrador

Descripción: Es el encargado de manipular el sistema y de realizar las operaciones sobre los datos de los usuarios.

Flujos que salen: Manejo de Datos

Anexo 11: CONVENIO

ACUERDO MUTUO DE CONFIDENCIALIDAD Y DE NO DIVULGACIÓN

Este acuerdo **MUTUO DE CONFIDENCIALIDAD DE NO DIVULGACIÓN** (de ahora en adelante denominado (el **"Acuerdo"**) se suscribe el día 11 de Noviembre de 2008 entre las siguientes Partes GRUPO CONDOR S.A. con domicilio en la ciudad de **Bucaramanga – Colombia, quien en adelante se denominará CONDOR** y MIGUEL ALEXANDER PORTILLA VILLAMIZAR identificado con Cédula de Ciudadanía No. 91.538.323 de Bucaramanga quien tiene domicilio en la ciudad de BUCARAMANGA (de ahora en adelante denominado(s) **"MIGUEL"**). En este acuerdo, tanto CONDOR como MIGUEL pueden denominarse de forma independiente como la **PARTE.**

Considerando la posibilidad del inicio de relaciones empresariales entre las partes (lo cual se denomina en el presente documento **"Transacción Propuesta"**), cada una de las Partes esta dispuesta a suministrar cierta información a la otra Parte referente a su empresa, proyecto o actividad. El suministro de esta Información Confidencial (así se le denomina en este documento) está condicionada a que los directivos, los empleados, socios, agentes, colaboradores y consultores (denominados todos ellos de ahora en adelante como los **"Representantes"**) acuerden en tratar a esta información de conformidad con las condiciones estipuladas en el presente contrato y actuar o abstenerse de actuar de acuerdo con el contenido del presente Acuerdo.

Por lo tanto, considerando los acuerdos suscritos en el presente documento, así como los compromisos especificados y otras consideraciones válidas, cuyo recibo y propiedad se reconocen en este acuerdo, las Partes que desean establecer este compromiso acuerdan lo siguiente:

1. **Información Confidencial**

(a) **"Información Confidencial"** es toda aquella información o datos que, sin importar su forma de presentación, se revela a una de las Partes (denominada **"Parte Receptora"**) por parte de o a nombre de la otra Parte (que se denomina la **"Parte Emisora"**) ya sea antes o después de la fecha en que se subscribe el presente acuerdo. De igual manera, se considera como Información Confidencial, toda la información y los datos generados por la Parte Receptora o sus representantes, que contenga, refleje o se derive de la información suministrada o de los datos, incluyendo, sin limitación alguna lo siguiente: información técnica o no técnica, lo cual incluye patentes, derechos de autor, secretos comerciales, información patentada, métodos, ideas, conceptos, diseños, inventos, procedimientos, procesos, programas software, documentos derivados de un software y las fórmulas relacionadas con los productos del pasado, presente y futuro, incluyendo los servicios que la Parte Emisora realice como investigación, trabajo experimental, desarrollo, detalles del diseño, especificaciones e ingeniería, estados financieros, predicciones, planes (ya sean empresariales, estratégicos, de mercadeo y otros), listados de clientes potenciales, datos respecto a las ventas, análisis de las ventas, equipo y otros activos, precios, costos, fuentes de suministro, métodos de fijación de precios, aspectos laborales y de personal, investigación de mercados y relaciones comerciales, ya sea que se consideren "Confidenciales o Patentadas".

(b) La confidencialidad y el compromiso de no revelar la información contenida en el presente acuerdo finalizará cuando la Parte Receptora compruebe que la información considerada como Confidencial:

i. Era de dominio público en el momento en que fue comunicada a la Parte Receptora por la Parte Emisora.
ii. Se convirtió en información de dominio público una vez fue comunicada a la Parte Receptora, sin que en este hecho haya participado la Parte Receptora.
iii. Se encontraba en posesión de la Parte Receptora sin que existiese sobre esta información compromiso alguno de confidencialidad en el momento en que la Parte Emisora la comunicó a la Parte Receptora.
iv. Fue comunicada de manera correcta a la Parte receptora sin que existiese la obligación de confidencialidad una vez que la información fue transmitida a la Parte Receptora.
v. Fue desarrollada de manera independiente por Parte de los Representantes de la Parte Receptora, sin que la información así desarrollada tuviese como referencia alguna información comunicada por la Parte Emisora.
vi. Fue revelada y divulgada obedeciendo a una decisión legal o a una orden emitida por algún juzgado u organismo gubernamental, siempre y cuando la Parte Receptora sujeta a esta orden judicial o decisión gubernamental cumpla con los requisitos establecidos en el numeral seis (6). *

