UNIVERSIDAD SIMÓN BOLÍVAR
Decanato de Estudios Profesionales
Coordinación de Electrónica

Diseño e Implementación de un Sistema de Control de Acceso

Por
Justo Javier Saavedra Guada

Sartenejas, Febrero 2006

UNIVERSIDAD SIMÓN BOLÍVAR
Decanato de Estudios Profesionales
Coordinación de Electrónica

Diseño e Implementación de un Sistema de Control de Acceso

Por
Justo Javier Saavedra Guada

Realizado con la Asesoría de
Ingeniero Nelson Mambre
Profesor Antonio Salazar

PROYECTO DE GRADO
Presentado ante la Ilustre Universidad Simón Bolívar
Como requisito parcial para optar al título de Ingeniero Electrónico
Sartenejas, Febrero 2006

UNIVERSIDAD SIMÓN BOLÍVAR
Decanato de Estudios Profesionales
Coordinación de Electrónica

Diseño e Implementación de un Sistema de Control de Acceso

Por
Justo Javier Saavedra Guada
Realizado con Asesoría del Ingeniero Nelson Mambre y el Profesor Antonio Salazar.

RESUMEN

El presente informe trata sobre el proyecto de pasantía "Diseño e Implementación de un Sistema de Control de Acceso" desarrollado para la empresa Seebeck Instrumentación y Control C.A. El proyecto surge debido a la necesidad de la empresa de ofrecer a sus clientes un sistema de control de acceso automatizado, totalmente configurable, con dispositivos de identificación confiables y a un precio más acorde a la realidad económica de Venezuela. Sistemas anteriores aun cuando confiables, no era configurables al nivel requerido por los clientes. El sistema desarrollado está basado en un controlador embebido que posee un CPU Am188 ES, cuya función es controlar de forma autónoma el acceso de personas a distintas zonas, mediante la apertura de cerraduras electrónicas, en los diferentes puntos de acceso en una empresa, banco u oficina. El mecanismo de identificación es a través de tarjetas de Identificación por Radio Frecuencia (RFID por sus siglas en ingles), que al ser energizadas por el campo magnético producido por las lectoras PROMAG PCR948, envían al lector información de identificación. El controlador embebido procesa el número de identificación comparándolo con una base de datos, verificando atributos de los usuarios como días, horas y puertas de acceso, para posteriormente ejecutar las acciones necesarias. Luego, la transacción realizada es guardada en la memoria Flash del sistema, con el objetivo de monitorear el acceso

de usuarios en determinadas zonas de una localidad. La configuración del sistema y de los usuarios es mediante una interfaz gráfica, que permite al cliente definir los parámetros del sistema. El diseño e implementación del Sistema de Control de Acceso abarca el estudio de las distintas memorias a ser utilizadas en el controlador embebido, las pruebas de los tipos de memoria, la implementación del sistema de memoria escogido, el desarrollo del Sistema de Control de Acceso y la elaboración de la interfaces de configuración y monitoreo del Sistema.

PALABRAS CLAVES

Control de acceso, Controlador, Embebido, RFID.

Aprobado con mención:_____

Postulado para el premio:_____

Sartenejas, Febrero 2006

Dedicado a mis futuros hijos,

A mi Madre,

A mi Padre,

A mi Abuela Nelly,

A mi Abuelo Justo

Y a mis amigos

Agradecimientos

A mi abuela por haberme cuidado desde pequeño y por haberme preparado todas esas comidas tan rica, espero que lo sigas haciendo por mucho tiempo más.

A mi madre y a mi padre, por muchas cosas.

Al Ingeniero Pedro Bortot, por haberme dado la oportunidad de realizar la pasantía.

Al ingeniero Nelson Mambre, mi tutor Industrial por haberme ayudado y enseñado en el transcurso de la pasantía.

A mi tutor Antonio Salazar, por haberme ayudado en la realización de este libro.

Al Ingeniero Benjamín Martins, por todo el apoyo brindado.

Índice General

Índice de Tablas y Figuras

Figuras:

Tablas:

GLOSARIO

ADO	Objetos de Datos Activex *("ActiveX Data Objects").*
CE	Controlador Embebido
CPU	Unidad Central de Proceso *("Central Processing Unit").*
E/S	Entradas/Salidas.
EEPROM	Memoria de solo Lectura Borrable y Programable Eléctricamente ("Electrically-Erasable Programmable Read-Only Memory").
FAT	Tabla de Asignación de Archivos *("File Allocation Table").*
JFFS	Sistema de Ficheros Flash con soporte a Transacciones *("Journaling Flash File System").*
PC	Computadora Personal *("Personal Computer").*
RFID	Identificación por Radio Frecuencia *("Radio Frecuency Identification").*
RS-232	Estándar de Comunicación Serial
RS-485	Estándar de Comunicación Serial
RTOS	Sistema Operativo en Tiempo Real *("Real Time Operating System").*
SCA	Sistema de Control de Acceso.
SQL	Lenguaje de Búsqueda Estructurado *("Structured Query Language").*
SRAM	Memoria de Acceso Aleatorio Estática *("Static Random Access Memory").*
YAFFS	Sólo otro Sistema de Ficheros Flash *("Yet Another Flash File System")*

1. INTRODUCCION

El proyecto de grado, “Diseño e Implementación de un Sistema de Control de Acceso,” surge debido a la necesidad de la empresa Seebeck Instrumentación y Control C.A de ofrecer a sus clientes un sistema de control de acceso automatizado, totalmente configurable, con dispositivos de identificación confiables y a un precio más acorde a la realidad económica de Venezuela. Seebeck Instrumentación y Control C.A es una empresa tecnológica, dedicada al desarrollo de productos, proyectos y servicios enmarcados en el área de la automatización industrial, comercial y centros de investigación, para que estos logren posiciones de mayor productividad y competitividad, con el fin de incrementar sus utilidades y mejorar el servicio que prestan a la comunidad.

El proyecto de pasantía tenía por objetivo principal, diseñar e implementar un Sistema de Control de Acceso (SCA) automatizado, englobando lo referente a la selección del tipo de memoria a utilizar, el diseño de las estructuras referentes a las bases de datos, el desarrollo del programa del SCA y las pruebas del Sistema. El SCA desarrollado está basado en un controlador embebido (CE), que posee un CPU Am188 ES y maneja una memoria Flash de 8 MBytes, para almacenar la base de datos correspondiente a los usuarios y las transacciones.

Un sistema de Control de Acceso permite controlar el acceso libre y aleatorio, a través de puntos de accesos (puertas de seguridad, etc.), a zonas específicas en una empresa u oficina, así como formar un registro de los movimientos de cada uno de los usuarios del sistema. Ofrecen un método seguro de control mediante tarjetas con banda magnética, tarjetas de Identificación por radio frecuencia (RFID), mecanismos de identificación por huellas dactilares u otro mecanismos, los cuales llevan almacenada información referente al usuario que las utiliza. Estos sistemas se encargan de la supervisión y control de los puntos de acceso de distintas zonas, registrando las actividades, las cuales pueden ser reportadas posteriormente en informes concisos.

Los desarrollos anteriores realizados en Seebeck no eran autónomos, ya que dependían de computadoras, en particular para el manejo de las bases de datos que contenían la información de control. Posteriormente se desarrolló un sistema de control de acceso basado en una memoria SRAM de 512KB con reserva de batería, el cual aunque autónomo, no contenía información del nombre y apellido del usuario en su base de datos debido al reducido espacio de memoria. Este desarrollo por otra parte no cumplía con las características de configuración requeridas por los clientes, ya que trabajaba con cuarenta y seis (46) perfiles de configuración, impidiendo que se pudieran configurar a los usuarios de forma independiente.

El SCA desarrollado en este proyecto de pasantía, está conformado por el controlador embebido, un módulo de entradas digitales y salidas de relé, las lectoras RFID y la interfaz de configuración del sistema. Las lectoras se encuentran comunicadas con el CE, a través de un puerto de comunicaciones, que opera bajo el estándar RS-485, por el cual viajan los datos provenientes de la lectura de las tarjetas RFID. El CE se encarga de procesar los datos, autentificar a los usuarios y ejecutar las acciones pertinentes.

Este libro esta divido en seis (6) capítulos:

- El capítulo (2) expone el planteamiento del problema, donde se revisan los antecedentes, objetivos y etapas involucradas en el desarrollo del proyecto.
- En el capítulo (3) se explican los fundamentos teóricos involucrados en el desarrollo del sistema de control de acceso, como lo son la Memoria Flash, la tecnología RFID y los Sistemas Embebidos.
- En el capítulo (4) se muestra las especificaciones de los equipos utilizados conjuntamente con la metodología empleada, explicando cada una de las fases involucradas en el proyecto.
- En el capitulo (5) se explica el funcionamiento del SCA, el tipo de memoria escogido, el diseño de las estructuras de la base de datos, su implementación y el manejo de memoria en el sistema. Se estudiarán las funciones más importantes

implementadas en el sistema. El desarrollo y empleo de la interfaz gráfica. Para finalizar con la recomendación para futuras implementaciones

- El capitulo (6) incluye las conclusiones.

2. PLANTEAMIENTO DEL PROBLEMA

En este capítulo se revisan los antecedentes del Sistema de Control de Acceso, así como los Objetivos Generales y Específicos establecidos en el desarrollo del nuevo Sistema de Control de Acceso, para posteriormente finalizar con una revisión de la etapas propuestas en el proyecto, las cuales permitieron cumplir con los objetivos definidos.

2.1 Antecedentes de Sistema de Control de Acceso Seebeck

En Seebeck existen dos sistemas de control de acceso realizados anteriormente. En el 2001, Erick Argüello, de la USB realizó como proyecto de pasantía el "diseño e implementación de un control de acceso de aplicación general", donde estructuró el sistema en forma de red de manera que permitiese su instalación y conexión a un computador personal bajo Windows 98. En el 2004, Elba Parra, de la USB realizó como proyecto de pasantía el "diseño e implementación de un sistema de control de acceso autónomo y automatizado", el cual se basó en el mismo controlador embebido utilizado para el desarrollo de este sistema de control de acceso, pero con la diferencia que en este se implementó un módulo de memoria SRAM de 512KB con respaldo de batería.

2.2 Objetivo General

Diseñar, programar e implementar un sistema de control de acceso automatizado, basado en un controlador embebido suministrado por la empresa, orientado a satisfacer las necesidades particulares de la pequeña y mediana empresa venezolana, que requieran sistemas de control de acceso para supervisión y monitoreo de su personal.

2.3 Objetivos Específicos

- Definir los parámetros necesarios para llevar a cabo un control de acceso eficiente.
- Re-Organizar la estructura de la base de datos existente para su ubicación en memoria y desarrollar el algoritmo de control de acceso.
- Implementar en el algoritmo de control de acceso las funciones requeridas por los clientes.
- Probar el sistema revisando el correcto funcionamiento del manejo de memoria implementado en el sistema.

2.4 Etapas del Proyecto

A continuación se presentan las etapas involucradas en el desarrollo del proyecto de pasantía, que incluyen el diseño, implementación y pruebas del Sistema de Control de Acceso.

Tabla 1: Etapas del Proyecto

Etapa	Descripción
1	Estudio de los distintos módulos de memoria SRAM y FLASH que pueden ser implementados en el controlador embebido.
2	Definición de la memoria a utilizar en el sistema de control de acceso (SRAM o FLASH) verificando sus alcances, capacidades, características y ventajas.
3	Definición de las estructuras a implementar en memoria referentes a las bases de datos y transacciones realizadas
4	Programación del sistema de control de acceso e implementación de las funciones requeridas.
5	Prueba y ajustes del sistema.
6	Desarrollo de una aplicación basada en Agilent VEE Pro 7.0 capaz de servir como interfaz primaria, de fácil uso para la configuración y visualización del sistema de control de acceso.

3. FUNDAMENTO TEORICO

En este capítulo se exponen ciertos conocimientos teóricos básicos relacionados al funcionamiento y características de las distintas tecnologías involucradas en el proyecto, como los son; la Memoria Flash, la tecnología RFID y los Sistemas Embebidos, para de esta manera comprender mejor la filosofía de la aplicación desarrollada. Pudiendo conocer así la magnitud de alcance del prototipo desarrollado.

3.1 La Memoria Flash

Es importante conocer las características de la Memoria Flash, ya que constituye el Módulo de Memoria implementado en el Controlador Embebido, el cual almacena la base de datos y las transacciones realizadas en el Sistema. Sus características y funcionamiento, permiten tener ideas claras sobre la implementación y confiabilidad del sistema en cuanto a datos se refiere. La Memoria Flash es una forma evolucionada de la memoria EEPROM que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos, a diferencia de los otros tipos de memoria, que sólo permiten escribir o borrar una única celda cada vez. Por ello, la Memoria Flash permite funcionar a velocidades muy superiores cuando los sistemas emplean lectura y escritura en diferentes puntos de esta memoria al mismo tiempo.

Las Memorias Flash son de tipo no volátil, esto significa que la información almacenada no se pierde cuando el dispositivo se desconecta de la corriente, lo que representa una característica muy valorada para la multitud de usos en los que se emplea este tipo de memoria, ya que brinda seguridad de almacenamiento frente a cortes de energía. Este tipo de memoria son usadas principalmente en pequeños dispositivos basados en el uso de baterías como teléfonos móviles, PDA, pequeños electrodomésticos, cámaras de fotos digitales, reproductores portátiles de MP3, etc.

Las capacidades de almacenamiento de las tarjetas que integran Memorias Flash comenzaron en 4 MB, pero actualmente se pueden encontrar en el mercado tarjetas de hasta 8 GB. La velocidad de transferencia de estas tarjetas, al igual que su capacidad, se ha ido incrementando progresivamente con el tiempo de manera tal que actualmente se encuentran tarjetas con velocidad de lectura de hasta 20 MB/sec. Ofrecen, además características de gran resistencia a los golpes. Su pequeño tamaño también es un factor determinante a la hora de escogerlas para un dispositivo portátil, debido a que son muy ligeras y ofrecen versatilidad para múltiples usos.

Sin embargo, todos los tipos de Memoria Flash sólo permiten un número limitado de escrituras y borrados, generalmente este tipo de memoria acepta un ciclo de borrado/escritura aproximadamente entre 100.000 y 1.000.000 de veces, dependiendo del tipo de celda, de la precisión del proceso de fabricación y del voltaje necesario para su borrado.

La desventaja de la Memoria Flash es que su programación es relativamente complicada. Se debe tener mayor cuidado en la lectura y escritura, y por las características propias del dispositivo es imposible escribir una data y después sobre-escribirla. Para poder escribir nueva información a la Memoria Flash se debe borrar la información vieja primero. Este proceso de borrado se efectúa con grandes bloques de memoria, en vez de simplemente borrar las secciones que se quieren sobre-escribir. Cuando se ejecutan varias operaciones repetidas de escritura, todo el proceso se puede tornar complicado.

Este tipo de memoria está fabricado con puertas lógicas NOR o NAND para almacenar los 0’s ó 1’s correspondientes. Actualmente hay una gran división entre los fabricantes de un tipo u otro, especialmente a la hora de elegir un sistema de archivos para estas memorias. Sin embargo se comienzan a desarrollar memorias basadas en ORNAND. Los sistemas de archivos para estas memorias están en pleno desarrollo aunque ya en funcionamiento como por ejemplo JFFS (Journaling Flash File System) originalmente para NOR, evolucionado a JFSS2 para soportar

además NAND o YAFFS (Yet Another Flash File System), ya en su segunda versión, para NAND. Sin embargo, en la práctica se emplea un sistema de archivos FAT (File Allocation Table) por compatibilidad, sobre todo en las tarjetas de memoria extraíble, este sistema de archivos desarrollado para MS-DOS y Windows, es relativamente sencillo, y debido a esto es soportado por casi todos los sistemas operativos para PC's, facilitando compartir información entre diversos sistemas operativos.

Las aplicaciones más habituales de Memoria Flash son: el llavero USB que, además del almacenamiento, puede incluir otros servicios como radio FM, grabación de voz y, sobre todo como reproductores portátiles de MP3 y otros formatos de audio; las PC Card; y las tarjetas de Memoria Flash que son el sustituto del carrete en la fotografía digital, ya que en las mismas se almacenan las fotos.

3.2 Identificación por Radio Frecuencia (RFID)

Es importante conocer el funcionamiento de la tecnología RFID, ya que es la utilizada en el desarrollo del Sistema de Control de Acceso. A continuación se mostrarán las características, componentes, funcionamiento y el uso actual de ésta tecnología, para con ello tener una visión clara sobre el tipo de seguridad que representa el uso de los dispositivos basados en la misma.

La Identificación por radiofrecuencia (RFID) es un método de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas RFID. Los cuales contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren

3.2.1 Características

- Es un sistema de identificación automático que no depende del contacto
- Se basa en radio frecuencias.
- Las etiquetas pueden ser reprogramadas

- Las etiquetas pasivas no requieren de alimentación eléctrica
- Posee múltiples aplicaciones

3.2.2 Componentes de un sistema de control de acceso basado en RFID

A continuación se presenta una tabla, que muestra los principales componentes de un sistema de Identificación por Radio Frecuencia. (Ver Tabla 2).

Tabla 2: Componentes de un Sistema RFID

Componentes	Especificaciones
La Antena	Las hay de distintos tamaños y de distintos rangos de frecuencia pudiendo variar entre: 50 - 500 Khz; 13.56 MHz; 0.9 – 2.5 Ghz; 5.8 Ghz Transmite a través de objetos no-metálicos
La Etiqueta RFID	Puede ser de lectura o de lectura/escritura. Se pueden definir como pasivas o activas; las pasivas son aquellas que reciben la energía de una antena, mientras que las activas utilizan una batería para transmitir su ID.
La Lectora	Sirve para energizar la tarjeta de identificación y capturar su número, para posteriormente enviarlo a un sistema de control o un computador que se encargue de procesar los datos.
El controlador o Computador	Este se encarga de recibir y procesar los datos pertenecientes al número de identificación de la tarjeta presentada en la lectora

Los elementos de la etiqueta RFID, se pueden ver en la Figura 1. La Etiqueta está constituida por un microchip que almacena la información referente al número de identificación, el condensador se encarga de energizar el microchip una vez que

la tarjeta ingresa a un campo magnético, y la antena se encarga de enviar la información que contiene el microchip.

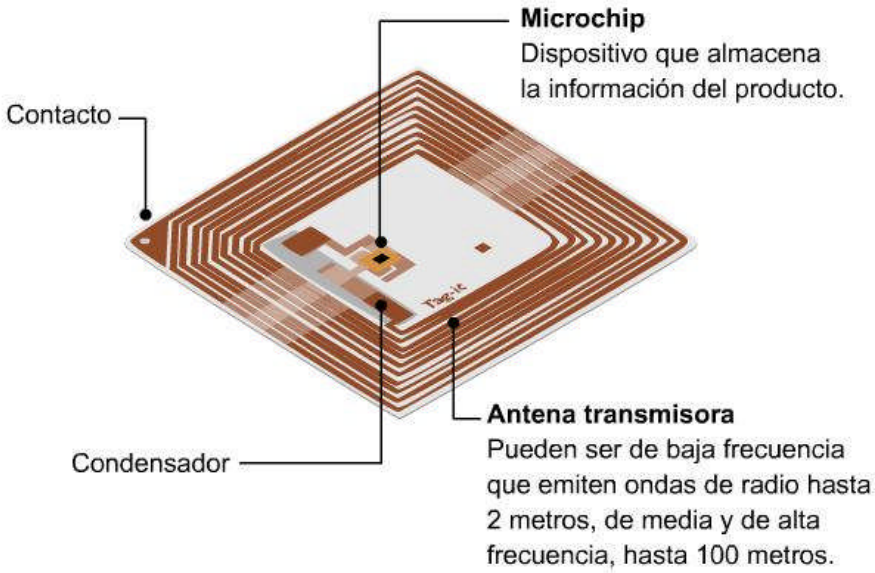


Figura 1: Elementos de la etiqueta RFID

3.2.3 Como funciona un sistema basado en RFID

1. La etiqueta entra en el campo de radio frecuencia.
2. La señal RF proveniente de la lectora energiza la Etiqueta RFID.
3. La etiqueta transmite su ID (Identificación) hacia la lectora.
4. La lectora captura los datos.
5. La lectora envía los datos a un computador.
6. La computadora procesa los datos y genera la acción pertinente.

