ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

CARRERA DE INGENIERÍA AUTOMOTRIZ

DISEÑO Y CONSTRUCCIÓN DE UN CIRCUITO ELECTRÓNICO COMANDADO POR HUELLA DIGITAL PARA LA PUESTA EN MARCHA DE UN VEHÍCULO JEEP GRAND CHEROKEE 5.2 LT.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO AUTOMOTRIZ

CHICAIZA AIMACAÑA LUIS EDISON

MARTÍNEZ TORRES CARLOS ANDRÉS

LATACUNGA - ECUADOR

JUNIO 2010

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA AUTOMOTRIZ

DECLARACIÓN DE RESPONSABILIDAD

Yo: Luis Edison Chicaiza Aimacaña, y

Yo: Carlos Andrés Martínez Torres

DECLARO QUE:

El proyecto de grado denominado: "DISEÑO Y CONSTRUCCIÓN DE UN CIRCUITO ELECTRÓNICO COMANDADO POR HUELLA DIGITAL PARA LA PUESTA EN MARCHA DE UN VEHÍCULO JEEP GRAND CHEROKEE 5.2 LT." ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme a las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Latacunga, Junio de 2010.

_____	_____
Luis Edison Chicaiza Aimacaña	Carlos Andrés Martínez Torres
CI: 0502456338	C.I. 1002816179

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA AUTOMOTRIZ

CERTIFICADO

Ing. Juan Castro (DIRECTOR)

Ing. Sixto Reinoso (CODIRECTOR)

CERTIFICAN:

Que el trabajo titulado "DISEÑO Y CONSTRUCCIÓN DE UN CIRCUITO ELECTRÓNICO COMANDADO POR HUELLA DIGITAL PARA LA PUESTA EN MARCHA DE UN VEHÍCULO JEEP GRAND CHEROKEE 5.2 LT.", ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que constituye un trabajo de excelente contenido científico que coadyuvará a la aplicación de conocimientos y al desarrollo profesional SI recomendamos su publicación.

Latacunga, Junio de 2010.

_____	_____
Ing. Juan Castro	Ing. Sixto Reinoso
DIRECTOR	CODIRECTOR

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA AUTOMOTRIZ

AUTORIZACIÓN

Yo: Luis Edison Chicaiza Aimacaña, y

Yo: Carlos Andrés Martínez Torres

Autorizamos a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la institución del trabajo “DISEÑO Y CONSTRUCCIÓN DE UN CIRCUITO ELECTRÓNICO COMANDADO POR HUELLA DIGITAL PARA LA PUESTA EN MARCHA DE UN VEHÍCULO JEEP GRAND CHEROKEE 5.2 LT.”, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Latacunga, Junio del 2010

_____ _____

Luis Edison Chicaiza Aimacaña

CI: 0502456338

Carlos Andrés Martínez Torres

CI: 1002816179

ÍNDICE

CAPITULO I. 15
INTRODUCCIÓN 1
1.1 ANTECEDENTES GENERALES 1
1.2 PRESENTACIÓN DEL PROBLEMA 2
1.3 PRESENTACIÓN DE LA SOLUCIÓN 4
1.4 OBJETIVOS 5
1.4.1 OBJETIVO GENERAL 5
1.4.2 OBJETIVOS ESPECÍFICOS 5
1.5 DESCRIPCIÓN 5
1.6 FUNCIONALIDADES BÁSICAS 6
CAPITULO II. 7
SISTEMAS DE CONTROL DE ACCESO 7
2.1 SISTEMAS BASADOS EN TARJETAS INTELIGENTES 7
2.1.1 DEFINICIÓN DE TARJETAS INTELIGENTES 7
2.1.2 ARQUITECTURA 8
2.1.3 FUNCIONAMIENTO 9
2.1.4 CLASES DE TARJETAS INTELIGENTES 10
2.1.5 TIPOS DE LECTORES 12
2.1.6 VENTAJAS Y DESVENTAJAS 12
2.1.7 SEGURIDAD EN TARJETAS INTELIGENTES 13
2.2 RFID (IDENTIFICACIÓN POR RADIO FRECUENCIA) 14
2.2.1 COMPONENTES DE UN SISTEMA RFID 14
2.2.2 FUNCIONAMIENTO 15
2.2.3 CONECTIVIDAD RFID 17
2.3. INMOVILIZADOR ELECTRÓNICO BASADO EN RFID 19
2.3.1 GENERALIDADES 19
2.3.2 COMPONENTES DEL SISTEMA: 19
2.3.3 FUNCIONAMIENTO 21
2.3.4 TIPOS DE TRANSPONDERS 21
2.3.5 LAS LLAVES 22