2. **Confidencialidad.**

Cada una de las Partes se compromete por medio del presente documento a que esa Parte o sus representantes utilice la información confidencial únicamente con el propósito desarrollar las labores encomendadas, que dicha información tendrá un carácter estricto de confidencialidad y a que esta Parte o sus representantes no divulgará Parte alguna de esta Información Confidencial a ninguna persona, firma o entidad de ninguna manera. Cada Parte se compromete a transmitir la Información Confidencial únicamente a aquellos Representante que (A) necesitan conocer la Información Confidencial para poder evaluar la Transacción Propuesta. (B) se encuentran informados de los términos de este Acuerdo y (C) se comprometen a cumplir con lo dispuesto en el presente Acuerdo como si fuesen una de las Partes. En cualquier caso, cada Parte será responsable en caso de revelar la información violando de esta manera los términos aquí descritos. En cualquier caso, será responsable por la divulgación de información efectuada que viola las condiciones del presente acuerdo. Además, cada parte o sus Representantes se comprometen a no divulgar a ninguna persona, sin que cuente con una autorización escrita de la otra Parte para hacerlo, que tiene acceso a Información Confidencial, o a detalles relacionados con las negociaciones de la Transacción Propuesta o ningún otro dato, termino o condición aquí especificada.

3. Duración.

Por medio del presente acuerdo, cada Parte reconoce que se le ha entregado Información Confidencial de conformidad con los términos de este acuerdo que, por un periodo de sesenta (60) meses contados a partir de la terminación de las negociaciones entre las Partes con respecto a las labores encomendadas. Ni esta Parte ni sus representantes podrá, de manera directa o indirecta, solicitar, buscar, ofrecerse a efectuar o efectuar, (A) ninguna forma de negocio o transacción que involucre la otra Parte o cualquiera de sus asociados, incluyendo aunque no necesariamente limitándose a una fusión, asociación, oferta pública para la adquisición de acciones, oferta de intercambio o liquidación de los activos de la otra Parte. (B) cualquier solicitud o propuesta para renunciar, terminar o corregir los términos del presente acuerdo o (C) cualquier propuesta u otra clase de declaración que sea inconsistente con lo estipulado en el presente acuerdo, a menos y hasta que esta Parte reciba una notificación por escrito o una aprobación por escrito que esté firmada por las dos partes en relación con la realización de este procedimiento.

4. No negociación.

Cada una de las Partes se compromete a que durante el tiempo que dure el presente Acuerdo y por un periodo de tres (3) años contados a partir de la fecha del presente Acuerdo, ninguna de las Partes ni sus Representantes podrán iniciar directa o indirectamente ninguna discusión o negociación que conlleve a la contratación de oficiales o empleados de la otra Parte que estuvieron empleados o relacionados comercialmente en ese momento, sin que exista un consentimiento por escrito de la otra Parte.

5. Requerimientos de cierto grado de divulgación.

En el caso en que cualquiera de las Partes, o la persona que suministra la información confidencial, reciba una orden para qu revele toda o parte e esta Información Confidencial bajo los términos estipulados en una citación judicial, algún juzgado o alguna entidad gubernamental. Esta Parte se compromete a (A) Notificar a la otra Parte respecto a la existencia, términos y circunstancias de la solicitud en cuestión. (B) Consultar con la otra Parte sobre la posibilidad de tomar los pasos legales que fuesen necesarios para reducir o minimizar esta solicitud y (C) si se considera inevitable que tal Información Confidencial deba ser revelada para evitar problemas mayores a la Parte Receptora o castigos legales, suministrar únicamente una porción de la información Confidencial que, en opinión de la Parte Receptora, sea la que es necesario divulgar y hacer todo lo posible para obtener una orden o cualquier otra garantía confiable respecto al tratamiento confidencial que bebe dársele a esta Información.