En la Figura 2 se muestra, la estructura circuital del proceso de lectura de una etiqueta RFID. En la misma se puede ver que dicha etiqueta contiene una unidad de alimentación, un codificador, un decodificador, una unidad de control y la unidad de

memoria, la cual posee el número de identificación de esa etiqueta. Al ingresar la etiqueta al campo de la lectora, se energiza el sistema y a través de la unidad de control se envía la información contenida en la memoria de la tarjeta, la cual posteriormente es recibida, por el decodificador de lectora.

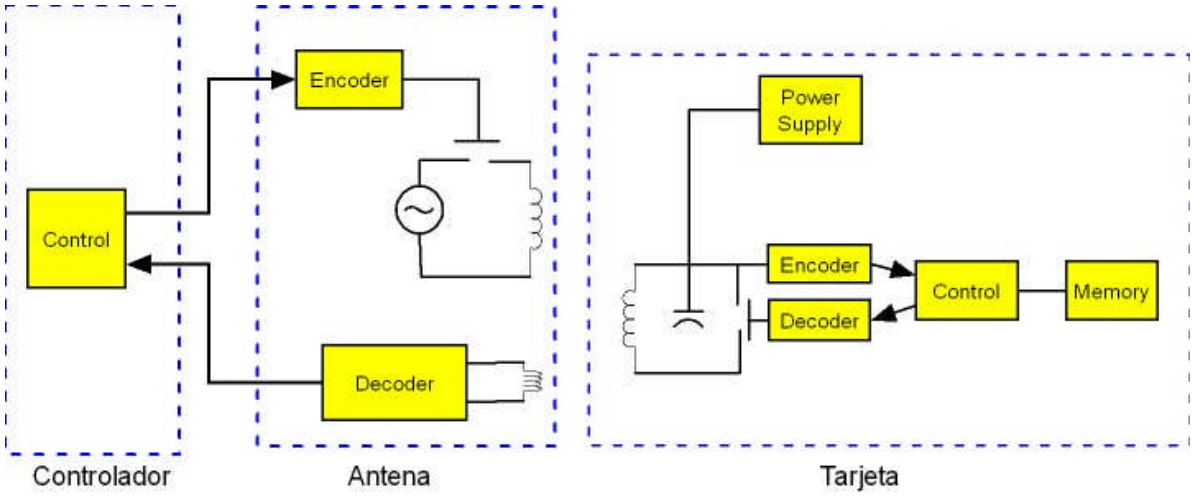


Figura 2: Como funciona el sistema RFID

A manera gráfica se puede observar en la Figura 3, de una forma más sencilla el funcionamiento del proceso de lectura de una etiqueta RFID, donde se aprecia claramente que la etiqueta RFID entra en el campo de la lectora, recibe la energía proveniente de ésta y finalmente envía su identificación a la lectora, la cual se encarga de decodificar la misma.

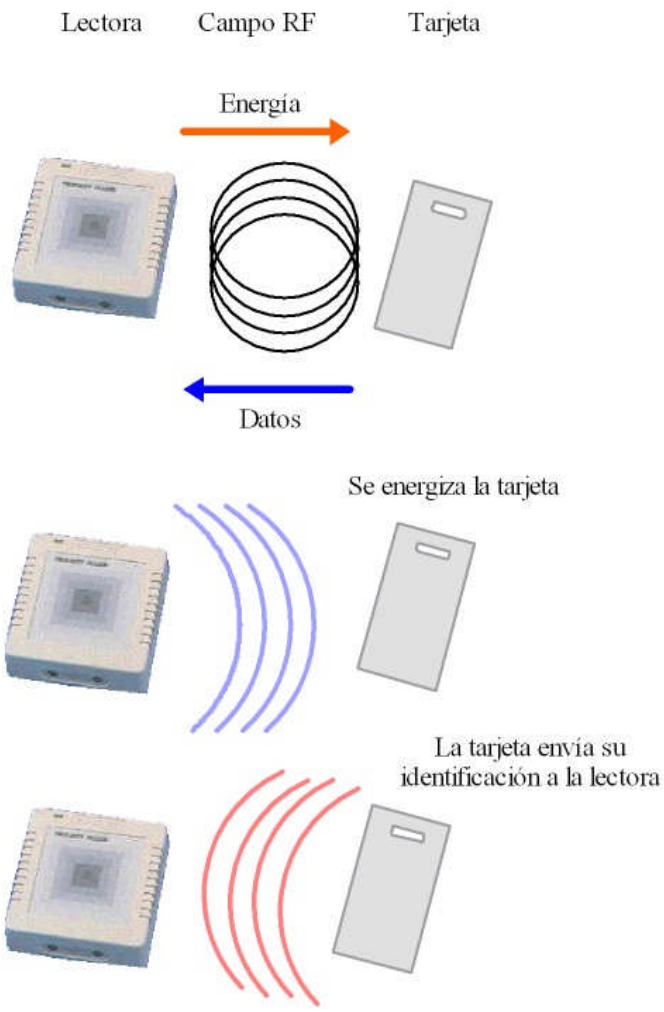


Figura 3: Proceso de lectura de una tarjeta

3.2.4 Regulación y estandarización

No hay ninguna corporación pública global que gobierne las frecuencias usadas para RFID. En principio, cada país puede fijar sus propias reglas. Las principales corporaciones que gobiernan la asignación de las frecuencias para RFID son:

- EE.UU.: FCC (Federal Communications Commission).
- Canadá: DOC (Departamento de la Comunicación).
- Europa: ERO, CEPT, ETSI y administraciones nacionales.

- Japón: MPHPT (Ministry of Public Management, Home Affairs, Post and Telecommunication).
- China: Ministerio de la Industria de Información
- Australia: Autoridad Australiana de la Comunicación (Australian Communication Authority).
- Nueva Zelanda: Ministerio de desarrollo económico de Nueva Zelanda (New Zealand Ministry of Economic Development.

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 kHz y 140 - 148.5 kHz) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia. La frecuencia ultra alta (UHF: 868 - 928 MHz) no puede ser utilizada de forma global, ya que no hay un único estándar global. En Norteamérica, la frecuencia ultra elevada se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la energía de transmisión. En Europa la frecuencia ultra elevada está bajo consideración para 865.6 - 867.6 MHz. Su uso es sin licencia sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la energía de transmisión. El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de la frecuencia ultra elevada. Cada aplicación de frecuencia ultra elevada en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la energía de transmisión.

3.2.5 Posibles Aplicaciones

Las etiquetas RFID de baja frecuencia se utilizan comúnmente para la identificación de animales, control de mercancía y como llave de automóviles con sistema antirrobo. En ocasiones se insertan en pequeños chips en mascotas, para que puedan ser devueltas a su dueño en caso de pérdida. En los Estados Unidos se utilizan dos frecuencias para RFID: 125 Khz. (el estándar original) y 134,5 Khz. (el

estándar internacional). Las etiquetas RFID de alta frecuencia se utilizan en bibliotecas y seguimiento de libros, control de acceso en edificios, seguimiento de equipaje en aerolíneas y seguimiento de artículos de ropa. Un uso extendido de las etiquetas de alta frecuencia es la identificación de insignias, sustituyendo a las anteriores tarjetas de banda magnética. Sólo es necesario acercar estas insignias a un lector para autenticar al portador.

3.3 Sistema Embebido

En general, la aplicación desarrollada cabe dentro de lo que se conoce como un Sistema Embebido. Es por ello necesario entender las características, componentes, aplicaciones y ventajas del mismo. Un sistema embebido es un sistema informático de uso específico construido dentro de un dispositivo mayor. Estos sistemas se utilizan para usos muy diferentes y generalmente vienen integrados con dispositivos de memoria, módulos de entrada/salida y puertos de comunicación. En general, consiste en un sistema basado en un microprocesador o un CPU cuyo hardware y software están específicamente diseñados y optimizados para resolver un problema concreto de forma eficiente. Normalmente un sistema embebido interactúa continuamente con el entorno para vigilar o controlar algún proceso mediante una serie de sensores. Su hardware se diseña habitualmente a nivel de chips

Los microcomputadores embebidos generalmente son sistemas que controlan electrodomésticos tales como: televisores, videos, lavadoras, alarmas, teléfonos inalámbricos, etc. Incluso un PC tiene microcomputadores embebidos en el monitor, impresora, y periféricos en general, adicionales a la CPU del propio PC. Un automóvil puede tener hasta un centenar de microprocesadores y microcontroladores que controlan cosas como la ignición, transmisión, dirección asistida, frenos antibloqueo (ABS), control de la tracción, etc.

Un sistema embebido complejo puede utilizar un sistema operativo como apoyo para la ejecución de sus programas, sobre todo cuando se requiere la

ejecución simultánea de los mismos. Cuando se utiliza un sistema operativo, lo más probable es que se tenga que tratar de un Sistema Operativo en Tiempo Real (RTOS, por sus siglas en ingles), que es un sistema operativo diseñado y optimizado para manejar fuertes restricciones de tiempo asociadas con eventos en aplicaciones de tiempo real. En una aplicación de tiempo real compleja, la utilización de un RTOS multitarea puede simplificar el desarrollo del software.

3.3.1 Componentes de un Sistema Embebido

- **CPU:** Es la unidad donde se ejecutan las instrucciones de los programas y se controla el funcionamiento de los distintos componentes del ordenador.
- **Memoria:** Puede ser interna o externa. El subsistema de memoria almacena las instrucciones del programa que controlan el funcionamiento del sistema. La memoria también almacena varios tipos de datos: datos de entrada que aún no han sido procesados, resultados intermedios del procesado y resultados finales en espera de salida al exterior.
- **Comunicación:** Es un componente de gran importancia debido a que permite que el sistema pueda comunicarse mediante una interfaz, la cual puede ser del tipo RS232, RS485, SPI, I²C, CAN, USB, IP, WiFi, GSM, GPRS, DSRC, etc.
- **Actuadores:** Son los posibles elementos electrónicos que el sistema se encarga de controlar. Puede ser un motor eléctrico o un conmutador tipo relé.
- **Módulo de entrada y salidas E/S:** Estas pueden ser analógicas y digitales, suelen emplearse para digitalizar señales analógicas procedentes de sensores, activar diodos LED y reconocer el estado abierto/cerrado de un conmutador o pulsador.
- **Módulo de Reloj:** Es el encargado de generar las diferentes señales de reloj a partir de un único oscilador principal. El tipo de oscilador es importante por varios aspectos: por la frecuencia necesaria, por la estabilidad necesaria y por el consumo de corriente requerido. El oscilador

con mejores características en cuanto a estabilidad son los basados en resonador de cristal de cuarzo.

- **Modulo de energía:** Se encarga de generar las diferentes tensiones y corrientes necesarias para alimentar los diferentes circuitos del sistema embebido. Usualmente se trabaja con un rango de posibles tensiones de entrada, a partir de la cuales mediante conversores ac/dc o dc/dc se obtienen las diferentes tensiones necesarias para alimentar los diversos componentes activos del circuito.
- **Conversores ac/dc y dc/dc.**

3.3.2 Aplicaciones de un PC Embebido

Los lugares donde se pueden encontrar los sistemas embebidos son numerosos y de diversas naturalezas. A continuación se exponen varios ejemplos para ilustrar las posibilidades de los mismos:

- Puntos de servicio o venta: Las cajas donde se cancela la compra en un supermercado son cada vez más completas, integrando teclados numéricos, lectores de códigos de barras mediante láser, lectores de tarjetas bancarias de banda magnética o chip, pantalla alfanumérica de cristal líquido, etc. El PC embebido en este caso requiere numerosos conectores de entrada y salida y unas características robustas para la operación continuada.
- Puntos de información al ciudadano: En las oficinas de turismo, grandes almacenes, bibliotecas, etc. existen equipos con una pantalla táctil, donde se puede pulsar sobre la misma y elegir la consulta a realizar, obteniendo una respuesta personalizada en un entorno gráfico amigable.
- Decodificadores para la recepción de televisión: Cada vez existe un mayor número de operadores de televisión que aprovechando las tecnologías vía satélite y de red de cable, ofrecen un servicio de televisión de pago diferenciado del convencional. En primer lugar, envían la señal en formato digital MPEG-2 con lo que es necesario un procesado para decodificarla y mandarla al televisor. Además viaja cifrada para evitar que la reciban en claro

usuarios sin contrato, lo que requiere descifrarla en casa del abonado. También ofrecen un servicio de televisión interactiva o Web-TV que necesita de un software específico para mostrar páginas Web y con ello un sistema basado en procesador con salida de señal de televisión.

- Sistemas radar de aviones: El procesado de la señal recibida o reflejada del sistema radar embarcado en un avión, requiere alta potencia de cálculo además de ocupar poco espacio, pesar poco y soportar condiciones extremas de funcionamiento (temperatura, presión atmosférica, vibraciones, etc.).
- Equipos de medicina en hospitales y ambulancias
- Máquinas de revelado automático de fotos.
- Cajeros automáticos.
- Pasarelas (Gateways) Internet-LAN.
- Y un sin fin de posibilidades aún por descubrir o en estado embrionario como son las neveras inteligentes que controlen su suministro vía Internet, PC's de bolsillo, etc.

3.3.3 Ventajas de un PC Embebido sobre las soluciones industriales tradicionales

Los equipos industriales de medida y control tradicionales, están basados en un microprocesador con un sistema operativo propietario o específico para la aplicación correspondiente. Dicha aplicación se programa en ensamblador para el microprocesador dado o en lenguaje C, realizando llamadas a las funciones básicas de ese sistema operativo, que en ciertos casos ni siquiera llega a existir. Con los modernos sistemas PC embebido, basados en microprocesadores x86 se llega a integrar el mundo del PC compatible con las aplicaciones industriales. Ello implica numerosas ventajas:

- Posibilidad de utilización de sistemas operativos potentes, que ya realizan numerosas tareas: comunicaciones por redes de datos, soporte gráfico, concurrencia con lanzamiento de hilos (threads), etc. Estos sistemas

operativos pueden ser los mismos que para PC’s compatibles (Linux, Windows, MS-DOS) con fuertes exigencias en hardware o bien ser una versión reducida de los mismos, con características orientadas a los PC’s embebidos.

- Al utilizar dichos sistemas operativos se pueden encontrar fácilmente herramientas de desarrollo de software potentes, así como numerosos programadores que las dominan, dada la extensión mundial de las aplicaciones para PC’s compatibles.
- Reducción en el precio de los componentes hardware y software debido a la gran cantidad de PC’s en el mundo.

4. MARCO METODOLOGICO

En el siguiente capítulo, se muestran tanto los equipos utilizados en el desarrollo e implementación del Sistema de Control de Acceso, así como las fases del proyecto. Para ello se mostrarán las especificaciones de los equipos involucrados y se explicará el proceso seguido para cumplir con cada una de las fases del proyecto.

4.1 EQUIPOS DEL SISTEMA DE CONTROL DE ACCESO

4.1.1 Controlador Embebido

Este módulo embebido integra entradas y salidas digitales. Está basado en CPU y posee dos puertos de comunicaciones; un puerto RS-232 el cual lo comunica a la PC y por donde se le carga el programa a ejecutar, y un puerto RS-485, para comunicarse con otros dispositivos (Ver Figura 4).

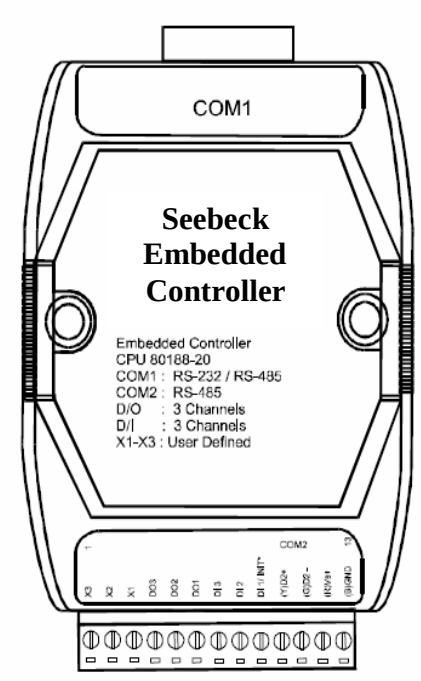


Figura 4: Controlador Embebido Seebeck

Especificaciones

Sistema

- CPU: Am188™ ES, 20M Hz
- Memoria SRAM: 128K bytes
- Memoria FLASH de solo lectura: 256K bytes
- Puerto de Comunicaciones: COM1, COM2
- Memoria EEPROM de 2048 bytes (8 bloques, c/u de 256 bytes)

Memoria Flash

- 256K bytes
- Bloque de borrado de 64K bytes
- 100,000 ciclos de borrado/escritura

COM1

- RS-232 o RS-485
- RS-232: TXD, RXD, RTS, CTS, GND
- RS-485: D1+, D1-,
- Velocidad de comunicación: 115200 bps como máximo.

COM2

- RS-485: D2+, D2-.
- Velocidad de comunicación: 115200 bps como máximo.

4.1.2 Módulo de Memoria FLASH NAND de 8 MB

Este módulo representa la expansión de memoria implementada en el controlador embebido, la cual es utilizada para almacenar las bases de datos de los usuarios y de las transacciones, que maneja el controlador embebido (Ver Figura 5).

Figura 5: Módulo de Memoria FLASH NAND de 8 MB

- Tamaño de la memoria : 8 M Bytes
- Rendimiento : 1,000,000 ciclos de borrado/escritura
- Retención de la data : 10 años
- Consumo de Energía : 0.4 W

4.1.3 Módulo de Expansión Entrada/Salidas de Relé

Este módulo representa la expansión del manejo de entradas digitales y salidas de relé, del controlador embebido. A través del puerto de comunicaciones RS-485, se encarga de recibir las instrucciones provenientes del controlador embebido, que permiten controlar el estado de las salidas de relé y censar las entradas digitales, las cuales posteriormente son enviadas al controlador embebido, que se encarga de procesar los datos (Ver Figura 6).

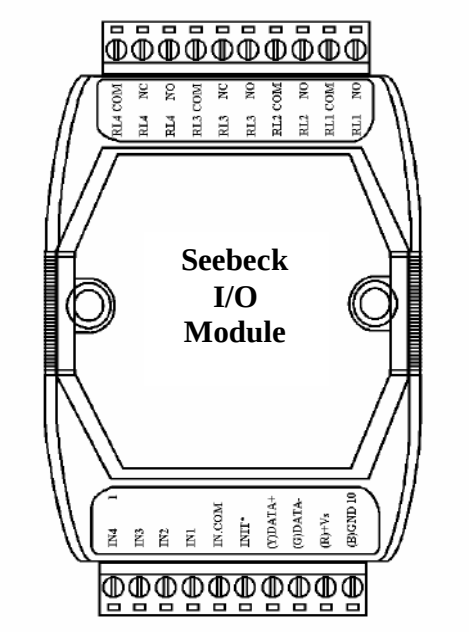


Figura 6: Módulo de extensión de E/S

Especificaciones

Canales de Salida: 4
Tipos de Relé: RL1, RL2 Tipo A RL3, RL4 Tipo C
Tiempo de operación: 3mS
Tiempo de Apertura: 2mS
Nivel Digital 0: +1V may
Nivel Digital 1: +4 a +30V
Impedancia de Entrada: 3K ohms
Alimentación: +10 hasta +30 VDC
Consumo de Energía: 1.3W

4.1.4 Lectora RFID PROMAG PCR948

Este dispositivo se encarga de energizar las tarjetas RFID, y decodificar sus datos, para luego a través de su puerto de comunicaciones enviarlos al controlador embebido, que se encarga de procesar los datos (Ver Figura 7).