2.3.6 TIPOS DE ANTENAS 23
2.3.7 INMOVILIZADOR FIAT CODE I 24
2.3.8 SISTEMA DE SEGURIDAD PASIVA ANTI ROBO -PATS 26
2.4 SISTEMAS BIOMÉTRICOS 33
2.4.1 DEFINICIÓN 33
2.4.2 CARACTERÍSTICAS 33
2.4.3 TIPOS DE SISTEMAS BIOMÉTRICOS 33
2.4.4 ARQUITECTURA 35
2.4.5 FASE OPERACIONAL DE UN SISTEMA DE IDENTIFICACIÓN PERSONAL 36
2.4.6 EXACTITUD EN LA IDENTIFICACIÓN: MEDIDAS DE DESEMPEÑO 37
CAPITULO III 39
DISPOSITIVO BIOMÉTRICO FIM2030 39
3.1 GENERALIDADES 39
3.2 CUALIDADES DEL SENSOR 42
3.4 VENTAJAS DEL FIM 2030 FRENTE A SENSORES CAPACITIVOS. 44
3.5 DESCRIPCIÓN DEL DISPOSITIVO 44
3.5.1 PRINCIPALES CARACTERÍSTICAS 46
3.5.2 MODELOS 47
3.5.3 APLICACIONES 47
3.5.4 REFERENCIAS DEL PRODUCTO 48
3.6 FUNCIONAMIENTO 49
3.6.1 RESET 49
3.6.2 COMUNICACIÓN 50
3.6.3 ZONA DE DATOS DE USUARIO 50
3.6.4 RELÉS DE SALIDA 50
3.6.5 TECLAS DE FUNCIÓN 51
3.6.6 CONTROLADOR PRINCIPAL 51
3.6.7 FUNCIONAMIENTO DEL SISTEMA DE RELÉ 52
3.7 PROTOCOLO DE COMUNICACIÓN SERIAL 52
3.7.1 ESTRUCTURA DE PAQUETE 52
3.7.2 DEFINICIÓN DE CAMPOS 53
3.7.3 CÓDIGO DE ERROR 54
3.7.4 COMO SE UTILIZAN LOS PAQUETES 55

3.8 GUÍA DE DISEÑO MECÁNICO 56
3.8.1 MONTANDO EL MÓDULO ÓPTICO 56
3.8.2 CONSIDERACIONES ELÉCTRICAS. 58
3.8.3 DESCARGA ELECTROESTÁTICA 58
3.8.4 INICIALIZACIÓN DEL PUERTO SERIAL 59
3.8.5 CONSIDERACIONES AMBIENTALES 60
3.8.6 COMO FUNCIONA 60
3.8.7 CALIDAD DE IMAGEN DE LA HUELLA DACTILAR. 64
CAPITULO IV 68
OTROS DISPOSITIVOS RELACIONADOS AL DESARROLLO 68
4.1 MICROCONTROLADOR PIC 16F877A 68
4.1.1 LA FAMILIA DEL PIC16F877 69
4.1.2 CARACTERÍSTICAS GENERALES DEL PIC16F877 70
4.1.3 DESCRIPCIÓN DE LA CPU 72
4.1.4 ORGANIZACIÓN DE LA MEMORIA DEL PIC 74
4.1.5 OSCILADOR 78
4.2 VISOR 81
4.2.1 CARACTERÍSTICAS FÍSICAS 81
4.2.2 CARACTERÍSTICAS ELÉCTRICAS 83
CAPITULO V. 84
INTEGRACIÓN Y DESARROLLO 84
5.1 IMPLEMENTACIÓN DEL MICROCONTROLADOR 84
5.1.1 INTRODUCCIÓN 84
5.1.2 PROCESO DE IDENTIFICACIÓN 84
5.2 DESARROLLO 88
5.2.1 CONFIGURACIÓN PUERTO SERIAL 88
5.2.2 COMUNICACIÓN Y GENERACIÓN DE INSTRUCCIONES 89
5.2.3 MODO DE USO DE LOS COMANDOS 92
5.2.4 PEDIR LA CONEXIÓN 92
5.2.5 ENROLAMIENTO DEL USUARIO 93
5.3 PROGRAMA EN MICROCODE 96
5.3.1 CONFIGURACIÓN PARA USO DEL LCD 96
5.3.2 MANEJO DE PUERTOS I/O Y DECLARACIÓN DE VARIABLES 97

5.3.3 INICIALIZACIÓN 97
5.3.4 MANEJO DE LA EEPROM 98
5.3.5 CONSIDERACIONES PARA EL CONTROL DE ACCESO 99
5.3.6 TRANSMISIÓN DE PAQUETES DE COMANDO 100
5.3.7 ESTRUCTURA DE PAQUETES DE COMANDO 101
5.3.8 MANEJO DEL TECLADO 102
5.3.9 COMPARACIÓN DE CLAVES 103
5.3.10 CAMBIO DE CLAVE Y ESCRITURA DE EEPROM 104
5.3.11 MENÚ DE FUNCIONES 104
5.3.12 CONTROL DE POTENCIA 104
5.4 INTEGRACIÓN ELECTRÓNICA 105
5.4.1 INTEGRACIÓN DE COMPONENTES 106
5.5 CONTROL DE APERTURA DE PUERTAS POR RFID 113
5.5.1 METODOLOGÍA 113
5.5.2 FUNCIONAMIENTO 114
5.5.3 INTEGRACIÓN DE COMPONENTES 114
CAPITULO VI 118
PRODUCTOS 118
6.1 INTRODUCCIÓN 118
6.2 DESARROLLO DEL PRODUCTO 119
6.2.1 COMPONENTES 119
6.2.2 DISEÑO 120
6.3 PRESENTACIÓN DEL PRODUCTO 122
6.3.1 CARACTERÍSTICAS TÉCNICAS 122
6.3.2 ESPECIFICACIONES TÉCNICAS 122
6.4 FUNCIONAMIENTO 124
6.4.1 PROCESO DE IDENTIFICACIÓN 124
6.4.2 CONTROL DE PUESTA EN MARCHA DEL VEHÍCULO 125
6.4.3 OTRAS SOLUCIONES 126
CAPITULO VII 127
GESTIÓN DE MERCADO 127
7.1 VALOR DISTINTIVO 127
7.2 ANÁLISIS DE MERCADO 127