6. Propiedad y devolución de la información confidencial.

Cada Parte se compromete a que la información revelada por la Parte Emisora es y seguirá siendo de propiedad de la Parte Emisora y que la información confidencial y todas las copias relacionadas con la misma en cualquier medio tangible (incluyendo, aunque no limitándose a los reportes, memorandos o cualquier otro material preparado por y a discreción de la Parte Emisora), le será regresados a esta Parte Emisora o serán completamente destruidos al cabo de tres (3) días hábiles, a partir de la solicitud efectuada por la Parte Emisora. Además, MIGUEL se compromete a borrar de manera permanente la Información Confidencial almacenada en forma electrónica, magnética o de otra manera, de manera inmediata cuando le sea solicitado por CONDOR. En este Acuerdo no existe ningún estatuto que le de licencia a la Parte Receptora sobre esta información o que le otorgue derechos sobre la Información Confidencial que es de propiedad de la Parte Emisora.

7. Ausencia de seguridad y garantías.

Cada parte reconoce que la otra Parte no tiene seguridades implícitas/explícitas o garantía alguna y por lo tanto, no habrá responsabilidad alguna con especto a la confiabilidad, exactitud o integridad de la información contenida en la Información Confidencial. Cualquier seguridad o garantía se limitará a aquella seguridad o garantías especificadas en un acuerdo adicional, - es que existiese, entre las Partes.

8. Recursos.

Cada Parte reconoce y está de acuerdo en que si una de las Partes o sus representantes violan el presente Acuerdo, se ocasionará un daño irreversible a la otra Parte y que en este caso la otra Parte no tendrá soluciones legales para evadir esta violación. En el caso de que haya violación o haya intenciones de violación de cualquiera de los términos del presente, cada Parte está de acuerdo en que la Parte afectada puede iniciar una demanda en cualquier juzgado y que tendrá derecho obtener una reparación preliminar y permanente u otras soluciones apropiadas y equitativas.

9. No Renuncia.

La falta de cumplimiento de los términos del presente acuerdo o si cualquiera de las Partes no solicita que se cumplan las condiciones del presente acuerdo, estas acciones de ninguna manera afectan la validez de este acuerdo ni se constituyen en una causal de renuncia a los términos aquí contenidos ni eliminará el derecho de las Partes para exigir que los términos del presente Acuerdo se cumplan.

10. No Traspaso.

Este acuerdo no puede ser transferido por ninguna de las Partes, ni en forma total o parcial sin el consentimiento por escrito de la otra Parte.

11. Aspectos Legales.

La ley aplicable al presente Acuerdo de Confidencialidad es la ley colombiana, y los jueces competentes para conocer los asuntos relacionados con el presente Acuerdo, son los jueces colombianos. (Entre ellas Ley 190 de 1995, Ley 256 de 1996, Código Penal Colombiano y todas las demás que apliquen y vigilen el cumplimiento de este tipo de Acuerdos)

12. Duplicados.

Este acuerdo puede ejecutarse en cualquier número de duplicados con el mismo efecto que tiene el documento que se encuentra firmado. Cada uno de estos duplicados se considerara un original, aunque todos los duplicados juntos constituirían un solo y mismo instrumento.

13. Divisibilidad.

Si cualquiera de los términos del presente acuerdo se considera inconsistente y contrario a cualquiera de las normas legales aplicables, en este caso estos términos deben modificarse en la medida necesaria para poder cumplir con la ley. Una vez sea modificado, los términos seguirán ejerciéndose en toda su extensión con todos los efectos.

14. No Modificación.

Ninguna alteración, modificación o cambio que se le realice al presente acuerdo se considerara válido, a menos que se consigne por escrito y que se firme por todas las Partes que intervienen en este acuerdo.

15. Interpretación.

Sin importar cualquiera de los términos del presente acuerdo que indique lo contrario, la Partes acuerdan que la interpretación de este acuerdo se debe hacer sin que se siga ningún principio al respecto que de otra manera requeriría que este acuerdo se interpretara en contra de la Parte que ejecuta por vía legal el Acuerdo.

16. Acuerdo Completo.

Este acuerdo constituye el Acuerdo final respecto al asunto a tratar en el mismo.

17. Notificaciones.

Cualquier notificación del presente acuerdo debe hacerse por escrito y se considerará legalmente entregada cuando se entrega personalmente o tres (3) días después a la fecha del timbre de correos registrado y prepago del país de origen, considerando que el sobre se encuentra dirigido a la dirección de cada una de las Partes, dirección que se especifica al lado de la firma del presente acuerdo.