Figura 7: Lectora PROMAG PCR948

Características

- Indicador Led para mostrar el status de operación
- Beeper audible para mostrar el status de lectura
- De sencilla integración para sistemas de control de acceso

Especificaciones

- Alimentación: 5 o 12 volts
- Rango de lectura: entre 5 cm -12 cm
- Frecuencia: 125 Khz, ASK
- Temperatura de Operación: 0 – 55 grados centígrados
- Velocidad de conexión: 9600 bps o 19200 bps
- Interfaz: RS-485

Limitaciones

- Se puede conectar un máximo de 16 lectoras en el sistema de control de acceso.

4.2 FASES DEL PROYECTO

A continuación se presenta la descripción de las fases involucradas en la realización del proyecto, las cuales son:

- Fase de Investigación
- Fase de Diseño
- Fase de Implementación
- Fase de Pruebas

4.2.1 Fase de Investigación

Se basó en la revisión de la documentación de los equipos a utilizar con el objetivo de entender sus características y funcionamiento, para posteriormente realizar pruebas que permitieron establecer el correcto uso de los dispositivos. A través de la plataforma de desarrollo Borland C++ 3.1, se compilaron programas de demostración, los cuales fueron cargados al CPU, con el propósito de entender el funcionamiento de los recursos que manejaba el controlador embebido, por ejemplo:

- La Lectura y Escritura en memoria.
- La Adquisición de las Entradas Digitales
- El Control de las Salidas Digitales.
- El manejo del Puerto de Comunicaciones

Posteriormente, utilizando como base los códigos de los programas de demostración, incluidos en la documentación de los equipos, se fueron realizando programas más personalizados con el objetivo de familiarizarse mejor con el uso de las librerías del dispositivo. Superada esta etapa, se llevó a cabo la investigación de los distintos módulos de memoria a utilizar, que tenían como función almacenar la información de la base de datos del Sistema de Control de Acceso

Tomando en cuenta la existencia de los dos módulos de extensión de memoria, los cuales eran el módulo de Memoria SRAM de 512 KB con backup de

batería y el Módulo de Memoria Flash de 8 MB, se desarrollaron programas de lectura/escritura en ambos módulos, a fin de conocer mejor sus estructuras y así poder establecer la adecuada selección del módulo de memoria. Una vez dominados los procesos de lectura/escritura, se inició el proceso investigativo de selección de la memoria a usar, para ello se revisó el desarrollo previo hecho en Memoria SRAM y se revisaron las peticiones exigidas por los clientes, con el objetivo de establecer el módulo de memoria más adecuado a implementar en el Sistema.

Motivado a que la anterior implementación con Memoria SRAM de 512 KB con backup de batería, no cumplió con las exigencias establecidas, debido a que por la poca cantidad de memoria se tenía que trabajar por perfiles de grupo y la capacidad de la base de datos era muy limitada, entonces se enfocó la investigación hacia el módulo de Memoria Flash de 8 MB, el cual representaba una solución más conveniente ya que el tamaño de memoria permitía una gran capacidad y flexibilidad en el desarrollo del sistema de Control de Acceso. Esta fase duró aproximadamente 21 días.

4.2.2 Fase de Diseño

Esta fase abarca el diseño de la estructuras de las bases de datos a implementar en el módulo de memoria Flash de 8 MB, correspondientes a la información relacionada con los usuarios y las transacciones. Para ello fue importante tener una idea clara sobre el funcionamiento posterior del Sistema de Control de Acceso a implementar, en cuanto a funciones de búsqueda, escritura y borrado, debido a que así se establecían parámetros necesarios que mejoraban el desempeño del futuro Sistema de Control de Acceso a implementarse.

Las estructuras de datos en memoria Flash se dividen en dos ramas: la estructura de los usuarios y la estructura de las transacciones. Para definir claramente los parámetros a implementarse en estas estructuras fue necesario conocer los requerimientos y limitaciones del Sistema. Los requerimientos del prototipo son:

- Capacidad de Almacenar 1000 (mil) usuarios en la base de datos.
- Tener una capacidad de almacenamiento de Transacciones mayor al sistema implementado anteriormente con memoria SRAM, el cual tenía la capacidad de almacenar 65.000 transacciones.
- Brindar flexibilidad en la configuración de usuarios, permitiendo tener configuraciones individuales sobre cada uno de ellos.
- Capacidad de borrar a los usuarios

Tomando en cuenta estos requerimientos y conociendo la estructura de la Memoria Flash organizada por bloques y páginas, se inició la fase de diseño. Como primer paso se establecieron los parámetros de configuración de los usuarios, y pensando en una gran flexibilidad del sistema se hicieron bosquejos con respecto a estas posibles configuraciones que permitían:

1. Establecer las puertas de acceso del personal en general.
2. Establecer los días permitidos de acceso al personal.
3. Establecer el horario de entrada y de salida del personal por cada día de la semana.

Existiendo la posibilidad de implementar cada usuario por cada página en la Memoria Flash y conociendo los alcances, se avanzó hasta desarrollar una estructura que permitía gran flexibilidad con respecto a la configuración de usuarios, brindando la posibilidad de hacerlo personalizadamente.

Así mismo ocurrió con el diseño de las estructuras de las transacciones, para ello se establecieron los parámetros importantes a conocer en las transacciones como los son: nombre, apellido, puerta de acceso, hora, fecha y validez de la transacción. Una vez establecidos estos parámetros se procedió a organizarlos en las estructuras de Memoria Flash, de manera tal que se cumplieran los requerimientos establecidos. Esta fase duró aproximadamente 10 días.

4.2.3 Fase de Implementación

En esta fase se implementaron las estructuras de datos en la Memoria Flash, y se desarrollaron las funciones del Sistema de Control de Acceso, con base en las estructuras antes diseñadas. El desarrollo del Sistema fue de lo general a lo específico.

En primer lugar se incorporaron al sistema las lectoras RFID y se desarrollaron funciones que censaban el estado de las mismas, para posteriormente establecer manualmente las configuraciones de los usuarios y poder verificar utilizando las lectoras, el correcto funcionamiento de las funciones de búsqueda y procesamiento de los datos. A medida que se desarrollaban más funciones, se realizaban pruebas sobre la marcha, con el objetivo de determinar fallas, así como también verificar el rendimiento del sistema, en cuanto a tiempo de procesamiento.

Posteriormente se fueron implementando funciones más especificas con el objetivo de verificar atributos de los usuarios, como días de las semana, puertas de entrada, horarios de entrada y de salida. Finalizado el desarrollo de estas funciones se fueron enlazando con otras y así se constituyó en general el Sistema de Control de Acceso. Alternativamente se fueron desarrollando las interfaces gráficas con el objetivo de visualizar y someter a pruebas las distintas implementaciones hechas en el sistema.

La interfaz basada en HyperTerminal fue desarrollada dentro del programa del sistema del control de acceso. Permitiendo interactuar con el controlador embebido, configurando usuarios y monitoreando el Sistema de Control de acceso. La interfaz desarrollada en Agilent VEE Pro fue implementada con el objetivo de incorporar funciones específicas que permitieron la fácil configuración del SCA, pudiendo de esta forma observar mejor los resultados obtenidos al realizar las implementaciones. Esta fase duró aproximadamente 60 días.

4.2.4 Fase de Pruebas

Esta constituye la última fase donde el Sistema de Control de Acceso fue puesto en marcha. Se sometió a varias pruebas donde se evaluaban los tiempos de procesamiento, las configuraciones de los usuarios y su correcto procesamiento. En el capítulo que viene, se hablará más específicamente sobre las pruebas realizadas y los resultados obtenidos.

Es importante resaltar que a medida de que se desarrollaba el Sistema, éste era probado por etapas, es decir, en cuanto se terminaba una función, se probaba el correcto funcionamiento de la misma, sometiéndola a distintas pruebas, para de esta forma verificar el correcto funcionamiento de las implementaciones realizadas.

El desarrollo de las interfaces, tanto la de Agilent VEE Pro, como la interfaz diseñada para hyperterminal, ayudó de manera significativa en el proceso de pruebas, ya que a través de ellas, se monitoreaban los resultados obtenidos al someter el Sistema a distintos procesos. Esta fase duró 20 días.

5. DOCUMENTACION DEL PROYECTO

Este capítulo presenta la relación de la metodología tratada anteriormente con las implementaciones hechas en el Sistema. Para ello se tratarán aspectos relacionados con la Arquitectura del Sistema implementado, para lo cual se mostrarán gráficas a fin de comprender mejor las definiciones hechas. Los resultados del diseño e implementación de las estructuras en la Memoria Flash serán expuestos, explicando su forma de implementación y los parámetros relacionados a dichas estructuras. Las funciones más importantes del Sistema serán explicadas, haciendo referencia a sus diagramas de flujos, para así comprender el funcionamiento del Sistema y como se integran dichas funciones. De igual forma, se presentará el desarrollo involucrado en la implementación de las interfaces, diseñadas con la finalidad de facilitar la interacción entre el cliente y el sistema de control de acceso. Adicionalmente se expondrán los resultados de las Pruebas hechas al Sistema, mostrando el objetivo de las mismas y el procedimiento utilizado.

5.1 ARQUITECTURA Y FUNCIONAMIENTO DEL SISTEMA DE CONTROL DE ACCESO

El controlador embebido esta basado en una arquitectura Harvard debido a que utiliza dispositivos de almacenamiento físicamente separados para las instrucciones y para los datos. El Sistema de Control de Acceso, el cual esta integrado por el controlador embebido y por las lectoras RFID, constituye una arquitectura centralizada, donde el término centralizada corresponde al controlador embebido, ya que éste pregunta continuamente a las lectoras si poseen datos en sus respectivos buffers de memoria, para posteriormente procesar los datos provenientes de las lectoras, verificar los datos, autentificar a los usuarios y realizar las acciones necesarias que involucran el acceso o restricción a una zona determinada.

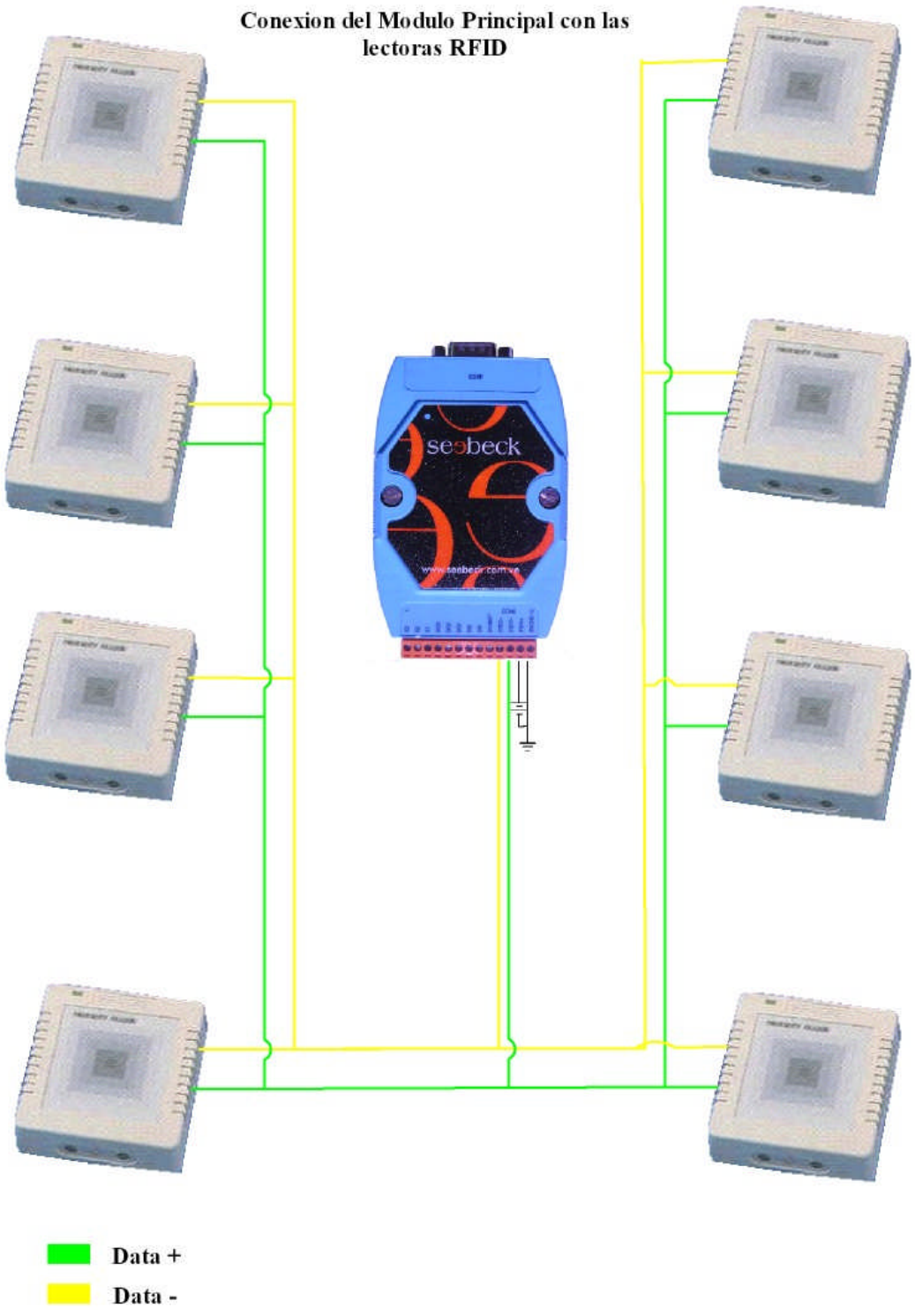


Figura 8: Conexión de las lectoras al controlador embebido

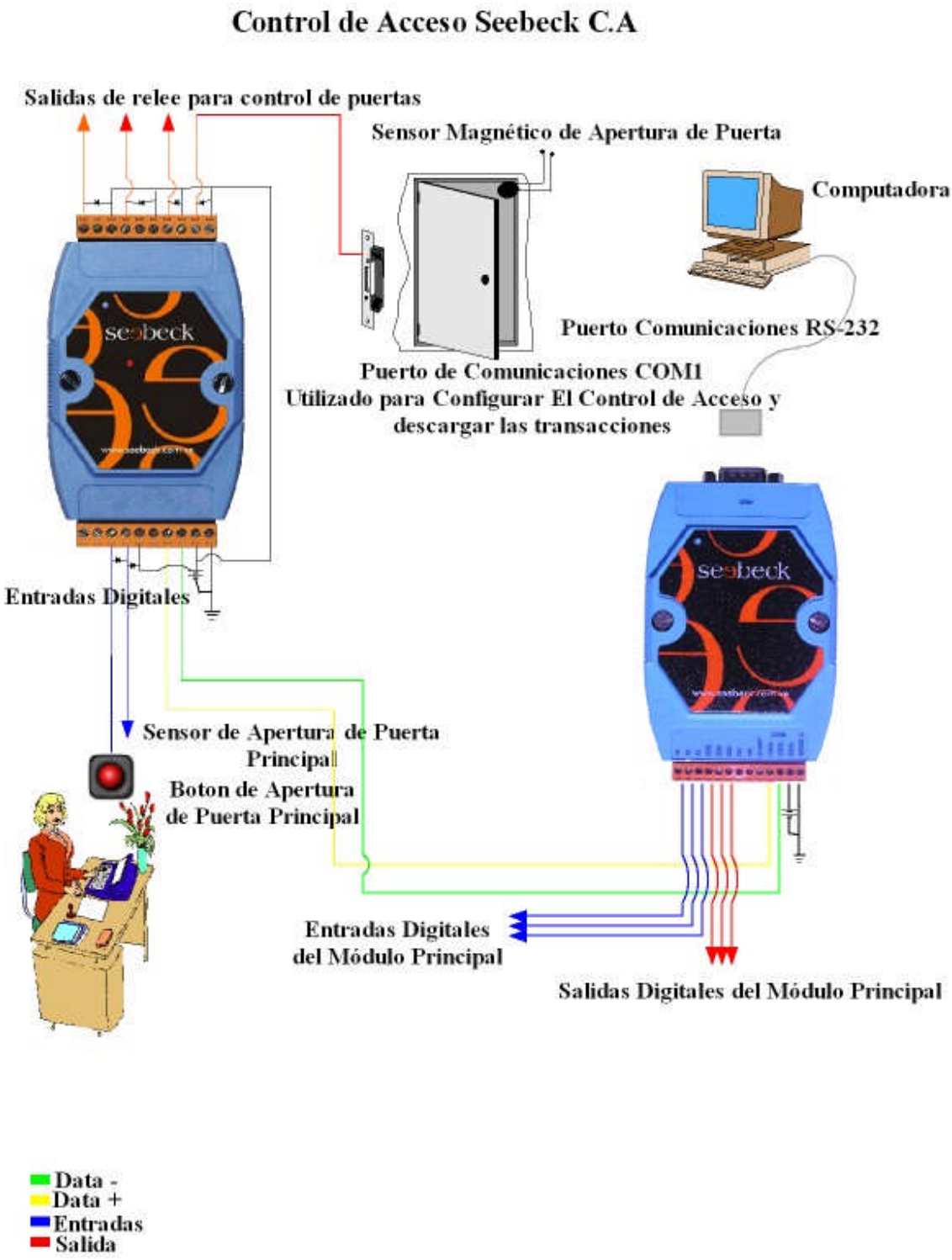


Figura 9: Arquitectura del sistema de control de acceso

Como se puede ver en la Figura 8 las lectoras están conectadas al controlador embebido mediante dos cables, los cuales constituyen la interfaz física de comunicación en la que está basada el estándar RS-485. Todas estas lectoras están conectadas en paralelo puesto que cada una de ellas posee un sistema de identificación basado en direcciones, las cuales son asignadas mediante pines (jumpers) dispuestos en cada una de las lectoras. Debido a especificaciones del fabricante, estas lectoras poseen un rango de direccionamiento máximo de dieciséis (16) direcciones, lo cual limita al sistema a utilizar un máximo de lectoras conectadas en paralelo. Cuando el controlador embebido pregunta si alguna de las lectoras posee datos en el buffer, lo hace hacia una lectora en específico, mediante un protocolo en el cual uno de los parámetros es la dirección de la lectora. Este mensaje llega a todas por igual, pero sólo la lectora que pertenece a la dirección, ejecuta las instrucciones recibidas en el mensaje, es por ello que se pueden conectar en paralelo, evitando conflictos en el sistema.

Al presentar un carnet en alguna de las lectoras, se guarda el número de identificación de la tarjeta en un buffer interno, el cual es enviado posteriormente al controlador embebido, cuando este solicite los datos almacenados por dicha lectora. El proceso de adquisición de datos es llevado a cabo por el controlador embebido de manera cíclica, haciendo preguntas a cada una de las lectoras dispuestas en el sistema.