7.2.1 COMPETENCIA 127
7.2.2 ESTRATEGIA DE VENTA 128
7.2.3 ENFATIZAR LAS ACTIVIDADES DE SERVICIO Y APOYO 129
7.2.4 ESTRATEGIA DE PROMOCIÓN 129
7.2.5 ESTRATEGIA DE FIJACIÓN DE PRECIOS 130
7.2.6 PRODUCTO NUEVO 132
7.2.7 CÓMO RESPONDER A LOS CAMBIOS DE PRECIO 132
7.3 ANÁLISIS DE COSTOS 133
CAPITULO VIII. 138
CONCLUSIONES 139
APÉNDICE A 142
APÉNDICE B 143
APÉNDICE C 144
DESCRIPCIÓN DE COMANDOS 144
BIBLIOGRAFÍA 170
SITIOS WEB 170

ANEXOS 173

ÍNDICE DE FIGURAS

FIGURA 2. 1 Estructura de una tarjeta Inteligente. 8
FIGURA 2. 2 Contactos de una tarjeta inteligente. 10
FIGURA 2. 3 Tarjeta inteligente sin contacto. 11
FIGURA 2. 4 Componentes de un sistema RFID; Funcionamiento de un *sistema RFID* 15
FIGURA 2. 5 Emisión de la señal de baja potencia del lector y entrada del transponder en el campo electromagnético 15
FIGURA 2. 6 Envío de datos por parte del transponder 16
FIGURA 2. 7 Transmisión de los datos contenidos en la memoria del transponder 17
FIGURA 2. 8 Ubicación en el automóvil del sistema inmovilizador Fiat CODE 20
FIGURA 2. 9 Componentes del sistema inmovilizador 20
FIGURA 2. 10 Imágenes de trasponders 21
FIGURA 2. 11 Imágenes de llaves con transponder 22
FIGURA 2. 12 Antena con módulo lector incorporado 23
FIGURA 2. 13 Antena sin módulo lector (solo bobina) 23
FIGURA 2. 14 DIAGRAMA ELECTRÓNICO DEL INMOVILIZADOR FIAT CODE 25
FIGURA 2. 15 UBICACIÓN DE LOS MÓDULOS DEL SISTEMA PATS 27
FIGURA 2. 16 ANÁLISIS DEL CÓDIGO DE LA LLAVE 28
FIGURA 2. 17 CONEXIONADO ELÉCTRICO DEL SISTEMA. 29
FIGURA 2. 18 En el esquema se aprecia la configuración de un FORD FIESTA. 31
FIGURA 2. 19 Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares 36
FIGURA 2. 20 Gráfica típica de FRR y de FAR como funciones del umbral de aceptación (u) para un sistema biométrico 38

FIGURA 3. 1 Diagrama de funcionamiento del sistema biométrico 41
FIGURA 3. 2 Tarjeta controladora del dispositivo biométrico 45
FIGURA 3. 3 SENSOR BIOMÉTRICO 45
FIGURA 3. 4 Diagrama de bloques del FIM2030 49
FIGURA 3. 5 Reset Externo 50
FIGURA 3. 6 Señal de tecla de función 51
FIGURA 3. 7 Conexión entre el fim2030, un microcontrolador y dispositivos externos. 52
FIGURA 3. 8 Estructura del paquete de datos 53
FIGURA 3. 9 Correcta posición del dedo 56
FIGURA 3. 10 Incorrecta posición del dedo 56
FIGURA 3. 11 Dimensiones del lector biométrico 57
FIGURA 3. 12 Dimensiones de la tarjeta controladora del FIM2030 57
FIGURA 3. 13 El efecto de descarga electroestática 59
FIGURA 3. 14 Señal generada por la inicialización del CPU 59
FIGURA 3. 15 Puntos bases en diversos patrones de la huella digital 61
FIGURA 3. 16 Detalles de las huellas digitales 61

FIGURA 3. 17 Trazado del patrón de detalles. 62
FIGURA 3. 18 Proceso de comparación. 63
FIGURA 3. 19 Muestras de huellas con baja calidad 64
FIGURA 3. 20 Correcto posicionamiento del dedo sobre el lector biométrico 65
FIGURA 3. 21 Errores comunes 65
FIGURA 3. 22 ROTACIÓN PERMITIDA 66
FIGURA 3. 23 EXPOSICIÓN DE LA IMAGEN 66

FIGURA 4. 1 PIC 16F877a 69
FIGURA 4. 2 Ciclo de instrucción 73
FIGURA 4. 3 DIAGRAMA DE BLOQUES 75
FIGURA 4. 4 DISTRIBUCIÓN DE PINES 76
FIGURA 4. 5 Cristal externo 79
FIGURA 4. 6 Circuito RC externo 79
FIGURA 4. 7 Oscilador externo 80
FIGURA 4. 8 Visor 81
FIGURA 4. 9 Dimensiones del LCD 82

FIGURA 5. 1 Diagrama de flujo de operación del microcontrolador 86
FIGURA 5. 2 Estructura del paquete de datos 89
FIGURA 5. 3 Diagrama de reconocimiento del comando 91
FIGURA 5. 4 Secuencia de petición de conexión 92
FIGURA 5. 5 Esquema de implementación 106
FIGURA 5. 6 Distribución de pines del circuito integrado max232 107
FIGURA 5. 7 Diagrama de conexión de teclado 108
FIGURA 5. 8 Diagrama de conexión del visor 109
FIGURA 5. 9 Diagrama completo de conexión 111
FIGURA 5. 10 Circuitos de control de dispositivos 112
FIGURA 5. 11 ID-12 113
FIGURA 5. 12 Diagrama de conexión sugerido por ID-Series 114
FIGURA 5. 13 Diagrama de conexión del control de apertura de puertas 115
FIGURA 5. 14 Circuito de control de acceso con ID-12 y Pic16F628A 115