En caso de que cualquiera de las partes cambie de dirección deberá notificar este cambio a la otra Parte, de conformidad con los términos contenidos en la cláusula

18. Definiciones

Los siguientes términos siempre que sean usados dentro del Acuerdo, incluida la presentación y consideraciones, deberán tener los siguientes significados, bien sean usados en singular o plural.

Propiedad Intelectual: Son los derechos relacionados con la Tecnología, dentro de los cuales se incluyen pero sin limitarse a ellos, el Know- How, secretos industriales, información técnica, materiales, diseños, metodología y conocimiento técnicos utilizados en el desarrollo de los proyectos y, específicamente, lo relacionado con los procedimientos aplicados en campo de la Tecnología.

Patentes: Son los derechos de propiedad intelectual que amparan la Tecnología y respecto de los cuales se han iniciado trámites tendientes a obtener su protección y reconocimiento legal por parte del Estado, bien sea que tal protección haya o no sido ya reconocida por parte de éste.

Tecnología: son aquellos productos, procesos y procedimientos desarrollados por cualquiera de las Partes.

Nuevos Desarrollos: Son todos los materiales, sustancias, productos, métodos, técnicas, aparatos, fórmulas o composiciones que constituyan de cualquier manera una mejora de la tecnología o que sean directamente útiles a ella y que hayan sido obtenidos por cualquiera de las Partes en desarrollo y durante la vigencia del presente Contrato. Para que un Nuevo Desarrollo pueda ser considerado de utilidad, requiere que su aplicación determine una mejora en la tecnología como consecuencia de elementos tales como, pero sin limitarse a, menores costos, mejores tiempos de respuesta o simplificación de los procedimientos de aplicación.

Acuerdo de Confidencialidad: Es el Acuerdo entre las partes descrito en la cláusula sobre Confidencialidad del Contrato para proteger el que la información sea revelada a terceros por alguna de las Partes.

Cláusula: Significa secciones de este contrato e irá siempre precedida del número correspondiente.

Contrato: Es el presente Acuerdo de Confidencialidad.

Parte: Es GRUPO CONDOR S.A., y/o MIGUEL ALEXANDER PORTILLA VILLAMIZAR

Información: Comprende de manera colectiva toda la información que, directa o indirectamente relacionada con los aspectos técnicos, financieros, comerciales, Tecnologías, las Patentes y la propiedad intelectual, en desarrollo del contrato y del Plan de Negocios del Proyecto, que una parte suministre a la otra, sus divisiones, subsidiarias, filiales o matrices, a través de sus empleados, asesores, agentes o representantes, individualmente o en conjunto, ya sea en forma escrita o verbal, incluidos todos os análisis, notas, resúmenes y conclusiones o cualquier otro documento preparado por las Partes. Para los efectos del contrato, se tendrá como confidencial toda la información, salvo aquella en la cual se indique de manera expresa que no es confidencial.

En constancia de lo anterior, y para dar inicio al Acuerdo de Confidencialidad y No Divulgación firman las partes a los 11 del mes de Noviembre de 2008.

_____fin de página_____

CONDOR:

Firma: _____
Nombre: NÉSTOR FABIAN SANTOS NOVA
Cargo: DIRECTOR PROYECTO MPI004-6
Dirección: Cra 19 # 35-02 Of: 326/308
Sede UIS Bucarica

MIGUEL:

Firma: _____
Nombre: MIGUEL ALEXANDER PORTILLA VILLAMIZAR
Dirección: Calle 15 # 32 – 26 La Castellana - Floridablanca
Documento: C.C. 91.538.323 de Bucaramanga

ACTA COMPROMISO

Consecutivo 172

IONIX Ltda presta a los señores MIGUEL PORTILLA con cédula número 91.538.323 de Bucaramanga y PABLO BARON con cédula número 109.862.3491 los siguientes equipos:

- ✓ Cable serial
- ✓ Tarjeta de desarrollo lectora RFID

Para trabajar en su tesis de grado de Ingeniería de Sistemas de la Universidad Autónoma de Bucaramanga (UNAB), quienes se comprometen a entregar estos equipos el día 28 de noviembre de 2008 en buen estado.

En constancia firman:

MIGUEL PORTILLA
91.538.323
Estudiante UNAB

PABLO BARON
109.862.3491
Estudiante UNAB

ROSITA MILENA SUAREZ Q
Directora de mantenimiento Médico
IONIX Ltda.