El controlador embebido recibe los datos por los mismos cables de comunicación basados en el estándar RS-485 (Ver Figura 8). Este los compara con una base de datos, verificando y autentificando al usuario. Los perfiles y configuraciones pertenecientes al usuario, son cargados en el controlador embebido desde la Memoria Flash, para de ésta manera procesar y tomar las acciones necesarias referentes a las peticiones del usuario.

Entre las acciones tomadas por el controlador embebido se encuentra la apertura de puertas mediante el módulo de Entradas/Salidas de relé, el cual funciona por mensajes, que son enviados desde el controlador embebido con instrucciones

especificas referentes a la dirección del módulo y de los relés de salida que se deseen abrir o cerrar, aumentando de esta manera las capacidades del controlador embebido, y por lo tanto las del sistema de control de acceso, para controlar más salidas.

Posteriormente el nombre, apellido, fecha, hora, puerta y validez de la operación, son almacenados en el sistema con el objetivo de llevar a cabo un control eficiente del Sistema de Control de Acceso implementado.

El módulo de expansión de Entradas/Salidas de relé, conjuntamente con el controlador embebido, permite manejar dispositivos que controlan la apertura de puertas y permite a través de sensores censar el estado de estas. También se dotó al sistema de una opción que permite registrar y controlar la apertura de la puerta principal mediante un pulsador a través del módulo de Entradas/Salidas de relé (Ver Figura 9). El pulsador configurado como una señal de entrada en el modulo, al ser presionado activa automáticamente el dispositivo de apertura de la puerta principal, y a través del protocolo de comunicaciones, entre el módulo de expansión de Entradas/Salidas de relé y el controlador embebido, se registra dicha operación.

5.2 DISEÑO E IMPLEMENTACION DE LAS ESTRUCTURAS EN MEMORIA FLASH

El módulo de Memoria Flash añadido al controlador embebido permite manejar hasta 8 MB, los cuales serán administrados de manera adecuada para almacenar la base de datos, transacciones y configuraciones del sistema. A continuación se explicarán las características y la forma de manejo de la estructuras de la Memoria Flash que permitieron implementar la base de datos, tanto de los usuarios como de las transacciones. Posteriormente, se verán las ventajas del uso de la Memoria Flash y se finalizará con un recorrido por las estructuras implementadas y los parámetros involucrados.

5.2.1 Características:

La Memoria Flash posee un rendimiento de 1.000.000 de ciclos de borrado/escritura y garantiza un almacenamiento de los datos por 10 años. La memoria se maneja por bloques y páginas, el módulo de memoria posee 1024 bloques, los cuales están conformados por 16 páginas (0-15) de 528 bytes cada una. (Ver Figura 10)

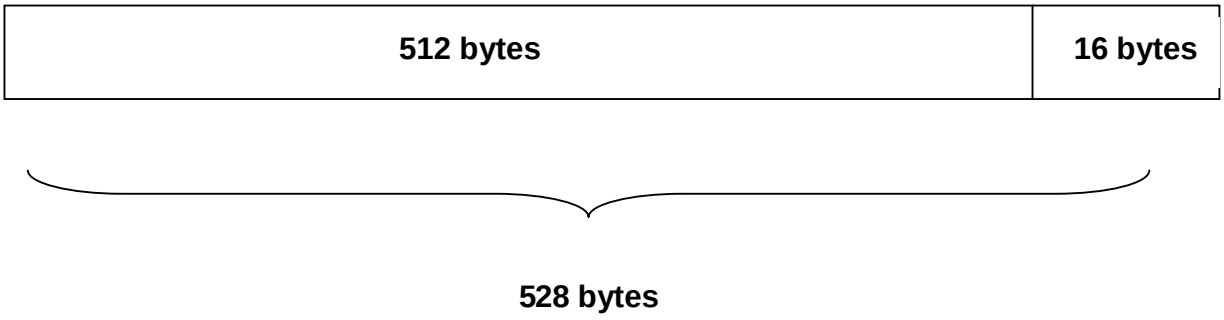


Figura 10: Estructura de la página de Memoria Flash

5.2.2 Manejo de la Memoria Flash

El módulo de memoria posee 8 MB de Memoria Flash la cual esta distribuida en 1024 bloques, cada bloque posee 16 páginas de 528 bytes, los cuales se dividen en un sub-bloque de 512 bytes y otro de 16 bytes. Cada bloque posee 16 páginas, por lo tanto

1024*16*512 bytes = 8 MB

Este módulo de Memoria Flash se puede administrar de distintas formas, con el objetivo de brindar facilidad y óptimo rendimiento en el almacenamiento de los datos. La memoria se administró de dos formas, una forma sencilla para el manejo de la base de datos de los usuarios y otra forma en grupo para el almacenamiento de transacciones. Cada una de ellas se explicará a continuación.

Si se aprovecha el manejo de las funciones de la Memoria Flash dadas por bloques y páginas, se puede definir un usuario por página (forma sencilla), desperdiciando cierta cantidad de memoria por usuario, pero que significativamente proporcionará una mayor facilidad a la hora de hacer las búsquedas de usuarios en memoria y ciertamente dará un mayor rendimiento en cuanto a tiempo se refiere, ya que no se tendrían que realizar ciertas funciones para hacer búsquedas definidas en ciertas direcciones de memoria.

Como sé pudo observar, anteriormente cada bloque de la Memoria Flash posee dieciséis páginas. Si guardamos un usuario por cada página, se poseen ventajas en cuanto al manejo de las funciones y como se tienen bytes sin utilizar, en un futuro se podrían implementar o agregar más parámetros de configuración, dando una gran flexibilidad al sistema de control de acceso, y por lo tanto el sistema puede ser mejorado con facilidad y habría la posibilidad de migrar hacia distintos sistemas de identificación sin problemas de espacio de memoria.

Como base para este prototipo el sistema de control de acceso posee capacidad para tener mil (1000) usuarios en la base de datos, esto quiere decir que se ocuparían (1000) páginas, es decir sesenta y tres (63) bloques, pero si vemos la capacidad de este módulo de memoria podríamos implementar una base de datos mucho mayor. Por ejemplo si se emplearan 3 MB para base de datos, se soportarían 6144 usuarios en una base de datos.

Si se observa la distribución de la Memoria Flash (Ver Tabla 3), se puede observar que no habrá inconveniente en el uso de la memoria aprovechando toda su capacidad.

Tabla 3: Administración de la Memoria Flash

Primer MB	Parámetros del sistema
Segundo MB	Base de Datos
Tercer MB	Base de Datos
Cuarto MB	Base de Datos
Quinto MB	Transacciones
Sexto MB	Transacciones
Séptimo MB	Transacciones
Octavo MB	Transacciones

El campo **Parámetros del Sistema** se refiere a datos relativos a configuraciones del sistema del control de acceso, como direcciones de las lectoras, arreglo de zonas y otras variables configurables por el administrador del sistema. El campo **Base de Datos**, se refiere a que en ese espacio de memoria, es posible almacenar, eliminar y re-configurar nuevos usuarios destinados a formar parte de la base de datos de usuarios en el sistema. El campo **Transacciones**, se refiere al espacio de memoria destinado al almacenamiento de las transacciones, las cuales serán almacenadas en la memoria en forma de grupos.

Cada transacción ocupa 56 bytes, agrupando por cada página, nueve (9) transacciones darían un total de 504 bytes, sólo se desperdiciarían 24 bytes, por cada 9 transacciones. Asumiendo entonces que 4 MB contienen 8192 páginas, entonces se pueden almacenar:

$$8192*9 = 73728 \text{ transacciones}$$

Debido a que el posicionamiento de las nueve (9) transacciones en cada página es el mismo, hace que el desarrollo de las funciones de lectura y escritura de transacciones no requiera alta complejidad.

5.2.3 Comparaciones entre uso de Memoria FLASH y SRAM

A continuación se presenta en la Tabla 4, un cuadro comparativo entre el empleo de la Memoria FLASH y la Memoria SRAM en el sistema de control de acceso, con el objetivo de apreciar las ventajas y desventajas que involucra el empleo de los distintos tipos de memoria, justificando de manera apropiada la migración hacia el sistema con Memoria Flash, el cual se presenta como más fiable, de mayor capacidad y de mayor flexibilidad

Tabla 4: Cuadro Comparativo entre Memoria Flash y Memoria SRAM

Aspectos	FLASH	SRAM
Número Transacciones	73.728	56.104
Flexibilidad Puertas por Usuario	1000	42
Flexibilidad Horarios por Usuario	Por Usuario (1000)	42
Flexibilidad Horarios-Puerta por Usuario	Por Usuario (1000)	42
Manejo de los usuarios	Asignada por bloques de memoria, haciendo más eficiente el uso de funciones y disminuyendo el tiempo de procesamiento de los datos. Facilidad para futuras actualizaciones del sistema	Saltos en memoria para rendir el espacio, incrementando el uso de funciones y por lo tanto aumentando el tiempo de procesamiento de la data.
Información de Transacciones	Incluyen Nombre, Apellido, #ID, Cedula, Operación, Puerta, Validez, Fecha y Hora	Incluye #ID, Validez, Fecha y Hora
Mercado	Destinado a Medianas y Pequeñas Empresas	Destinado a Mediana y Pequeñas Empresas

5.2.4 Ventajas en el uso de la Memoria Flash

A continuación se presentan las principales características y ventajas que representa el empleo de la Memoria FLASH en el sistema de control de acceso.

1. Posee mayor capacidad en el número de transacciones almacenadas, llegando a superar en el orden de las 15 mil transacciones a la Memoria SRAM.
2. Posee mayor flexibilidad a la hora de la configuración de los usuarios permitiendo tener un perfil por cada usuario. Se le pueden asignar las puertas de acceso permitidas y los horarios a cada uno de ellas, tanto en el horario de la mañana como en el horario de la tarde, para cada uno de los siete días de la semana. Es decir, se puede asignar a un mismo usuario distintos horarios para las distintas puertas entre los distintos días de la semana, teniendo así un mejor control a la hora de la supervisión del personal de las empresas
3. Facilidad en la implementación de las funciones de búsqueda y lectura, ya que se puede aprovechar la estructura de la Memoria Flash, optimizando así el sistema y los recursos del CPU.
4. Mayor cantidad de información de los usuarios, ya que se puede asignar tanto a la base de datos como a las transacciones datos más específicos del usuario, como su nombre, apellido, cédula, puerta, perfiles de puertas por cada día de la semana, horarios para cada puerta, tipos de operación (entrada / salida) y si fue procesada o invalidada su operación.
5. Capacidad de migración hacia otro sistema de identificación que requiera de más datos para la verificación y autentificación del usuario.

5.2.5 Estructura de Datos en la Memoria FLASH

A continuación se presentan las estructuras relacionadas con las bases de datos de los usuarios y las transacciones implementadas en la Memoria Flash del Controlador Embebido, haciendo referencia a los parámetros que integran dichas estructuras, su utilidad, capacidades y funcionamiento.

5.2.5.1 Usuarios en la base de datos

En la Tabla 5 se presentan la estructura de los usuarios en la base de datos, donde se indican los bytes utilizados por cada uno de los parámetros

Tabla 5: Estructura de Usuarios en la base de datos

Validez	1 byte
Nombre	20 bytes
Apellido	17 bytes
NumTarjeta	10 bytes
Restricciones	2 bytes
Arreglo de Puertas	8 bytes
Configuración	280 bytes
Total	**338 bytes**

Validez

Se refiere a la validez de una dirección en memoria

Valores:

255: El usuario es válido en el sistema

0: El usuario no esta válido en el sistema

Nombre

Se refiere al nombre del usuario

Apellido

Se refiere al apellido del usuario

Num Tarjeta

Se refiere al número de identificación del carnet asignado a cada usuario.

Restricciones

Se refiere a los diferentes perfiles que puede poseer un usuario, los cuales pueden ser; administrador, usuario normal, lista amarilla y lista negra. Se reservan 2 bytes previendo en el futuro colocar más funciones y perfiles requeridos por los clientes. El usuario administrador tiene acceso a todas las puertas del sistema y no posee ningún tipo de restricción. El usuario normal, se refiere a aquellos usuarios configurados como personal que labora en la empresa y que poseen ciertas restricciones en el sistema. El usuario lista amarilla es aquel que requiere de vigilancia ya que puede representar una amenaza a ciertas zonas. El usuario lista negra es aquel que por alguna razón representa una amenaza a la empresa, por lo cual se le es negado todo el acceso a las zonas de la empresa e inmediatamente solicite petición para acceder por cualquier puerta, será activada una alarma.

Arreglo de Puertas

Se refiere al arreglo que provee información acerca de las puertas permitidas en el usuario.

Valores:

255: Puerta Permitida

0: Puerta No Permitida

Configuración (Puerta-Día-Hora)

Este campo proporciona información acerca de los días y horas de acceso de los usuarios por cada puerta y por cada día de la semana. Suministra información tanto del horario de entrada como el horario de salida, brindando así gran flexibilidad a la hora de configurar usuarios de forma individual y avanzada. En la Figura 11 se muestra como queda definida en la memoria Flash la configuración para cada una de las puertas.

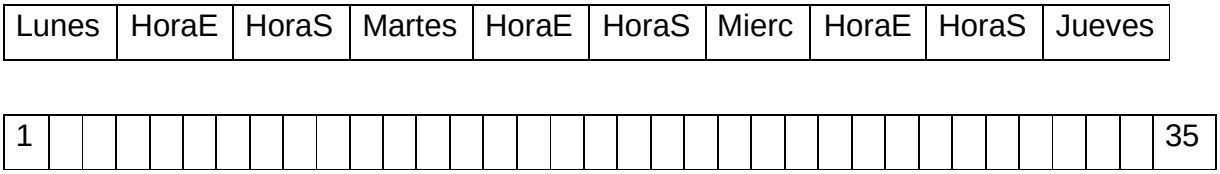


Figura 11: Estructura de Configuración de Puertas-Día-Hora

Y así sucesivamente hasta llegar al domingo, es decir que hay ocho (8) arreglos de esa forma, donde cada uno ocupa 35 bytes y como el sistema permite la configuración de 8 puertas, entonces el campo de configuración ocupa 280 bytes. Los campos usados que indican los días de la semana se refieren a información acerca de la accesibilidad del usuario ese día de la semana por determinada puerta, siendo 255 el indicador para día permitido y 0 el indicador para día no permitido. El campo **HoraE** y **HoraS** se refieren a la hora de entrada y a la hora de salida permitidas. Estos campos ocupan cada unos dos bytes, conteniendo información acerca de la hora y los minutos.

5.2.5.2 Transacciones

En la Tabla 6 se presenta la estructura definida para las transacciones a ser guardadas en Memoria Flash, la cual ocupa un total de 56 bytes, se muestran claramente los parámetros definidos en dicha estructuras y los tamaños asignados a cada uno de ellas.

Tabla 6: Estructura de Transacciones

Validez	1 byte
Num Tarjeta	10 bytes
Nombre	20 bytes
Apellido	17 bytes
Lectora	1 byte
Validez de Operación	1 byte
Fecha	3 bytes
Hora	3 bytes
Total	**56 bytes**

Lectora

Se refiere a la dirección de la lectora procesada por el cliente, pudiendo así determinar por cual puerta fue realizada la transacción, diferenciándose así la entrada y la salida de determinada zona.

Validez de la Operación

Se refiere a un byte que posee información acerca de la validez de la operación

Valores:

0: Acceso Negado por Antipassback, donde el término Antipassback se refiere a que un usuario utilizó una puerta dos veces seguidas. Como ejemplo: Un usuario que accesa a una zona y sin haber salido de ella, vuelve a hacer petición para acceder a la misma zona, lo cual genera un error y el sistema niega el acceso.

1: Acceso Negado por Lista Negra

2: Acceso Negado por Hora no Permitida

3: Acceso Negado debido a día no correspondido

4: Acceso Negado debido a puerta no permitida

127: Acceso Aprobado Lista Amarilla

255: Acceso Aprobado

Fecha

Se refiere al día, mes y año en la cual fue ejecutada la transacción.

Hora

Se refiere a la hora, minutos y segundos en la cual fue ejecutada la transacción.

5.2.5.3 Puertas del Sistema

En la Tabla 7 se presenta la estructura definida para la configuración de puertas en el Sistema de Control de Acceso, la cual ocupa un total de 51 bytes. El sistema utiliza la información perteneciente a estas estructuras para reconocer, los pares de lectoras asociados a cada una de las puertas, y las zonas que conforman.

Tabla 7: Estructura de Configuración Puertas en el sistema

Num Puertas	1 byte
Num Puertas SAP	1 byte
Arreglo Lectoras del sistema	16 bytes
Arreglo Lectoras SAP	16 bytes
Numero Puertas en una Zonas	1 byte
Arreglo de Zonas	16 bytes
Total	**51 bytes**

Numpuertas

Se refiere al número de puertas presentes en el sistema, permitiéndose un máximo de ocho (8) puertas a configurar en el sistema.

Num Puertas SAP

Se refiere al número de puertas SAP (sin anti-passback) presentes en el sistema, el cual permite configurar ocho (8) puertas en esta modalidad. De este modo el sistema de control de acceso puede operar en determinadas puertas con un nivel de seguridad bajo.

Arreglos de lectoras en el sistema

Es un arreglo que contiene la dirección física de todas las lectoras presentes en el sistema, ordenadas adecuadamente como lectoras de entrada y de salida. En la Memoria Flash el arreglo se ve de la siguiente manera (Ver Figura 12).

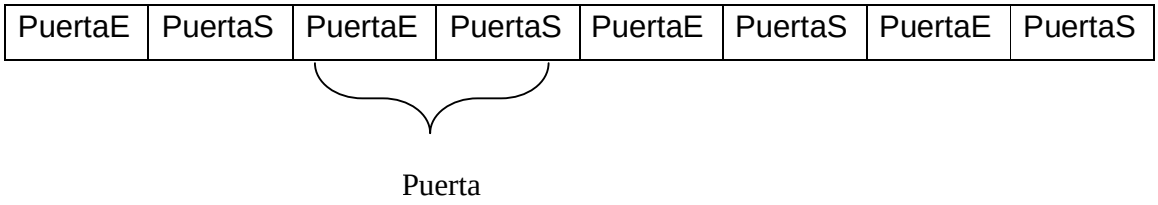


Figura 12: Estructura de Configuración de Puertas

El campo **PuertaE** corresponde a la lectora de entrada de una puerta, y el campo **PuertaS** corresponde a la lectora de salida de esa puerta. Las puertas se agrupan en pares, siendo el primer par el correspondiente a la primera puerta y así sucesivamente. Se ordenan de esa forma debido a que facilita el manejo de las funciones implementadas en el sistema.

Arreglo de lectoras SAP

Es un arreglo que contiene la dirección física de todas las lectoras que conforman las puertas SAP en el sistema

Número de Puertas en la zona

Se refiere al número de puertas las cuales se van a definir como una zona. La definición de zona viene dada por aquella localidad que posea dos o más puertas de acceso.

Arreglo de Zonas

Se refiere al arreglo que contiene la dirección física de las lectoras de entrada y salida de la zona. Con el parámetro anterior se definen la cantidad de puertas en la zona. El desarrollo de este sistema solo permite configurar una zona con 8 puertas.