FIGURA 6. 2 Diseño final 121
FIGURA 6. 3 Proceso de identificación 124

FIGURA 7. 1 Fijación de precios basada en el costo 132
FIGURA 7. 2 Factores que afectan en el cambio de precio 133

ÍNDICE DE TABLAS

TABLA 2. 1 ALGUNAS MARCAS DE TRANSPONDERS 22
TABLA 2. 2 TABLA COMPARATIVA DE SISTEMAS BIOMÉTRICOS 35

TABLA 3. 1 ESPECIFICACIONES DEL HARDWARE DE FIM 2030 48
TABLA 3. 2 ESPECIFICACIONES DE OPERACIÓN 48
TABLA 3. 3 SEÑAL DE TECLAS DE FUNCIÓN 51
TABLA 3. 4 CÓDIGO DE ERRORES 54
TABLA 3. 5 EJEMPLO DE PAQUETE DE COMANDO 55
TABLA 3. 6 ESPECIFICACIONES DE ENERGÍA 58

TABLA 4. 1 FAMILIA DEL PIC 16F877A 70
TABLA 4. 2 CARACTERÍSTICAS DEL PIC 16F877A 70
TABLA 4. 3 PERIFÉRICOS 72
TABLA 4. 4 DESCRIPCIÓN DE PINES DEL PIC16F877a 76
TABLA 4. 5 DESIGNACIÓN DEL OSCILADOR 78
TABLA 4. 6 CAPACITORES RECOMENDADOS SEGÚN LA FRECUENCIA DEL OSCILADOR 79
TABLA 4. 7 DISTRIBUCIÓN DE PINES DEL LCD 82
TABLA 4. 8 CARACTERÍSTICAS ELÉCTRICAS DEL LCD DE 16X2 83

TABLA 5. 1 PAQUETE DE COMANDO CMD_REQUEST_CONNECTION 92
TABLA 5. 2 PAQUETE DE RECONOCIMIENTO EXITOSO 93
TABLA 5. 3 PAQUETE DE COMANDO CMD_REGISTER_FP 94
TABLA 5. 4 LISTA DE COMPONENTES 116

TABLA 7. 1 GENERACIÓN DE PLAZOS DE RESPUESTA 128
TABLA 7. 2 COSTOS CONTROL DE ACCESO 134
TABLA 7. 3 INVERSIÓN INICIAL PARA EL CONTROL DE ACCESO 135
TABLA 7. 4 PROYECCIÓN DE PRODUCCIÓN DEL CONTROL DE ACCESO 136
TABLA 7. 5 CALCULO DEL VAN Y TIR PARA EL CONTROL DE ACCESO 137

TABLA A. 1 LISTA DE COMANDOS 142

TABLA B. 1 PAQUETES DE RESULTADOS 143

TABLA C. 1 CMD_REQUEST_CONNECTION....144
TABLA C. 2 CMD_GET_FIRMWARE_VERSION2....144
TABLA C. 3 CMD_DEVICE_INFO....145
TABLA C. 4 CMD_VERIFY_FP....146
TABLA C. 5 CMD_IDENTIFY_FP....147
TABLA C. 6 CMD_INSTANT_MATCHING....148
TABLA C. 7 CMD_GET_TEMPLATE....148
TABLA C. 8 CMD_CANCEL....149
TABLA C. 9 CMD_INSTANT_VERIFY....149
TABLA C. 10 CMD_INSTANT_IDENTIFY....150
TABLA C. 11 CMD_DELETE_FP....151
TABLA C. 12 CMD_DELETE_ALL_FP....152
TABLA C. 13 CMD_SET_MASTER....152
TABLA C. 14 CMD_LEAVE_MASTER_MODE....153
TABLA C. 15 CMD_SET_MASTER_PASSWORD....153
TABLA C. 16 CMD_READ_USER_DATA....154
TABLA C. 17 CMD_WRITE_USER_DATA....154
TABLA C. 18 CMD_ERASE_DATA_BLOCK....155
TABLA C. 19 CMD_DELETE_MASTER_PASSWORD....155
TABLA C. 20 CMD_ENTER_MASTER_MODE2....156
TABLA C. 21 CMD_GET_FP_LIST2....157
TABLA C. 22 CMD_GET_MASTER_LIST2....157
TABLA C. 23 CMD_READ_LOG_DATA2....158
TABLA C. 24 CMD_REGISTER_FP....159
TABLA C. 25 CMD_CHANGE_FP....160
TABLA C. 26 CMD_ADD_FP....162
TABLA C. 27 CMD_DELETE_ALL_LOG....162
TABLA C. 28 CMD_GET_FP....163
TABLA C. 29 CMD_SET_SYSINFO....164
TABLA C. 30 CMD_GET_SYSINFO....164
TABLA C. 31 CMD_SAVE_SYSINFO....165
TABLA C. 32 CMD_CHG_NUM_OF_TEMP....165
TABLA C. 33 CMD_DEFAULT_SYSINFO....165
TABLA C. 34 CMD_STATUS_CHECK....166
TABLA C. 35 CMD_GET_FP_IMAGE2....166
TABLA C. 36 CMD_UPGRADE_FIRMWARE2....167
TABLA C. 37 CMD_SET_TIME....167
TABLA C. 38 CMD_GET_TIME....168
TABLA C. 39 CMD_CTL_IO....168
TABLA C. 40 CMD_GET_IMAGE_QUALITY....169