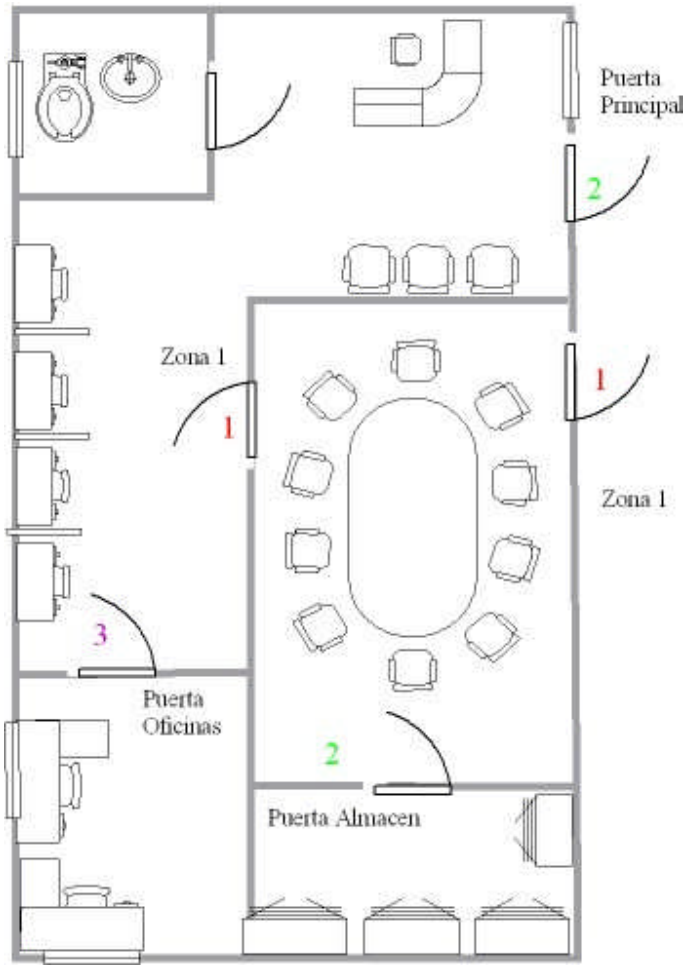


Figura 13: Distintos arreglos de puertas

Las zonas están definidas por dos o más puertas, las cuales representan una sola puerta. Son utilizadas para la entrada o salida por distintas vías en un mismo espacio de trabajo. En el ejemplo de la Figura 13 se observa que las puertas indicadas por el número **1** representan un arreglo de zona, donde los usuarios con acceso a ésta, pueden entrar o salir por las distintas puertas pertenecientes a la sala

de conferencias. Es importante resaltar que la importancia de las zonas radica en el uso de la función antipassback, la cual se basa principalmente en que una persona no puede entrar sin haber salido o viceversa. Las puertas denotadas con el número **2** representan una puerta con antipassback, debido a que la zona se refiere a un almacén, por lo tanto se requiere de cierta seguridad en el sentido de que no pueda haber transacciones corruptas hacia ese lugar. Otra puerta con ésta configuración es la puerta principal. Las puertas denotadas con el número **3** pueden representar una puerta sin antipassback, ya que son las oficinas de uso común y no requieren de tanta seguridad, pero queda a gusto del cliente.

5.3. IMPLEMENTACIONES DE LAS FUNCIONES DEL SISTEMA DE CONTROL DE ACCESO

A continuación se presentan las funciones más importantes del sistema de control de acceso, que muestran los procesos implementados en el sistema. El funcionamiento y los parámetros involucrados en ellas serán explicados, para entender la lógica del desarrollo realizado. En algunas se hará referencia el diagrama de flujo correspondiente, que nos mostrara la lógica utilizada y los alcances de las funciones.

5.3.1 PrincipalCA (void);

Es una de las funciones más importantes del sistema de control de acceso. Esta se encarga de hacer las llamadas a otras funciones con el propósito de censar el estado de las lectoras, hacer las búsquedas en base de datos, procesar a los usuarios, abrir las puertas y guardar las transacciones hechas. En la Anexo A, se muestra el diagrama de flujo de esta función, que ejecuta en forma cíclica la pregunta hacia las lectoras, para posteriormente en caso de que alguna de ellas contenga información en su buffer interno, realizar las búsquedas y procesar a los usuarios.

5.3.2 GuardarTransacción (Numtarjeta, Nombre, Apellido, Dirección, Validez):

Esta función se encarga de guardar las transacciones en la Memoria Flash. Al llegar al último bloque de escritura en Memoria Flash, la función automáticamente borra los primeros bloques asignados a las transacciones, para así efectuar la escritura cíclica de las transacciones, lo cual es una de las características principales del sistema.

5.3.3 GuardarUsuario (Nombre, Apellido, Numtarjeta, Restricciones, Configuración, Confpuertas);

Se utiliza para añadir un usuario nuevo en la base de datos. Los parámetros especificados en la función como el nombre y el apellido, se refieren a datos personales del usuario. Los otros parámetros se refieren a perfiles de configuración del usuario, los cuales se explican a continuación y que corresponden a las estructuras de los usuarios presentadas anteriormente en la Tabla 3.

Numtarjeta corresponde al número de identificación de la tarjeta RFID asignada al usuario.

Restricciones se refiere a la configuración del perfil del usuario, puede ser configurado como:

- Usuario Administrador
- Usuario Normal
- Usuario Lista Amarilla
- Usuario Lista Negra

Configuración es el arreglo que contiene información referente a los horarios, días de la semana y puertas asignadas al usuario a configurar.

Confpuertas corresponde al campo que contiene información referente a las puertas asignadas a cada usuario.

5.3.4 ProcessMessage (Función, Datos);

Esta función conjuntamente con la PrincipalCA, se ejecutan en un ciclo continuo, alternando la disposición del CPU en el controlador embebido. Esta función se encarga de procesar los mensajes provenientes de un computador, por el puerto de comunicaciones COM 1. El parámetro **función** indica la función a ejecutar y los **datos** contienen los parámetros a introducir en dichas funciones. Las configuraciones del sistema y de los usuarios, se hacen a través de ella. También procesa peticiones de aperturas y cerrados de emergencia, que se ejecutan en todas las puertas del sistema. (Ver Anexo B)

5.3.5 EliminarUsuario (Numtarjeta);

Se utiliza para eliminar un usuario de la base de datos. El número de identificación es buscado en la base de datos y es anulado del sistema.

5.3.6 ConfigurarPuertas (Numpuertas,Nunpuertassinap, Arreglopuertas, Arreglopuertasap, Arreglozonas);

Se utiliza para configurar las puertas presentes en el Sistema de Control de Acceso, el parámetro **(Numpuertas)** nos indica el número total de puertas existentes en el sistema, **(Numpuertassinap)** nos indica la cantidad de puertas en el sistema configuradas sin antipassback. Los otros parámetros de entrada representan arreglos que de forma ordenada suministran información acerca de direcciones de las lectoras de entrada y de salida correspondientes a cada una de las puertas y zonas configuradas en el sistema.

5.3.7 FijarFecha (año, mes, día);

Se utiliza para configurar la fecha en el módulo del sistema de control de acceso, la cual sirve de referencia para el procesamiento de usuarios y las transacciones del sistema.

5.3.8 FijarHora (hora, min, seg);

Se utiliza para configurar y fijar la hora en el módulo del sistema de control de acceso, la cual sirve de referencia para procesar a los usuarios, comparando los horarios permitidos de estos, con el horario del sistema para así otorgar acceso o restricciones en tiempos determinados.

5.3.9 VerTiempo (&hora, &min, &seg);

Se utiliza para obtener la hora del módulo del sistema de control de acceso, con el objeto de poder verificar y comparar, la hora real con la hora del modulo, para así en cualquier caso de desincronización poder tomar las acciones necesarias

5.3.10 VerFecha (&año, &mes, &dia);

Se utiliza para ver la fecha del módulo del sistema de control de acceso.

5.3.11 LeerTransacciones (xnum);

Se utiliza para descargar las transacciones guardadas en el sistema de control de acceso, a una velocidad de 38400 bps por el puerto COM 1. Dicha velocidad puede ser configurable hasta una velocidad de 115200 bps. El parámetro de entrada **xnum**, se refiere al número de transacciones que se desean descargar de la memoria. Esta función descarga las transacciones almacenadas, desde la última transacción realizada hacia la primera, llevando un contador interno que continuamente se compara con el parámetro de entrada, controlando así la cantidad de transacciones a leer. A través del diagrama de flujo expuesto a continuación en Anexo C se muestra el funcionamiento de esta función.

5.3.12 Antipassback (Numidentificación, Dirección);

La función antipassback como objetivo fundamental tiene la tarea de efectuar búsquedas en las transacciones anteriormente realizadas para así determinar con los parámetros **Numidentificación**, que se refiere al número de identificación del carnet RFID y la **Dirección**, que se refiere a la dirección de la lectora, si la transacción realizada a continuación es valida o no, ya que si un usuario hace una entrada ó salida por determinada puerta, tendrá que haber realizado anteriormente la operación contraria. Esto se hace posible dado que cada lectora de entrada tiene asignada una lectora de salida y ambas forman una puerta. En el caso de las zonas ocurre igual, ya que varias lectoras son asignadas como entradas con sus compañeras de salida, formando una sola zona entre ellas (Ver Anexo D).

5.3.13 OptimizarBaseDatos (void)

Esta función se utiliza para optimizar la base de datos presente en la memoria Flash del sistema. Al eliminar un usuario, solamente el byte de validez correspondiente a la página a la cual pertenece el usuario es modificado, invalidando de esta forma al usuario. No se realiza el borrado completo del usuario, ya que por las propiedades de la memoria, el borrado se hace por bloques, lo cual significaría borrar a 16 usuarios conjuntamente con el que borraríamos. Es por ello que sólo lo invalidamos modificando un byte. A medida de que se realizan re-configuraciones de usuarios y eliminaciones de los mismos, muchas páginas quedan invalidadas, lo que genera un gran desperdicio de la memoria. Luego de que la base de datos, llegue a un número relativo de usuarios entre borrados y activos, ejemplo 2000 usuarios, se optimiza la base de datos, sustituyendo los usuarios eliminados por usuarios válidos, mejorando así la velocidad de búsqueda de usuarios en la base de datos. A continuación se muestra una gráfica (Ver Figura 14) donde se puede apreciar, en forma de bloques la representación de la optimización de la base de datos en pequeña escala.

Figura 14: Visualización de de fragmentación de la memoria

Esta optimización de la memoria es muy parecida a la desfragmentación que se hacen en los discos duros, cuyo objetivo primordial es evitar hacer saltos grandes de memoria, para leer datos relacionados entre si, mejorando de esta manera la rapidez del sistema. El diagrama de flujo se puede ver en el Anexo E.

5.4. DESARROLLO DE LA INTERFAZ DEL SISTEMA DE CONTROL DE ACCESO

El sistema de control de acceso debe contar con una interfaz para poder configurarlo y monitorearlo. Para ello se desarrolló en el controlador embebido la posibilidad de configurar y monitorear a partir de dos distintas interfaces, la primera basada en comandos por teclado desarrollada para programas como Hyper Terminal y la otra desarrollada bajo la interfaz gráfica Agilent VEE PRO 7.0, la cual ofrece un ambiente más amigable para la configuración y monitoreo del sistema. Esta interfaz se comunica con el controlador embebido bajo un protocolo propio.

5.4.1 HyperTerminal

Esta primera interfaz se basa en el intercambio de datos entre el puerto COM 1 del controlador embebido y el PC. Posee un menú en el cual el usuario al presionar la opción solicitada es enviado a un submenú donde a través de instrucciones se

realizan las configuraciones y se monitorea el sistema de control de acceso (Ver Figura 15).

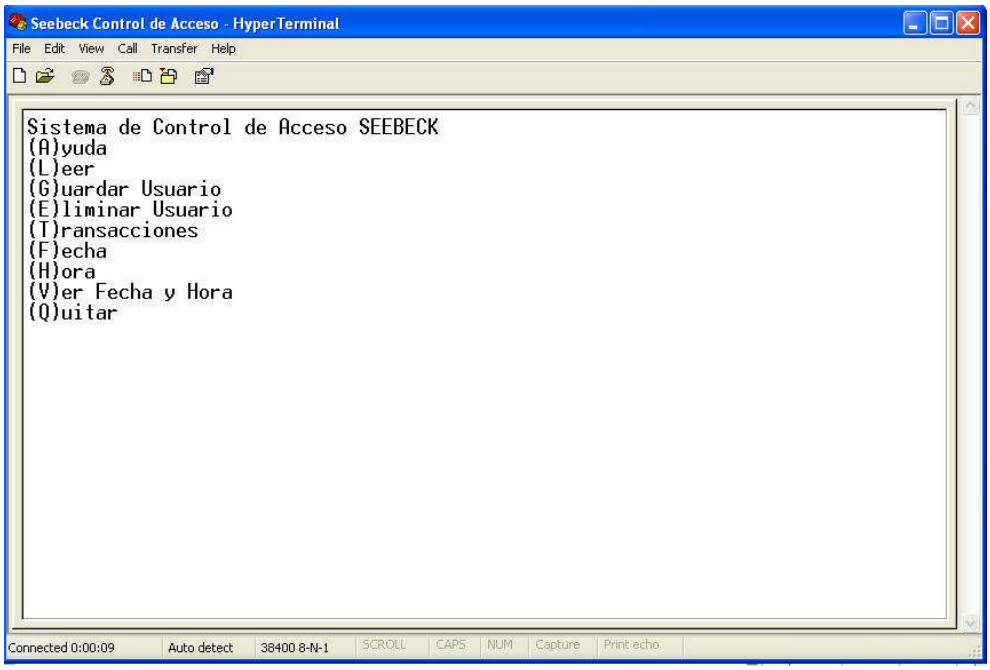


Figura 15: Menú del sistema CA Seebeck HyperTerminal

En el modo de lectura **(Leer)** se monitorea el acceso de los usuarios de forma instantánea, guardando de igual manera las transacciones. En este modo se muestra el nombre del usuario procesado junto con la validez de la operación, adicionalmente a modo de prueba se imprime el bloque, página y posición donde van a ser guardados los datos de la transacción en Memoria Flash. (Ver Figura 16)

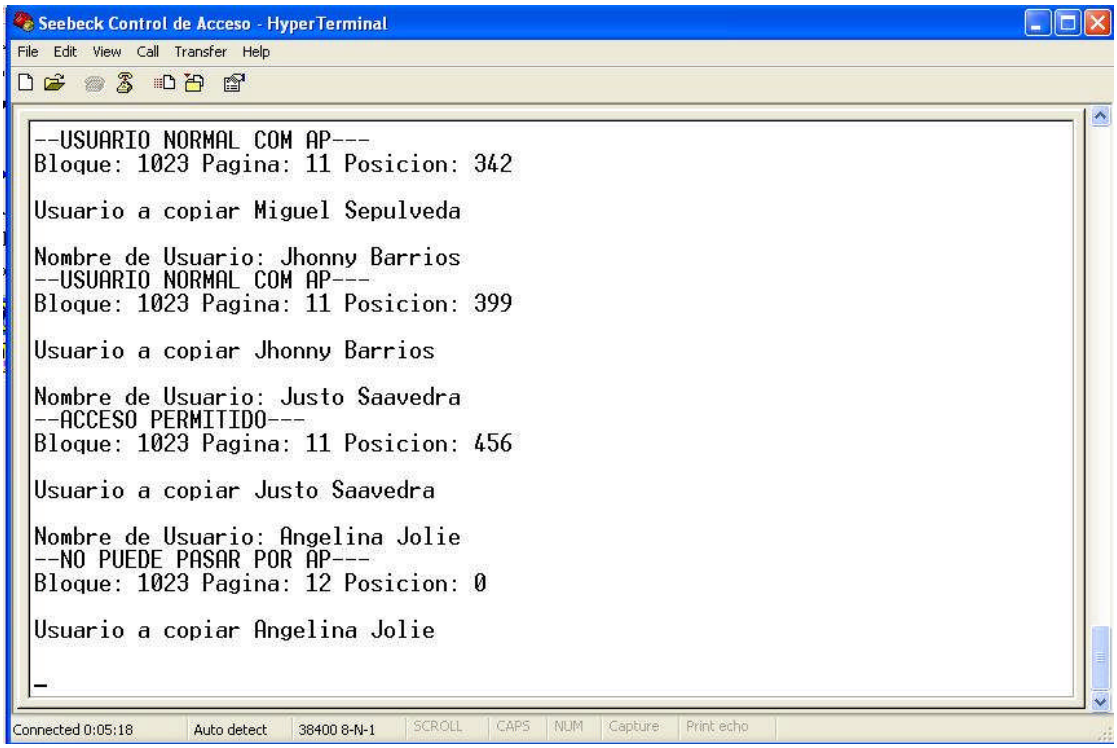


Figura 16: Modo Lectura CA Seebeck HyperTerminal

La configuración de usuarios se hace de forma ordenada, introduciendo el nombre, apellido, número de identificación correspondiente al carnet RFID, la configuración de puertas del usuario y sus horarios pertinentes en formato militar. La información es suministrada por comandos de teclado a través de un menú, el cual aparece a lo largo de la configuración (Ver Figura 17).