DEDICATORIA

Este logro se lo dedico a DIOS por darme la oportunidad de vivir y haber llegado hasta donde estoy, por darme fuerza en momentos de decepción y por darme motivos para sonreír. Se lo dedico a mi padre, José, por ser ejemplo de perseverancia, honestidad y sacrificio, además por haber sido el pedestal más sólido sobre el cual me he apoyado todo el tiempo en que he perseguido este sueño de ser un profesional competente; a mi madre, Carmen, por apoyarme todo el tiempo y por enseñarme a cultivar las virtudes necesarias para enfrentarme al desafío que representa ser una persona de bien, dispuesta a colaborar con la comunidad; a mis hermanos y hermanas que siempre han estado dándome palabras de aliento y de cierta forma ayudándome a mirar claros mis objetivos. De manera particular, dedico este logro a mi novia y a mi gran amiga Paola Proaño, por quienes he aprendido a cultivar muchos valores y por quien he aprendido lo que significa en realidad luchar por lo que uno quiere.

A todas estas personas les dedico cada uno de mis logros, diciéndoles simplemente que las amo y que todo lo hecho ha sido por y gracias a Uds.

ATENTAMENTE

LUIS CHICAIZA

RESUMEN

El Proyecto "**Diseño y construcción de un circuito electrónico comandado por huella digital para la puesta en marcha de un vehículo Jeep Grand Cherokee 5.2 Lt.**" está orientado al estudio y desarrollo de un dispositivo que permitirá crear productos comercialmente rentables, utilizando la tecnología biométrica de huella dactilar.

En este Proyecto se analizará y crearán las bases para el desarrollo de un dispositivo biométrico, utilizando la huella dactilar. Basado en un kit de desarrollo, el dispositivo requiere de la implementación de diversos componentes que permitirán crear un equipo autónomo para la identificación de personas.

Para la conformación de este proyecto se analizará la implementación de un microcontrolador, que permitirá controlar todos los dispositivos asociados al producto final. Cabe destacar que en este Proyecto se crearán las bases del desarrollo de los distintos productos posibles, es decir, se desarrollará el dispositivo autónomo de identificación para que luego se puedan implementar un sistema de control de acceso que pueda ser implementado en una diversidad de marcas de vehículos.

En cuanto a su desarrollo, el proyecto comenzará analizando, paso a paso, los distintos procesos de su evolución. Comenzando con el planteamiento del problema, los objetivos que se quieren alcanzar y el desarrollo de la solución.

Desde el tercer capítulo, se presentará el kit de desarrollo, sobre el cual se trabajará. Se describirán sus ventajas, funcionalidades y la manera en que se deberá desarrollar el dispositivo biométrico.

Asociado al kit de desarrollo, se integrarán diversos elementos que permitirán crear el equipo de identificación, como son el desarrollo de un microcontrolador y los dispositivos electrónicos relacionados a este desarrollo.

Finalmente, una vez desarrollado el equipo, se analizará el producto como

concepto comercial. Desarrollar la presentación propia del producto, su funcionamiento con sus ventajas y características, su valor distintivo frente a otros equipos de la competencia. El análisis de mercado del producto, permitirá posicionarlo en el nicho de negocios esperado, considerando la competencia y estrategia de venta, tomando en cuenta su análisis de costos y proyección de producción.

ABSTRACT

The Project "**Diseño y construcción de un circuito electrónico comandado por huella digital para la puesta en marcha de un vehículo Jeep Grand Cherokee 5.2 Lt.**" is oriented to study and development of a device that will allow creating commercially profitable products and using the biometric technology of fingerprint.

On this Project it will be analyze and will create the bases for the development of a biometric device, using the fingerprint. Based on development kit, this device requires the implementation of different components that will allow creating stand-alone equipment for the identification of people.

For the conformation of this project will be analyzed the implementation of a microcontroller, that it will allow controlling all the associated devices to the final product. It is necessary to emphasize that in this Project they will be created the bases of the development of the different possible products, that is, the stand alone device of identification will be developed to create system of access control that can be implemented in a diversity of marks of vehicles.

For the development, the project will begin analyzing, step by step, the different processes from its evolution. In order to begin, it is presented the problem, the objectives that are wanted to reach and the development of the solution.

From the second chapter, it is presented the kit of development, on which it will work on this project. Their advantages, functionalities will be described and the way in which the biometric device will be developed. Associated to kit of development, diverse components will be integrated that will allow to create the identification system, like they are the related development of a microcontroller and the electronics components to this development.

Finally, once created the equipment, the product like commercial concept will be analyzed. Its presentation will be developed, its operation with its advantages and characteristics, the difference that exists with the equipment of the market. The product market analysis, will position it in the niche of businesses hoped, taking into

account the competence and strategy of sale, their costs analysis and production projection.

CAPITULO I

INTRODUCCIÓN

1.1 ANTECEDENTES GENERALES

La llegada de nuevas tecnologías para su uso masivo y de altas prestaciones, se preocuparán de aumentar la productividad y del manejo de mejor calidad de información. De la utilización de estas tecnologías y la propia adaptación a las distintas realidades tecnológicas y de mercado de cada país, dependerá su éxito, desarrollo y evolución, ya sea en cada uno de los sectores productivos a la cual representa, como es el caso de la domòtica, el sector industrial, electrónica automotriz y de telecomunicaciones entre otras. Para el caso de la biometría, el ámbito de aceptación, desarrollo y potencial tecnológico es el mismo, donde cada región o país tiene sus propias barreras e incentivos que determinarán el propio desarrollo y adaptación de esta tecnología.