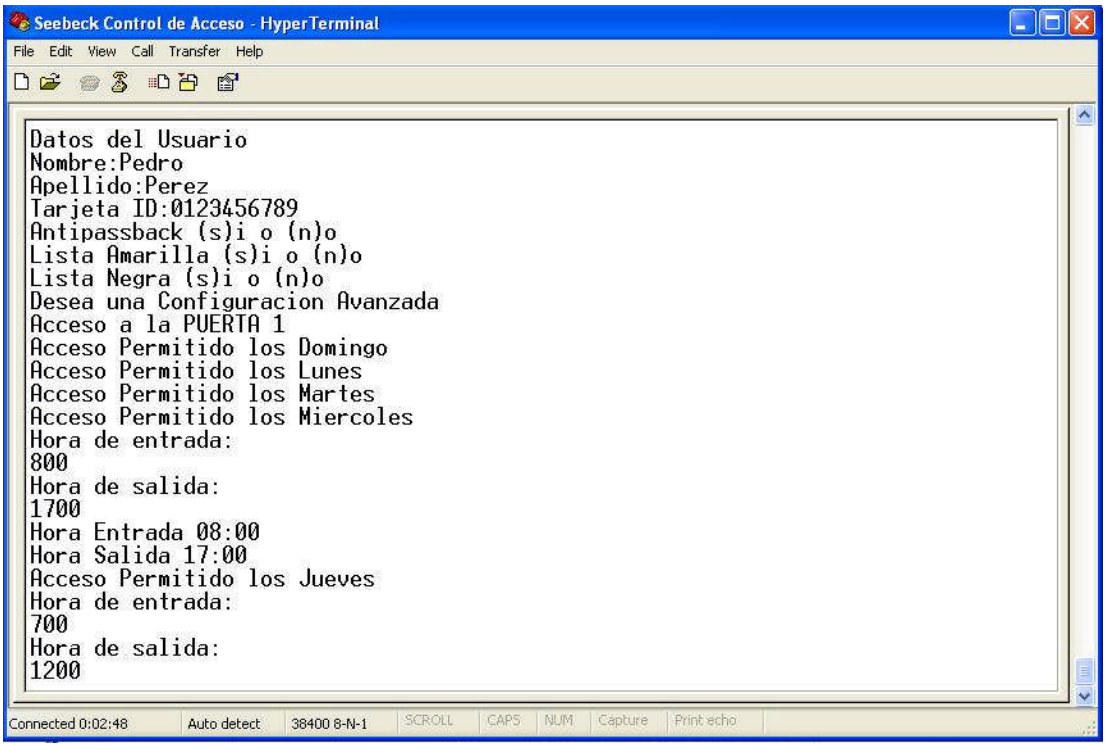


Figura 17: Configuración de usuarios CA Seebeck HyperTerminal

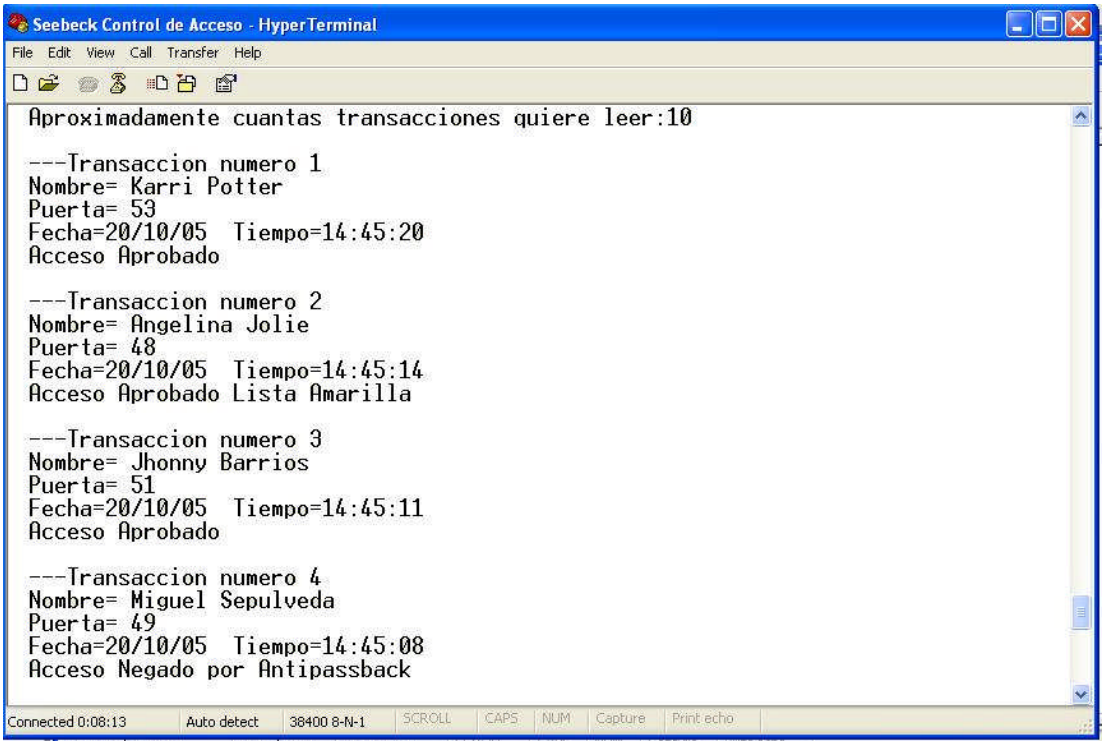


Figura 18: Descarga Transacciones CA Seebeck HyperTerminal

La lectura de las transacciones, se puede realizar indicando el número de transacciones a descargar. Para ello se puede hacer una captura de los datos recibidos en Hyperterminal y guardarlos en un archivo con formato de texto para posteriormente ser leído en aplicaciones como Wordpad o ser leídas directamente en la consola de HyperTerminal, como se puede ver en la Figura 18.

5.4.2 Agilent VEE PRO

Una segunda interfaz fue desarrollada en Agilent VEE PRO 7.0 con el propósito de brindar un sistema más amigable a los usuarios que administrarían el control de acceso, ya que muchos de ellos son personas no familiarizadas a interfaces como las de Hyperterminal. Por lo tanto se realizó una interfaz de fácil uso, con la cual los usuarios puedan sentirse cómodos y entender la configuración del sistema de control de acceso (Ver Figura 19).

Esta interfaz funciona mediante un protocolo, que se comunica con el controlador embebido, el cual constantemente verifica si el usuario ha solicitado una función mediante la interfaz gráfica. A diferencia de Hyper Terminal aquí se puede ver la hora, configurar usuarios, leer transacciones mientras se monitorea el acceso de usuarios en el sistema. Posee además un botón de apertura de emergencia, que abre todas las puertas del sistema, en caso tal de que haya una alarma o necesidad de evacuar la localidad.

La configuración de puertas y zonas se puede realizar a través de esta interfaz. Como se puede ver en la Figura 20, las direcciones de las lectoras presentes en el sistema, son configuradas por pares, formando puertas, las cuales pueden ser configuradas, como puertas normales o con antipassback.

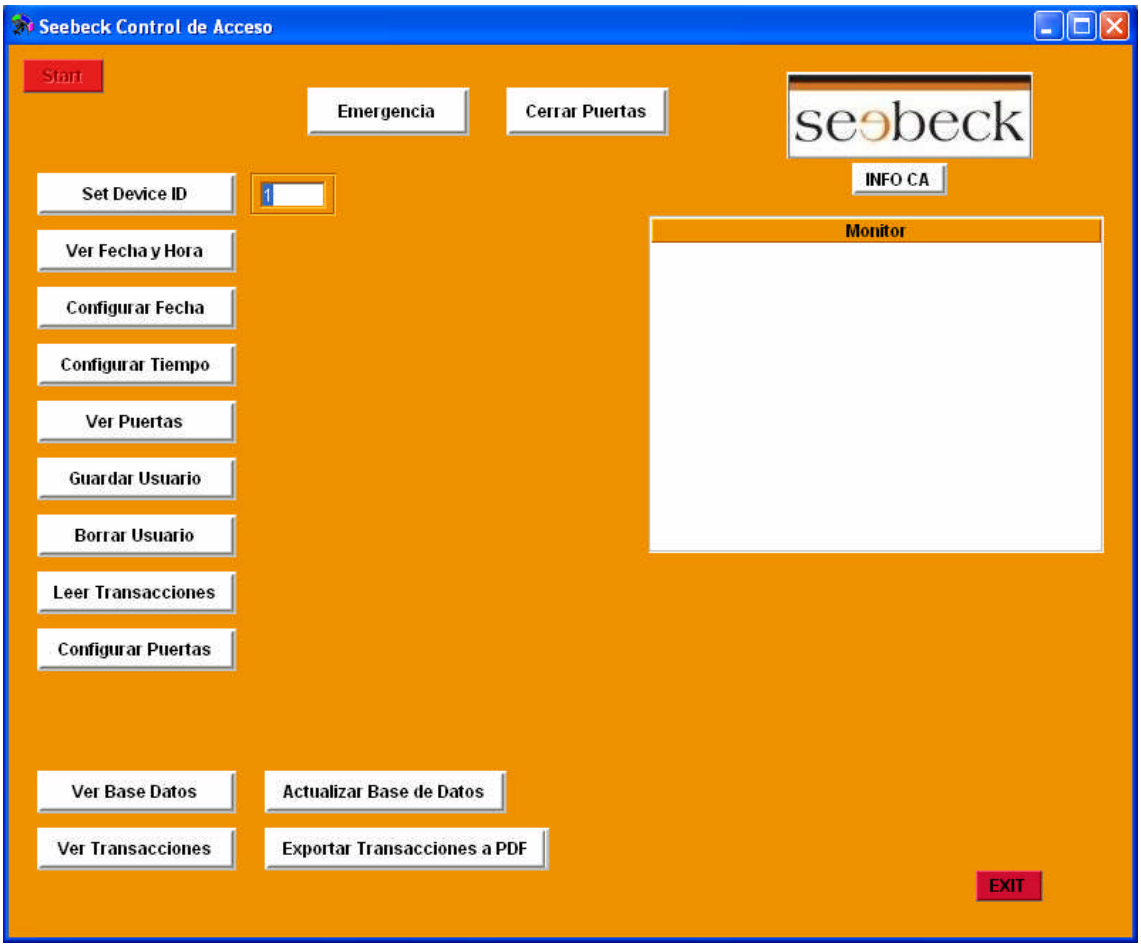


Figura 19: Menú Principal CA Seebeck Agilent VEE PRO

Figura 20: Menú Configuración de Puertas CA Seebeck Agilent VEE PRO

La ventana de configuración de usuarios, se puede ver en la Figura 21, ésta contiene campos que deben ser llenados para configurar nuevos usuarios en el sistema. Las restricciones, puertas de acceso, días de la semana y horarios son asignados a través de esta ventana. Es importante resaltar que las capacidades del sistema no establecen un mismo horario para cada puerta, pero el prototipo de interfaz desarrollado en Agilent VEE Pro, establece un mismo horario cada puerta.

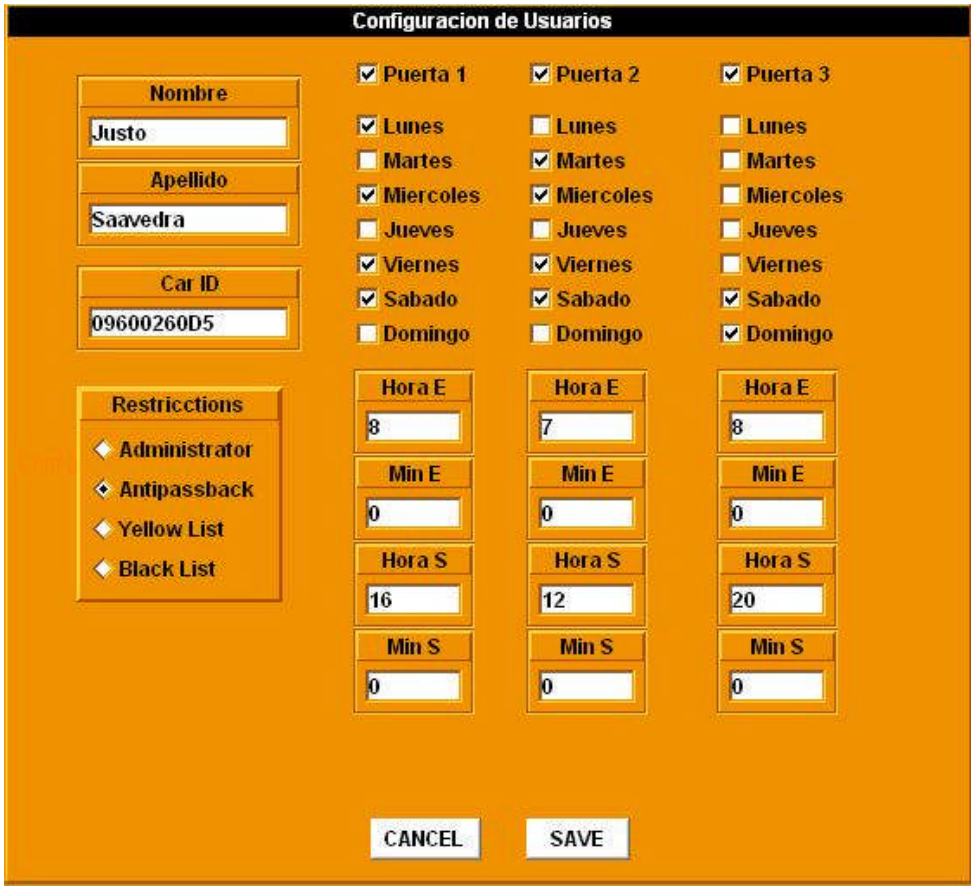


Figura 21: Menú Configuración de Usuarios CA Seebeck Agilent VEE PRO

Por otra parte la lectura de las transacciones se realiza indicando el número de transacciones a descargar. Estas se descargan hacia una archivo de texto .txt el cual se abre automáticamente finalizada la descarga, ejecutando el programa wordpad (Ver Figura 22). Las transacciones contienen información acerca de los usuarios, puertas solicitadas, fecha, hora y validez de la operación. El número de transacción indica la transacción más reciente, siendo esta la numero uno (1) y así sucesivamente. Dependiendo de la cantidad de transacciones a ser leídas el proceso tardara más o menos.

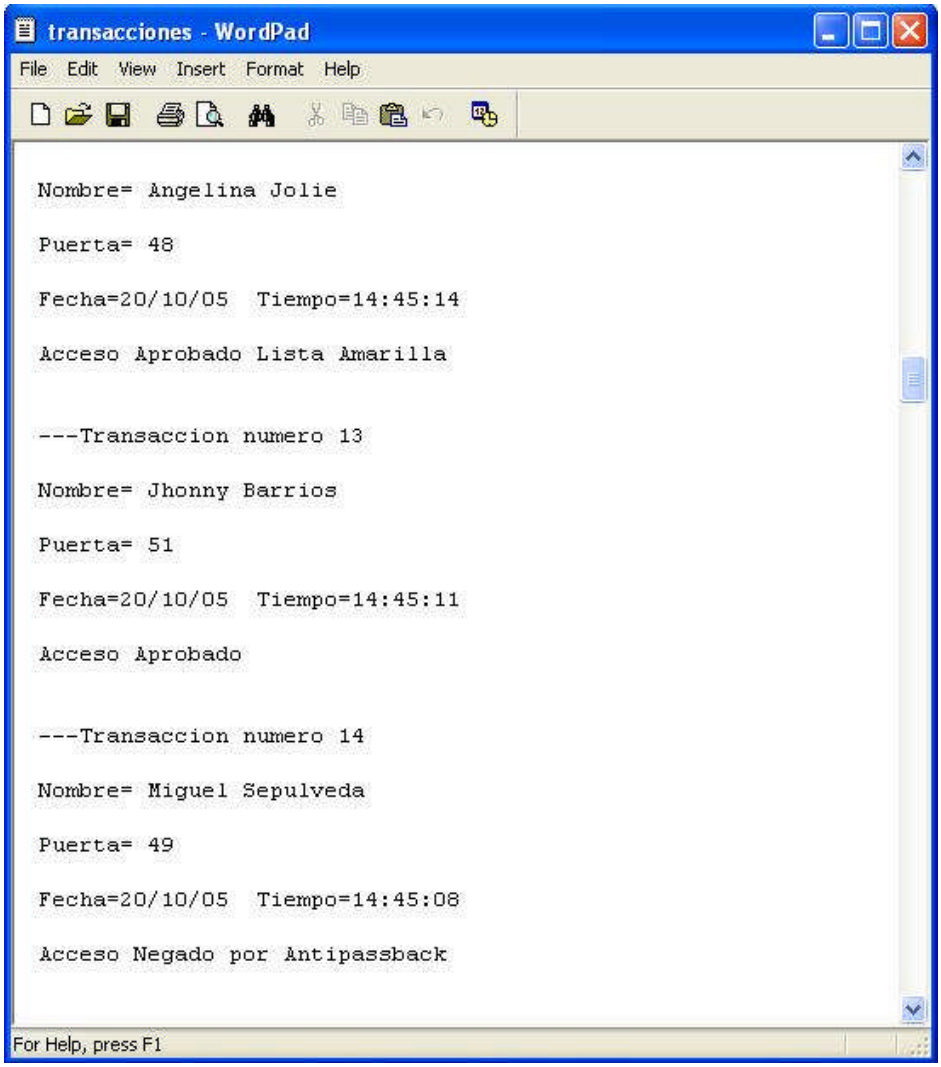


Figura 22: Transacciones.txt CA Seebeck Agilent VEE PRO

Otro aspecto importante es el manejo de la base de datos, la cual fue desarrollada en lenguaje SQL (Lenguaje de Búsqueda Estructurado). A través del botón (**Ver Base Datos**) se pueden visualizar los usuarios existentes en el sistema de control de acceso (Ver Figura 23). Este permite ver el nombre, apellido, y CarnetID de cada uno de los usuarios grabados en el sistema. Si se desea borrar algún usuario se procede a hacer un clic sobre la base de datos, en la celda que corresponda al nombre, apellido o NumeroID del usuario a borrar.

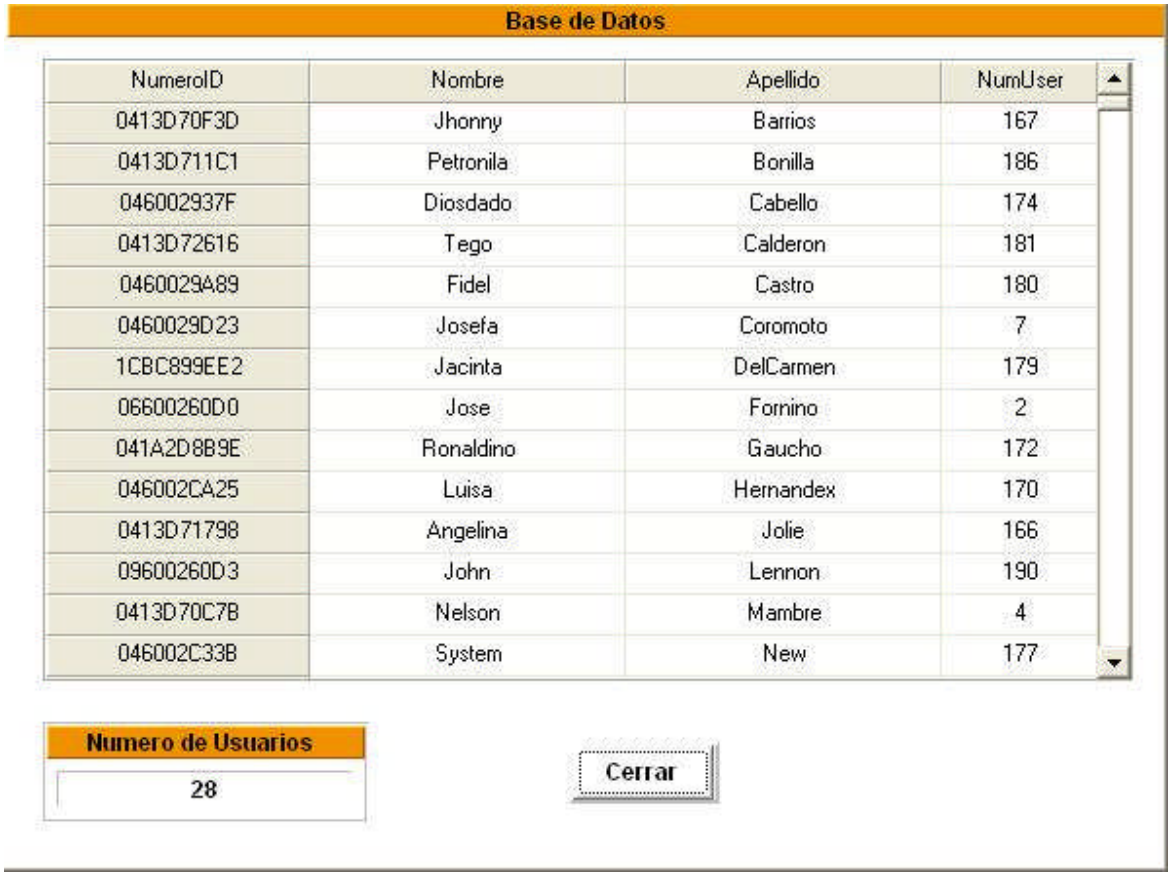


Figura 23: Base de Datos

Al hacer clic sobre el usuario, aparece un aviso que indica el nombre del usuario a eliminar, para de esta forma confirmar o abortar la eliminación (Ver Figura 24)

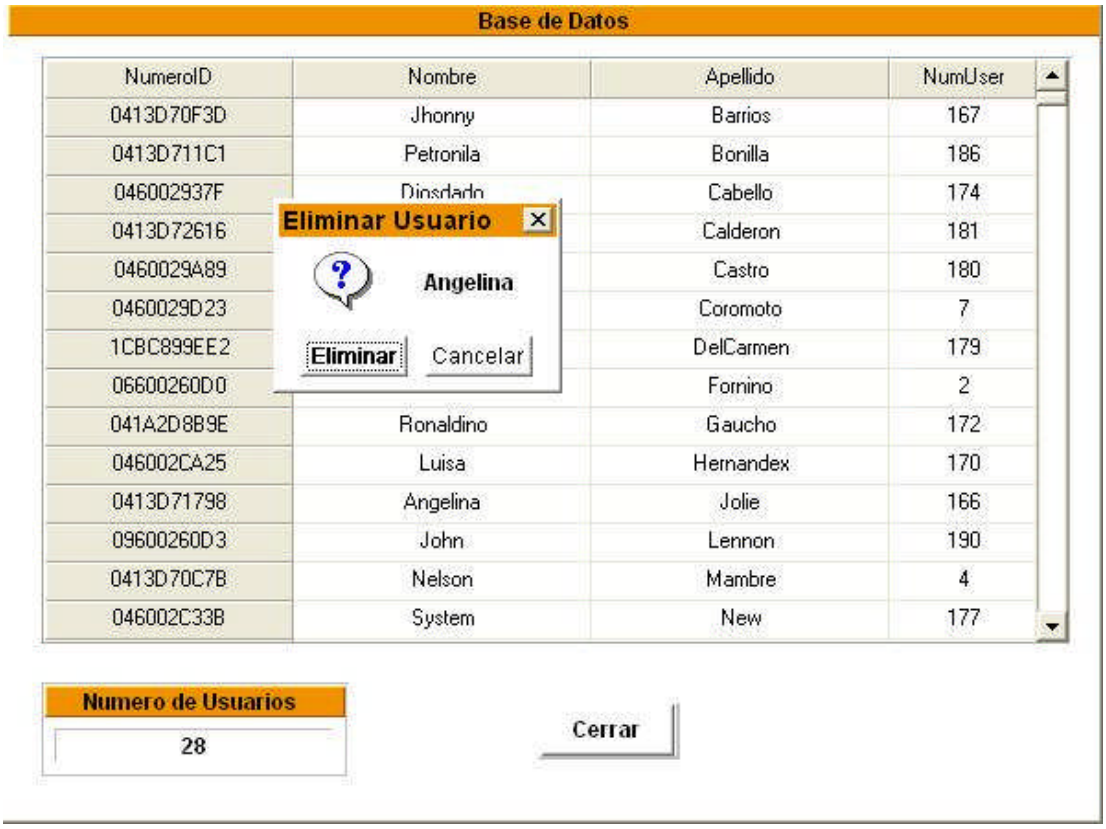


Figura 24 : Eliminar Usuario en la Base de Datos

5.6 PRUEBAS REALIZADAS AL SISTEMA

Las pruebas realizadas al sistema contribuyeron en gran parte a la mejora y desarrollo del mismo, ya que a medida de que se programaba el sistema, éste era probado por bloques. En gran parte de los casos, las pruebas conducían a una mejora o modificación del código debido a detalles que se pasaban por alto en la programación y que sólo eran visibles a la hora de la simulación del sistema.