Años atrás si hubiéramos pensado en tener un scanner de huella digital en el auto para ponerlo en marcha habría sonado como un accesorio en el auto del Agente 007. Hoy es un poco diferente, con el desarrollo de los chips y de los lectores biométricos, no es de locos pensar en colocarle este tipo de scanner al auto.

En nuestro país, la biometría, no ha sido ajena al desarrollo tecnológico en las distintas áreas donde se ha podido aplicar. Con una irrupción lenta, en la que se debió educar a la gente en cuanto a su definición y aplicaciones que podría abordar, pasando por el proceso de adaptación y de alguna manera reconociendo sus ventajas.

Como aplicación emblemática de la tecnología biométrica en Ecuador, se puede señalar que se ha creado una base de datos de usuarios en casi la totalidad de la Banca Privada, para lograr una identificación única e intransferible.

Otras soluciones radican principalmente e

n el control de personal de una empresa, que puede ser, tanto para acceder a recintos restringidos o como también, en el control de asistencia del personal. Cada una de estas soluciones representa al desarrollo tecnológico que es aceptado como una herramienta de productividad y, por lo tanto, se estaría dispuesto a invertir en ella. Es por esto, que la reducción de costos de desarrollo y fabricación de este tipo de productos, irá en directo beneficio a la masificación de los sistemas biométricos.

En este Proyecto se analizarán y describirán la secuencia de pasos que son necesarios para el desarrollo e implementación de un equipo autónomo de identificación de personas, utilizando la huella dactilar, en un vehículo de uso particular. Este dispositivo está orientado a ser un equipo base para generar una variedad de soluciones, las cuales se centrarán, principalmente, en generar productos para el control de asistencia, “control de acceso” y un dispositivo que se utilice para la implementación en diversos sistemas que requieran de un equipo que brinde seguridad en la identificación de personas. Todo esto aplicado al área de la industria automotriz, siendo para nuestro caso particular, el diseñar un elemento de control de acceso a través del cual se permitirá la puesta en marcha de un vehículo tras la verificación de usuarios.

Entre los temas a tratar, se considera el desarrollo e implementación de un microcontrolador que permitirá controlar los diversos dispositivos asociados al equipo, este desarrollo cuenta con toda la evolución que se realizó, tanto en su conectividad, como en su programa de control. Bajo esta arquitectura se detallarán todos los dispositivos utilizados para su integración. Además, se analizará el funcionamiento y estructura del kit de desarrollo biométrico que se utilizará en este proyecto, debido a la importancia de su funcionamiento es necesario explicar toda su estructura y forma de operar, de manera de establecer claramente los detalles de este desarrollo.

1.2 PRESENTACIÓN DEL PROBLEMA

Debido al poco desarrollo del mercado nacional respecto a soluciones biométricas, existe una visión de cierto distanciamiento en cuanto a integrar sistemas de seguridad en las distintas empresas e instituciones que podrían requerirlo.

Particularmente en la industria automotriz, la utilización de lectores biométricos se da únicamente en vehículos de muy alta gama, constituyendo un elemento más de seguridad a fin de reducir el índice de robos de vehículos. En cuanto a los vehículos de producción en serie, es decir, modelos de gran flujo comercial, la gran mayoría está conforme con sus sistemas actuales de identificación, como son las alarmas de control remoto sobre el cual en algunos casos requiere del ingreso de un código PIN (número identificador personal, en sus siglas en inglés), para la autorización de apertura del vehículo y el uso de un Switch + llave para el arranque del mismo. Sin embargo estos sencillos sistemas no son suficientes para los delincuentes, que en muchos casos clonan estos controles remotos.

Debido al creciente aumento en el índice de robos de vehículos, las casas comerciales han implementado sistemas inmovilizadores, los cuales trabajan por emisión de ondas de radio-frecuencia, emitiendo un código único desde un transponder en la llave de ignición para el reconocimiento del usuario, por tanto fácilmente puede ser transferible la identificación de cada persona (usuario), conformándose el usuario, sólo con el manejo de la información que genera cada elemento de control, para la seguridad de su vehículo, a pesar de la gran vulnerabilidad de estos sistemas.

Además de esto, muchas empresas públicas (municipios, departamentos gubernamentales y dependencias militares) y privadas (instituciones bancarias, compañías de transporte, entre otras) han requerido de un registro de horarios de uso de sus vehículos, el cual hasta hoy se ha realizado llenando hojas de control, siendo este sistema de control también fácilmente alterable.

De acuerdo a lo anterior, la introducción de la tecnología biométrica ha sido más lenta de lo que se esperaba, a pesar de la ventaja que es la identificación real de cada usuario, permitiendo que no pueda ser transferible el elemento de control. Teniendo en cuenta que los sistemas biométricos utilizan un elemento físico propio de cada persona como es la voz, el iris ocular, el reconocimiento de rostro, la geometría de la mano, la huella dactilar, entre los más conocidos, tienen asociado un alto grado de desarrollo tecnológico que se traduce en un mayor costo de fabricación y precio de venta final, lo que hacen más difícil su masificación.

Entonces, con la finalidad de educar y acercar este tipo de tecnologías a los usuarios, es necesario masificar las soluciones biométricas creando productos al alcance del mayor mercado potencial posible, por lo que se debe reducir costos de desarrollo, precios de venta y aumentar la potencialidad de estos sistemas de seguridad.

1.3 PRESENTACIÓN DE LA SOLUCIÓN

En base a la situación del mercado, se ha planteado la creación de un nuevo producto que será desarrollado y gestado en las propias dependencias de la empresa.

Con la generación de este dispositivo con tecnología biométrica para el control de personas en un formato que permitirá desarrollar y cumplir diversos objetivos, como es la creación de una cartera de productos y soluciones específicas enfocadas a las necesidades de cada cliente. Con la identificación biométrica de personas, se pretende abordar casos de control de accesos, control de asistencia del personal o funcionarios de una empresa y autenticar o identificar localmente la identidad de una persona de manera de ser integrado en sistemas específicos.

El potencial del proyecto se enfocará en los bajos costos de desarrollo, fabricación e integración del dispositivo, lo que generará ventajas competitivas para su introducción al mercado, además de contar con un diseño compacto que permita generar la versatilidad del producto.

Junto con su desarrollo será necesario crear una estrategia de negocios que permita determinar la inserción del producto en los segmentos esperados, determinando las herramientas de mercadeo y generación de negocios.

La resolución de los puntos críticos del desarrollo del nuevo dispositivo, permitirá crear bases sólidas para la sustentación del proyecto a mediano y largo plazo, generando proyecciones de nuevos negocios y marcando presencia en el mercado de soluciones con tecnología biométrica.

Este proyecto estará basado en un Kit de desarrollo de un capturador de huella

dactilar, este kit maneja un scanner de huella digital y una CPU integrada para realizar el proceso de indexación de la minucia generada en la lectura de la huella. A este kit se debe integrar toda la interfaz con el usuario como teclado y visor.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar, construir e implementar un circuito electrónico comandado por huella digital para la puesta en marcha de un vehículo Jeep Grand Cherokee 5.2 Lt.

1.4.2 OBJETIVOS ESPECÍFICOS

- Crear un dispositivo de captura e identificación de huella dactilar que permita obtener un producto comercialmente rentable, destinado a satisfacer principalmente los requerimientos de control de acceso y asistencia.
- Fabricación de un dispositivo de bajo costo.
- Crear un dispositivo capaz de identificar o autenticar de forma autónoma y compacta sin requerir de dispositivos o sistemas computacionales externos.
- Diseñar un producto que genere soluciones flexibles, a la medida de los clientes.
- Crear una cartera de soluciones estándares, sobre las cuales se realizarán las distintas adaptaciones requeridas, para generar soluciones integrales.
- Contribuir con la reducción del índice de robo de vehículos en nuestro país.
- Elaborar un manual que facilite el manejo y operación del prototipo.

1.5 DESCRIPCIÓN

En términos generales, el producto consiste en un dispositivo autónomo con tecnología biométrica que permita desarrollar soluciones a la medida de cada cliente, sin incurrir en grandes gastos de inversión. Como las características principales de este dispositivo son de obtener un bajo costo de fabricación y de un diseño compacto, para ello se utilizará un equipo de desarrollo con tecnología biométrica.

Este dispositivo consiste en un lector biométrico el cual tiene la capacidad de almacenar y procesar en forma autónoma las huellas dactilares de los usuarios,

previamente enrolados, debido a la incorporación de una unidad de procesos dedicada a este tipo de aplicaciones.

Este desarrollo considera la integración de una interfaz con el usuario como es la de un **display** de visualización y teclado.

La versatilidad se reflejará en las adaptaciones propias que cada cliente necesite, ya sea en el ámbito de la seguridad, como en la adaptabilidad de sus sistemas.

El dispositivo está centrado a desarrollar soluciones para:

- Control de acceso.
- Control de asistencia.
- Soluciones que requieran de un módulo pequeño y altas prestaciones de control biométrico (autenticación e identificación) y su adaptabilidad a sistemas.

1.6 FUNCIONALIDADES BÁSICAS

Este producto pretende desarrollar una diversidad de soluciones que permitan un control y, principalmente, una autenticación biométrica de personas de forma autónoma. De tal forma que pueda manipularse las funciones eléctricas esenciales del vehículo de forma privada y sin la necesidad de usar llaves o switch’s de contacto, sino únicamente tras la autentificación de la huella dactilar del usuario.

Para el modo de Servicio, el dispositivo brindara la opción de puesta en marcha del vehículo a través del reconocimiento de una contraseña.

En su configuración estándar contendrá un dispositivo biométrico de lectura de huella dactilar para la autenticación y control, además de un visor que permitirá desplegar una interfaz de información que puede ser personalizada dependiendo de las necesidades del cliente, además dispondrá de un teclado numérico, ya sea para navegación o para la introducción de **password** o claves personales.

CAPITULO II.

SISTEMAS DE CONTROL DE ACCESO

Este capítulo presenta una breve descripción de algunas de las tecnologías de control de acceso utilizadas actualmente. Entre ellas se describe a los sistemas basados en tarjetas inteligentes, sistemas biométricos y sistemas de control por radio-frecuencia, a fin de proveer un contexto global dentro del cual se pueda evaluar la contribución del presente trabajo.

2.1 SISTEMAS BASADOS EN TARJETAS INTELIGENTES

2.1.1 DEFINICIÓN DE TARJETAS INTELIGENTES

En la vida diaria es muy común el uso de tarjetas que sirven para identificar a una persona, acceder a edificios, áreas restringidas, realizar transacciones bancarias, etc. Estas tarjetas han ido evolucionando de una manera rápida hasta el punto de añadir un chip con un microprocesador interno que permita almacenar una mayor cantidad de información, pero el objetivo de esto no sólo es almacenar una mayor cantidad de información de manera segura sino también el poder tener la posibilidad de almacenar dicha información en otros sistemas, a este conjunto de características se las denomina un sistema basado en tarjetas inteligentes.