A partir de la función **ToCom(Port,Data)** fue posible visualizar tanto el avance del sistema, como el valor de ciertas variables importantes, pudiéndose de esta forma verificar la correcta operación del sistema. Posteriormente, toda esta información proveniente del módulo hacia la interfaz del usuario. fue comentada

debido a que solamente constituía información acerca del funcionamiento del sistema, la cual es irrelevante para el usuario. A continuación se explicarán algunas de las pruebas más importantes al sistema.

5.6.1 Guardar Usuarios y Verificación de Perfiles Mediante Pruebas

Una de las funciones más importantes del sistema corresponde a la escritura y lectura apropiada de la base de datos, debido a que esta es la que caracteriza al sistema de control de acceso como seguro y confiable.

Para probar la función de GuardarUsuarios, se realizaron numerosas pruebas las cuales consistían en guardar un usuario con características específicas de perfiles, horarios, días de la semana y puertas de acceso para luego probar su correcta lectura y procesamiento.

Esta prueba fue realizada por fases; primero se configuraban usuarios determinando las puertas a las cuales podían acceder y seguidamente se probaba el sistema, a fin de determinar si el sistema procesaba correctamente las peticiones hechas por los usuarios. Posteriormente se implementaron a las configuraciones, los días de la semana, los cuales originaron errores por fallos presentados en las funciones ejecutadas, estas fueron corregidas y nuevamente probadas. Terminada esta fase se implementaron los horarios para cada uno de los días de la semana. Para ello se configuraron varios usuarios con diferentes horarios, diferentes días de la semana con determinadas puertas, a fin de probar toda la función. Se realizaron ajustes en las funciones debido a fallas presentadas en el procesamiento de los horarios, debido a que las horas de salida no eran leídas correctamente en el sistema.

Luego de los ajustes realizados, el resultado final fue que los usuarios configurados en el sistema eran correctamente procesados tanto en sus horarios, días y puertas asignadas. Las pruebas se realizaron configurando

aproximadamente 40 usuarios con perfiles diferentes, para posteriormente confirmar el correcto procesamiento de los mismos.

5.6.2 Lectura de Transacciones y posterior descarga para su comparación

La escritura adecuada de las transacciones es un factor relevante en el sistema de control de acceso, ya que a través de su lectura se puede verificar el acceso de los usuarios a una empresa y de forma adecuada se puede controlar y verificar las entradas/salidas de un usuario. Es por ello que esta sección del programa debido a su importancia requiere pruebas rigurosas que garanticen su correcto funcionamiento.

Las pruebas fueron las siguientes. A través del programa **RealTerm** se capturó la lectura de usuarios que eran procesados por el sistema de control de acceso, se hicieron pruebas con 50, 100, 200, 500 usuarios. Posteriormente se descargaban las transacciones en otro archivo el cual era comparado en detalle con el procesamiento de usuarios.

Se presentaron problemas debido a la pérdida de datos, los cuales posteriormente fueron resueltos. Su causa se debió a problemas con el tamaño del buffer de recepción del programa desarrollado en AgilentVEE.

5.6.3 Tiempo de apertura de puertas

A través de las salidas del controlador embebido así como de las salidas correspondientes al módulo entradas/salidas de relé, se probó el sistema en función del tiempo de apertura de las puertas, el cual oscilaba entre 5 y 10 segundos. También se conectaron leds a las salidas del módulo entradas/salidas de relé para visualizar los tiempos de aperturas de las puertas. Estas pruebas llevaron a ajustes de los tiempos de apertura, los cuales eran ejecutados por un temporizador dentro del CPU.

5.6.4 Optimización de Base de Datos

La función de optimización de base de datos fue probada de la siguiente manera. Se guardaron en la base de datos 50 usuarios, algunos de ellos fueron invalidados y posteriormente vueltos a grabar, de esta forma quedaban páginas invalidadas en la memoria. El número total de usuarios entre activos e invalidados en el sistema eran aproximadamente 80. Se hacia correr la función de optimización cuando el número de usuarios llegara a más de 80 usuarios. Posterior a la corrida de la misma, los bloques inválidos fueron borrados y los datos correspondientes a los usuarios fueron copiados satisfactoriamente, desfragmentando el espacio de memoria correspondiente a la base de datos. Las primeras corridas generaron errores ya que se perdían bloques enteros, debido a la fallas en las escrituras del buffer de optimización, se fue mejorando el desempeño de la función, hasta lograr los resultados deseados. Para verificar el correcto funcionamiento se hicieron alrededor de 20 pruebas similares a fin de corroborar su correcto funcionamiento.

A través de un sencillo programa desarrollado a fin de verificar la data en la memoria Flash llamado FLASHREADER, en el cual se puede verificar los datos de la memoria por bloques y páginas, se pudo verificar la optimización correcta de la base de datos en la memoria.

5.6.5 Escritura y lectura de la memoria cíclica por 6 periodos consecutivos

La memoria cíclica fue probada aproximadamente 30 veces. Para ello se implementó una función de prueba la cual guardaba transacciones cada cierto tiempo en la Memoria Flash, con el nombre “Transacción Nro XX”. La prueba consistía primeramente en reducir el espacio de memoria asignado a las transacciones, para ello se modifico la definición de bloques asignados a las transacciones en el código fuente del programa, reduciendo la capacidad

de escritura a 576 transacciones. Posteriormente luego de aproximadamente 20 horas, se estimó según el temporizador implementado, que la memoria habría cumplido 6 ciclos de escritura, las transacciones fueron descargadas y se verificó que la escritura de la memoria fue satisfactoria, ya que cumplió los ciclos de borrado para así poder grabar nuevas transacciones. Es importante resaltar que la Memoria Flash no se puede sobrescribir, por lo que requiere de un proceso de borrado especial, de tal forma que si el proceso no se hubiese hecho de la forma correcta, la lectura hubiese mostrado los fallos.

Antes de esta prueba se realizaron pruebas menores con el objeto de monitorear detalladamente el proceso de escritura cíclica, a fin de no perder detalle y así poder verificar el correcto funcionamiento, en el momento de ejecutar los ciclos.

La lectura cíclica de la memoria también fue satisfactoria. Esta se basa en leer la última transacción hecha, hacia la primera.

5.6.6 Pruebas Antipassback

La función antipassback es una de las más requeridas por los clientes que solicitan el sistema de control de acceso, por lo tanto esta debe funcionar correctamente. Las pruebas hechas a esta función están contempladas desde el instante en que se empezó el desarrollo de la misma, hasta que se verificó su perfecto funcionamiento. Posteriormente no se han presentado errores debido al modo de implementación, que se basa en la búsqueda de transacciones anteriores.

Al principio, las búsquedas de transacciones anteriores originaban errores debido a que no se tomaban en cuenta la validez de las transacciones hechas, originando de esta forma errores en la ejecución de la función, ya que el sistema no diferenciaba si el usuario había entrado o sencillamente se la había negado el acceso anteriormente. Se hicieron los ajustes necesarios,

incluyendo en la función la verificación de la validez de las transacciones realizadas y se sometió el sistema a diversas pruebas, que mostraron la efectividad de la función.

El modo de probar el sistema de una forma rigurosa, se basa en acceder por una entrada o salida de una puerta y posterior a eso, realizar varias operaciones en lectoras distintas a las correspondientes a esa puerta. Luego se vuelve a efectuar la misma operación, la cual origina una restricción, indicando que el usuario, esta realizando una petición corrupta.

5.6.7 Pruebas de Zonas

Las pruebas a las zonas contemplan las pruebas antipassback pero realizadas en grupo. Para ello se define una zona y se realizan varias operaciones entre las puertas de entrada y las puertas de salida. Debido a que existen varias lectoras asignadas para las entradas y salidas de una zona, se incorporó a la función antipassaback, la capacidad de reconocer en sus búsquedas cada una de las lectoras asignadas a la zona especifica, mediante un arreglo que contenía la dirección de las lectoras de entrada y de salidas, agrupadas de forma ordenada.

5.6.8 Pruebas a la puerta principal

A través de la maqueta, de una puerta mostrada en la Figura 25, la cual dispone de sensores y una cerradura eléctrica, se puso en marcha el control de una puerta principal, guardando transacciones más elaboradas que contienen información acerca de que si el usuario abrió la puerta, no la abrió o la dejó abierta, con el objeto de monitorear mas detalladamente el control de una puerta.

Figura 25: Maqueta de la Puerta

Las pruebas se hicieron varias veces con la maqueta. Esta también cuenta con un botón de emergencia que fue conectado a modo de interruptor de la secretaria, del cual también quedaba guardada la transacción correspondiente.

5.6.9 Tiempo de Procesamiento

El tiempo de procesamiento de los datos desde que el usuario ingresa un carnet y es leído, fue puesto a prueba. Estos tiempos oscilan entre los 0.5 segundos y 2.5 segundos. Al presentar un carnet no identificado en el sistema, este es comparado con 2500 posibles usuarios, tomándose el tiempo máximo de 2.5 segundos, lo cual constituye una prueba rigurosa.

Como conclusión los tiempos son bastantes adecuados y se adaptan bien, si se quiere mas rapidez de procesamiento se puede implementar en el controlador embebido un CPU de mayor velocidad.

5.7. FUTURAS IMPLEMENTACIONES

5.7.1 Función Trampa

Esta función puede ser requerida por clientes. Esta se basa en que una puerta no puede ser abierta mientras otra no esté cerrada, es de uso común en bancos y zonas que requieren de alta seguridad. Para ello se deben tener sensores especializados, que integrados al sistema de control de acceso nos permitirán realizar los procedimientos de forma adecuada.

5.7.2 Función Solitario

Esta función es de alta seguridad. Se basa en la restricción del número de personas, que pueden estar en una zona en específico. Para ello el sistema de control de acceso debe ser integrando a ciertos sensores, que permitan recaudar información fiable sobre la cantidad de personas presentes en una zona en específico y de esta forma tomar las acciones correspondientes. En el caso de que el número de personas en la zona haya superado el máximo, entonces se restringirá el acceso del personal hacia esa zona o de lo contrario permitirá el acceso.

5.7.3 Control de Acceso basado en reconocimiento de huellas dactilares

El programa cargado al controlador embebido referente al sistema de control de acceso toma los datos pertenecientes a la lectoras, pero su sistema puede ser migrado a otras tecnologías como la de huellas dactilares, puesto que las funciones no cambian, solamente el modo de lectura y seguramente el largo de la data a verificar, comparar y procesar cambiaría, por lo tanto el código es reusable y por ende, la migración hacia otro sistema es fácil de implementar.

6. CONCLUSIONES

A través del diseño y desarrollo del proyecto, se verificó la importancia que tienen cada una de las etapas (investigación, diseño, implementación y pruebas) en la ejecución de un proyecto, ya que el éxito de cada una de ellas, depende directamente del resultado de la etapa anterior. El estudio previo de ambos sistemas de memoria y el posterior diseño del manejo e implementación de las estructuras en la memoria Flash, contribuyeron directamente en el éxito del sistema de control de acceso. La decisión de implementar la memoria Flash en el sistema, fue el factor determinante en la ejecución del proyecto, ya que esta representa dieciséis (16) veces más memoria que la implementada en el sistema de control de acceso anterior basado en uso de Memoria SRAM, proveyendo de esta forma mayor capacidad de almacenamiento de transacciones, y mas memoria útil para configuraciones específicas de cada usuario. En cuanto a la pérdida de información, este módulo posee mucha más seguridad, ya que aguanta cortes de energía debido a que es una memoria no volátil, por lo que representa una opción confiable en la implementación de un sistema de control de acceso.

Por otra parte, se implementaron nuevas y distintas funciones que permiten una gran flexibilidad en el manejo de los usuarios, pudiendo configurar para cada uno de ellos, distintas horas de entrada y de salida por cada día de la semana por cada una de las puertas de acceso. El sistema también integra funciones automáticas para el mantenimiento tanto de la base de datos como de las transacciones guardadas, las cuales optimizan el espacio en memoria, evitando así que el sistema colapse y pueda trabajar continuamente, teniendo como resultado una mayor eficiencia. El SCA permite la configuración individual de más de mil (1000) usuarios en el sistema, conjuntamente con la capacidad de almacenar más de setenta mil (70.000) transacciones, lo cual se traduce en flexibilidad, rendimiento y seguridad en cuanto al manejo de la base de datos e información recaudada de las transacciones realizadas por los usuarios, brindando de esta manera confiabilidad y seguridad.

El sistema fue desarrollado de lo general a lo específico. El procedimiento era probar el funcionamiento básico de las funciones en el sistema y posteriormente se desarrollaban las mismas, verificando su funcionamiento en detalle. El prototipo desarrollado cumplió con todas las especificaciones propuestas, mejorando notablemente los desarrollos anteriormente realizados, en cuanto a capacidad y flexibilidad de configuración de usuarios. El sistema fue probado y actualmente el prototipo posee la capacidad para cumplir con el control de acceso en una localidad de hasta ocho (8) puertas. Por su parte las funciones relacionadas al manejo de zonas y antipassback, están operativas y cumplen con su función.

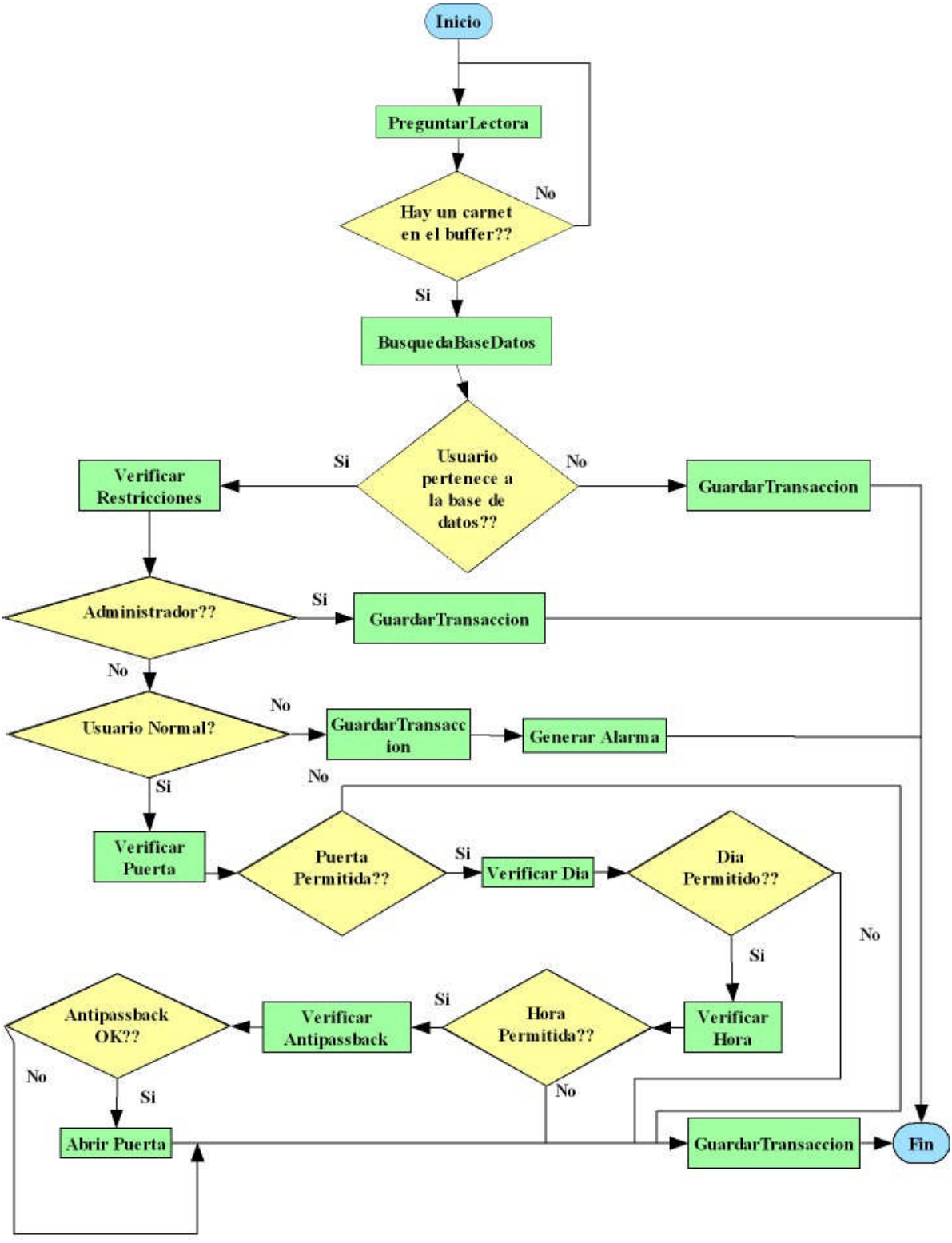
El sistema de control de acceso posee limitaciones debido a las lectoras RFID PROMAG. Estas lectoras poseen direcciones las cuales pueden ser externamente modificadas mediante pines de configuración. Su limitante es que el rango de direcciones comprende un rango entre las direcciones (0 – 15), lo cual nos da 16 lectoras. Esto constituye una limitante para el sistema de control de acceso ya que nos limita para controlar 16 lectoras. Como opción alternativa se pueden configurar 32 lectoras en el mismo controlador, conectando 16 lectoras a una velocidad de 9600 bps y las otras 16 lectoras a 19200 bps. De esta manera se podrían conectar dos lectoras con igual dirección física, evitando conflictos.

El manejo y aprendizaje de varias herramientas de desarrollo, estuvieron involucrados en el desarrollo del proyecto. Entre las herramientas utilizadas se encuentra Agilent VEE Pro 7.0, con la cual se pueden crear interfaces amigables que comuniquen a los usuarios con los equipos, a través de una computadora, permitiendo de esta forma monitorear y configurar parámetros del sistema de una manera sencilla y apropiada. Otra lenguaje importante aprendido y empleado fue SQL (Lenguaje de Búsqueda Estructurado), a través del programa MySQL, el cual fue integrado al sistema de control de acceso a través de la interfaz primaria, con el objetivo de manejar las bases de datos correspondientes a los usuarios y las transacciones realizadas, permitiendo llevar un control adecuado y característico de un control de acceso. También el empleo de varios controles Activex (Activex

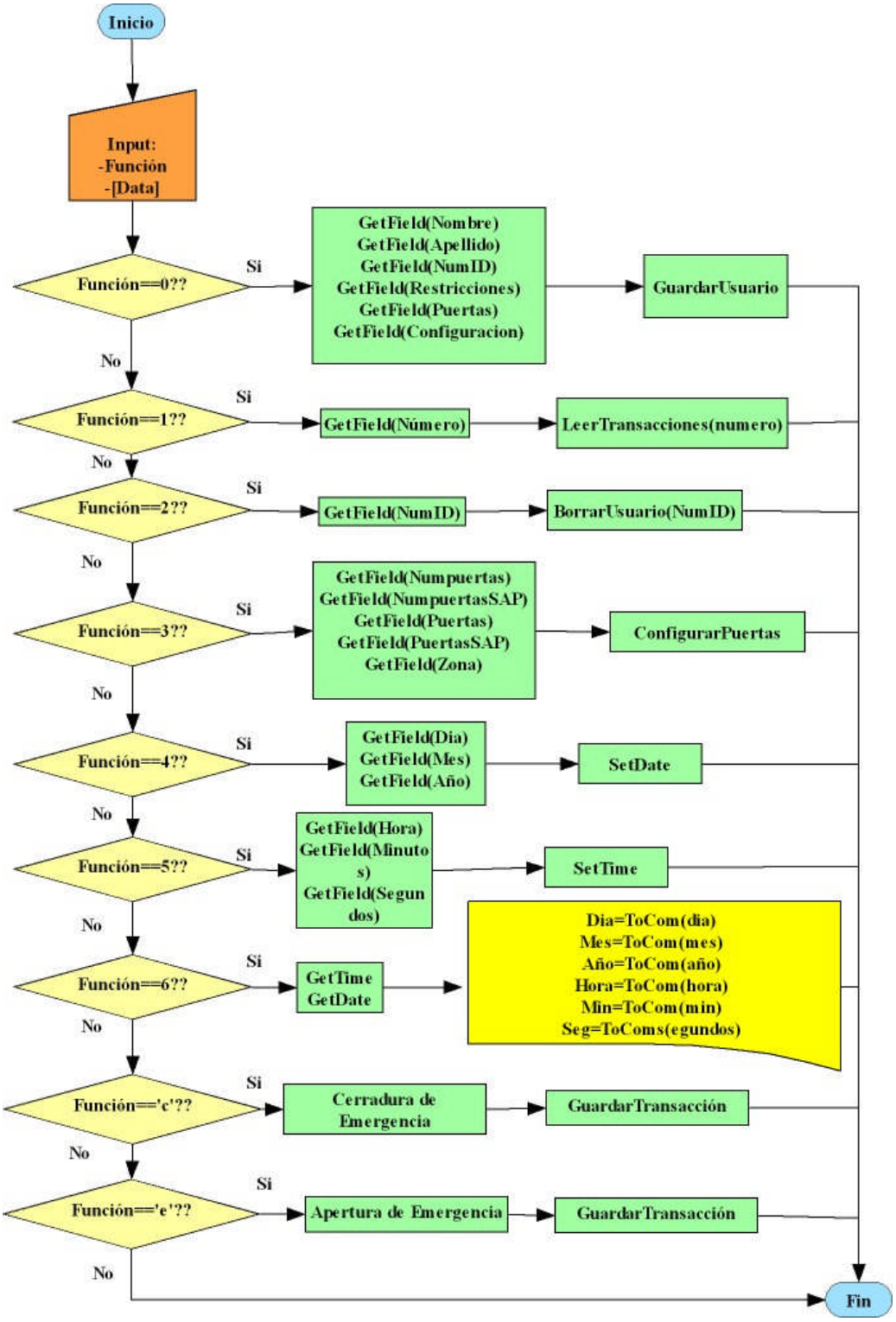
Controls) estuvieron presentes, los cuales fueron muy importantes, ya que permitieron realizar la comunicación entre las bases de datos y la interfaz primaria desarrollada en Agilent, a través de ADO (ActiveX Data Objects) y otros como SCGrid y ReportManager, que estuvieron presentes con el objetivo de mejorar la presentación de la interfaz primaria, lo cual constituye un aspecto fundamental, ya que a través del software, interactuamos hoy en día con los diversos sistemas electrónicos.

En cuanto a los desarrollos referentes a la interfaz grafica bajo Agilent VEE Pro y que abarcan el manejo de bases de datos desarrolladas en SQL, constituyen un primer avance para el desarrollo de una aplicación final, que conjuntamente con el sistema electrónico del control de acceso formen un solo producto hardware/software propio de la empresa, que garantice el optimo funcionamiento del sistema y que se adapte a las realidades del mercado nacional.

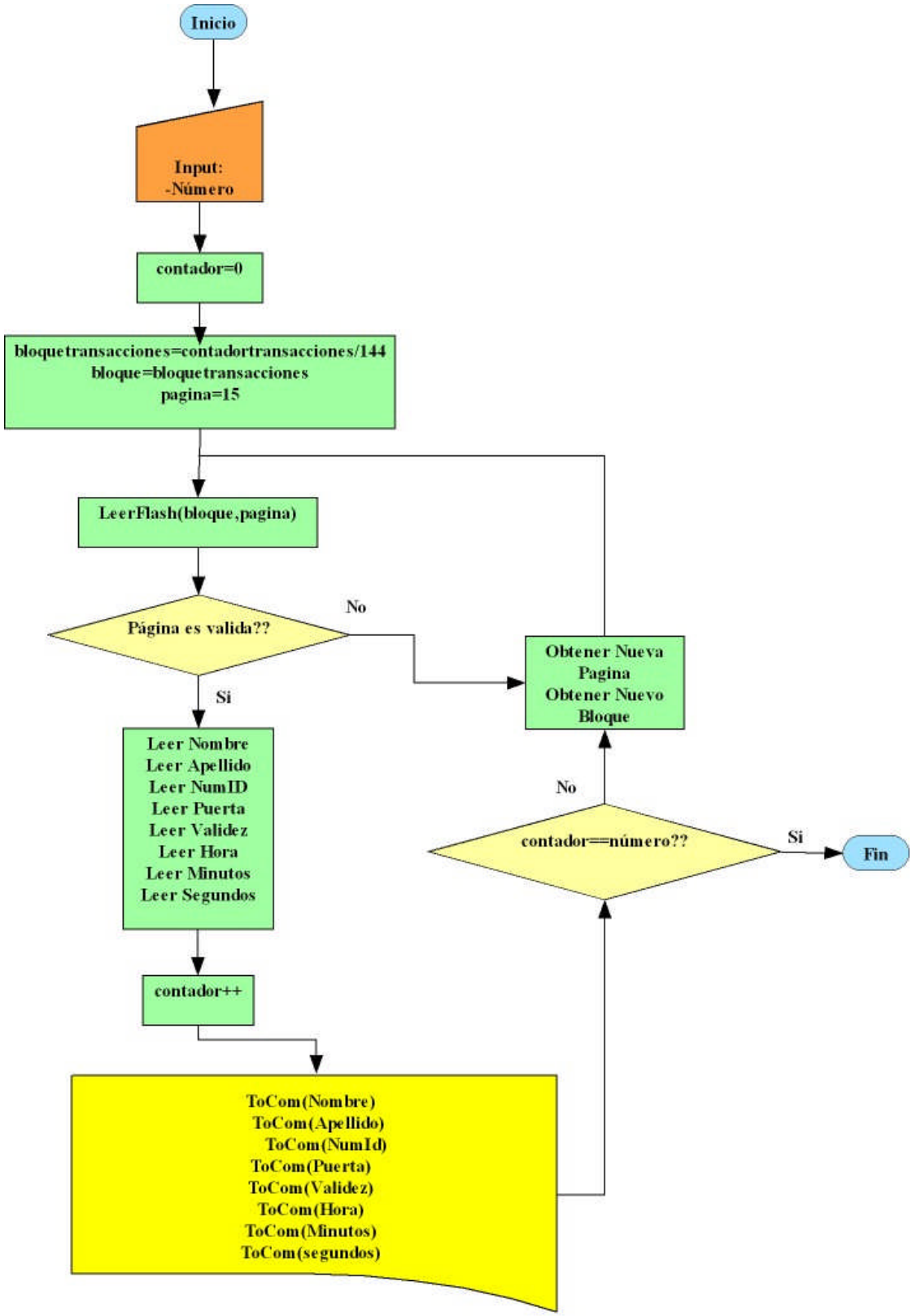
ANEXO A: DIAGRAMA DE FLUJO FUNCIÓN “FUNCIÓN PRINCIPAL”



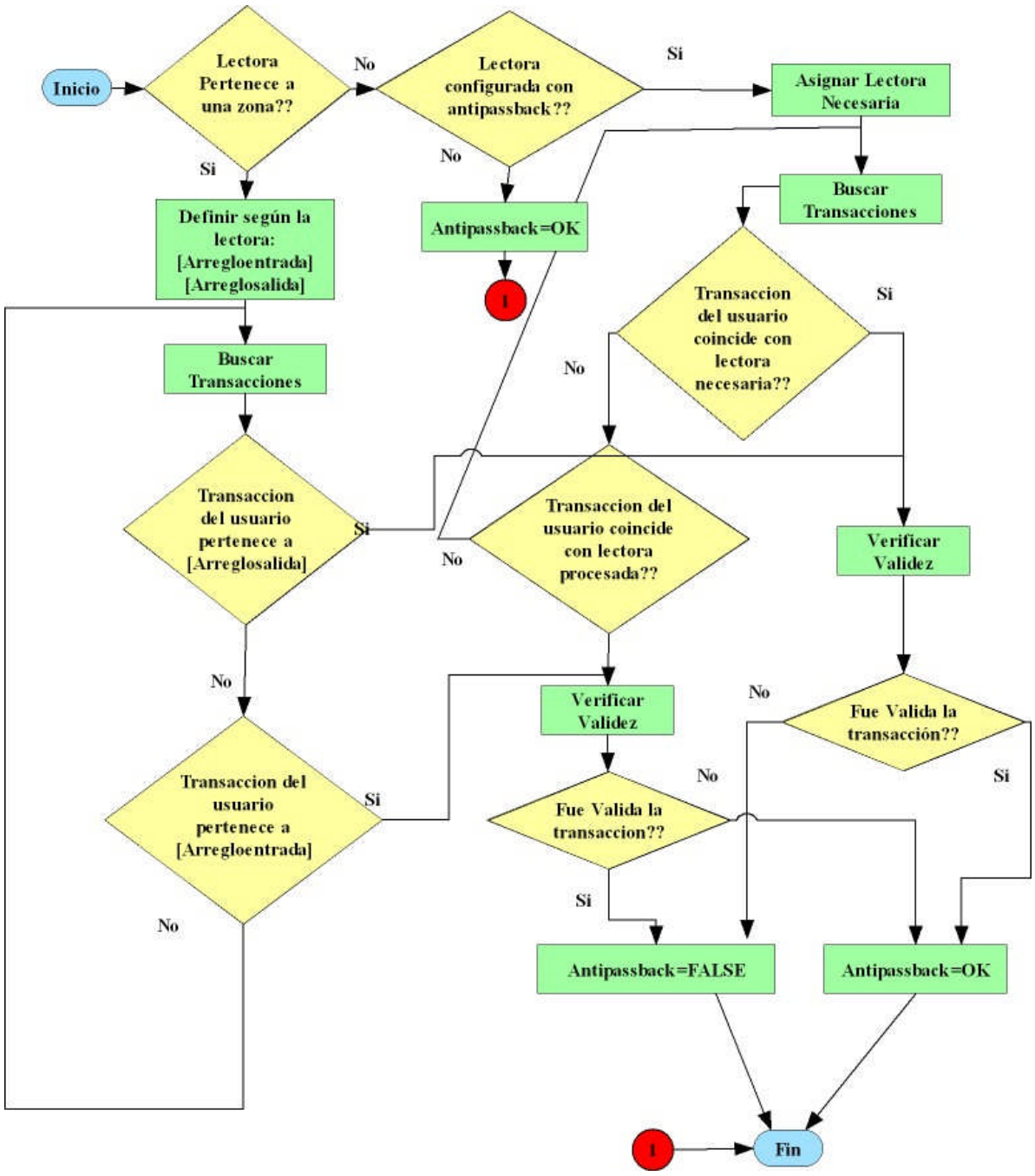
ANEXO B: DIAGRAMA DE FLUJO FUNCIÓN "PROCESS MESSAGE"



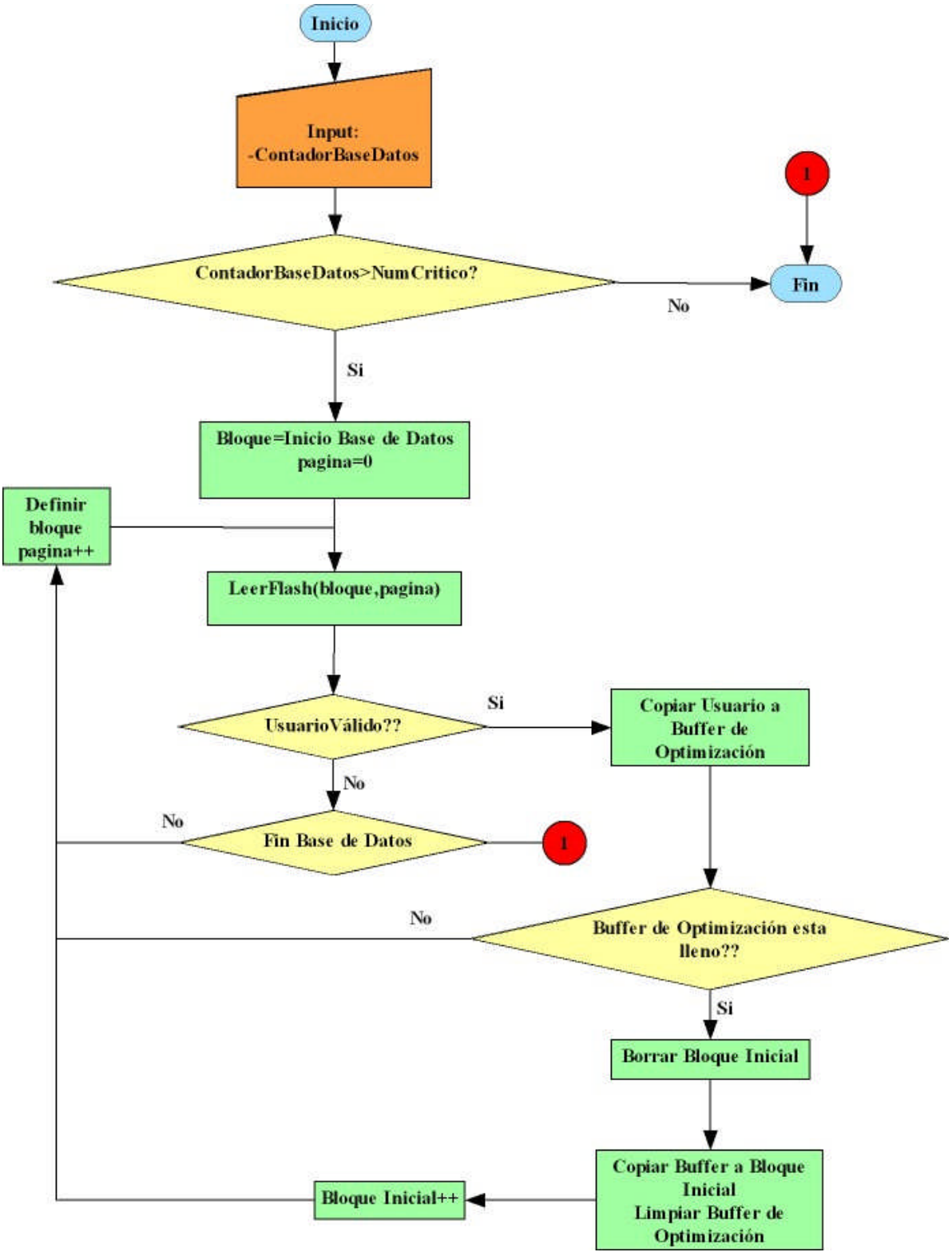
ANEXO C: DIAGRAMA DE FLUJO FUNCIÓN “LEER TRANSACCIONES”



ANEXO D: DIAGRAMA DE FLUJO FUNCIÓN “ANTIPASSBACK”



ANEXO E: DIAGRAMA DE FLUJO FUNCIÓN “OPTIMIZAR BASE DE DATOS”



7. REFERENCIA BIBLIOGRAFICAS

[1] Schildt, Herbert. “Turbo C/C++ 3.1 Manual de Referencia”. McGraw Hill 1994

[2] Dubois, Paul. “MySQL™ The definitive guide to using, programming, and administering MySQL 4.1 and 5.0 Third Edition”. Sams 2005

[3] “Agilent VEE Pro. User Guide”. Agilent Technologies 2003

[4] Colby, Jhon & Wilton, Paul. “Begining SQL”. Wrox 2004

[5] Finkenzeller, Klaus. “RFID Handbook Second Edition”. Jhon Whiley & Sons 2003

[6] “SCGrid Activex Control – Version 6”. 2000.

[7] Manual del Controlador Embebido

[8] Memoria Flash. Disponible en: **http://es.wikipedia.org/wiki/Memoria_flash**

[9] How Flash Memory Works. Disponible en: **http://computer.howstuffworks.com/flash-memory1.htm**

[10] Memoria Ram. Disponible en: **http://es.wikipedia.org/wiki/RAM**

[11] RFID. Disponible en: **http://es.wikipedia.org/wiki/RFID**

[12] Sistema Embebido. Disponible en: **http://es.wikipedia.org/wiki/Sistema_embebido**

[13] About RFID. Disponible en: **http://www.rfid-handbook.de/rfid/**

[14] Introduction to RFIF. Disponible en: **http://www.rfidc.com/docs/introductiontorfid.htm**

[15] Arquitectura Von Neumann. Disponible en: **http://es.wikipedia.org/wiki/Arquitectura_Von_Neumann**

[16] Arquitectura Harvard. Disponible en: **http://es.wikipedia.org/wiki/Arquitectura_Harvard**

[17] MyODBC Whit VB:ADO, DAO and RDO. Disponible en: **http://dev.mysql.com/doc/refman/5.0/en/myodbc-with-vb.html**

[18] ADO Tutorial. Disponible en: **http://www.w3schools.com/ado/default.asp**