Las tarjetas inteligentes nacieron en la década de los 70, básicamente una tarjeta inteligente es un chip con un microprocesador el cual está encapsulado en una tarjeta PVC con determinadas dimensiones, dicho chip dispone de contactos exteriores o campos electromagnéticos que permiten tener una comunicación con él para poder almacenar y procesar información de una manera segura, ésta puede ser información personal, bancaria, historiales clínicos, claves privadas de acceso, etc.

La seguridad en este tipo de tarjetas es mayor ya que el chip contiene una tecnología interna sofisticada que hace que las posibilidades de manipulación física se reduzcan, esta tecnología además permite soportar procesos criptográficos

complejos que permiten tener un sistema de seguridad mucho más sólido.

2.1.2 ARQUITECTURA

El chip de una tarjeta inteligente generalmente consta de un CPU o microprocesador, memoria, control de encendido y circuitos especiales para la seguridad y comunicación con el mundo exterior. Como se puede observar en la figura 1 el acceso a las áreas de memoria sólo es posible a través de la unidad de entrada/salida y de la CPU lo que permite aumentar la seguridad del sistema.

Algunas tarjetas también cuentan con un generador de números aleatorios, que se usa cuando se requiere una autenticación two-ways que consiste en que ambas partes envíen un número aleatorio, para que se realice un tipo de procesamiento y este resultado sea devuelto a su emisor, y así poder comprobar la autenticidad de la identidad de su interlocutor.

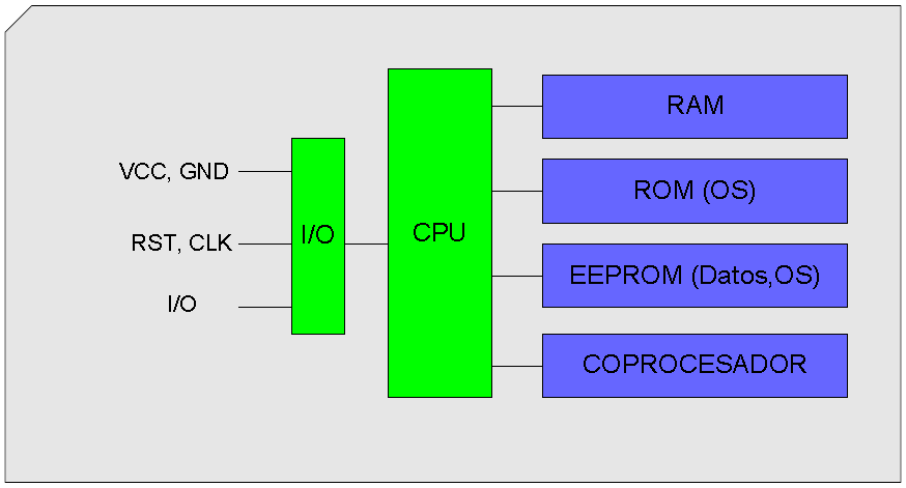


FIGURA 2. 1 Estructura de una tarjeta Inteligente.

- RAM (Random Access Memory).-

Esta es la memoria de trabajo del microprocesador aquí se almacena los datos de sesión, al ser volátil ésta pierde toda su información al momento de ser desconectada de su alimentación de energía.

- La ROM: (Read Only Memory).-

Aquí es donde se encuentra el sistema operativo (OS) el cual se encarga de manejar la asignación de almacenamiento de la memoria, la protección de accesos y las comunicaciones descartando así la posibilidad de poder introducir externamente comandos falsos que puedan comprometer la seguridad del sistema.

- EEPROM: (Electrical Erasable Programmable Read Only Memory).-

Memoria no volátil que contiene todos los datos que deben permanecer en la tarjeta a lo largo de múltiples sesiones, así como también el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre del usuario, número de identificación personal o PIN (Personal Identification Number)

- COPROCESADOR:

Este elemento se utiliza básicamente para propósitos de criptografía.

- CPU:

Controla el funcionamiento del resto de componentes y además realiza operaciones de cálculo.

- I/O:

El puerto de entrada/salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit.

2.1.3 FUNCIONAMIENTO

Las tarjetas se activan al introducirlas en un lector de tarjetas que son el dispositivo que actúa como la interface entre el usuario y el sistema, existe una gran diversidad de lectores y sus capacidades varían de acuerdo a las necesidades de los usuarios. Los lectores pueden ser alámbricos, inalámbricos, con teclado, sin teclado, con pantalla o sin ella. Un contacto metálico, un campo magnético o incluso una lectura láser, permite la transferencia de información entre el lector y la tarjeta.

“Las comunicaciones de las tarjetas inteligentes se rigen por el estándar ISO

7816/3, en donde se define las señales eléctricas, los protocolos de transmisión, niveles de tensión y los procedimientos para iniciar la comunicación".[1]

2.1.4 CLASES DE TARJETAS INTELIGENTES

Las tarjetas inteligentes se clasifican en dos grandes grupos que son:

De contacto.

Sin contacto.

2.1.4.1 Tarjetas inteligentes de contacto

Este tipo de tarjetas tienen la estructura mencionada en el apartado 2.1.2 y necesitan ser insertadas físicamente en una terminal con lector inteligente para que por medio de contactos pueda ser leída. El chip de este tipo de tarjetas tiene 8 contactos (Figura 1.2) de los cuales se utilizan sólo 6 los mismos que son el único interfaz electrónico existente entre la tarjeta y el terminal lector. Todas las señales eléctricas circulan a través de estos contactos.

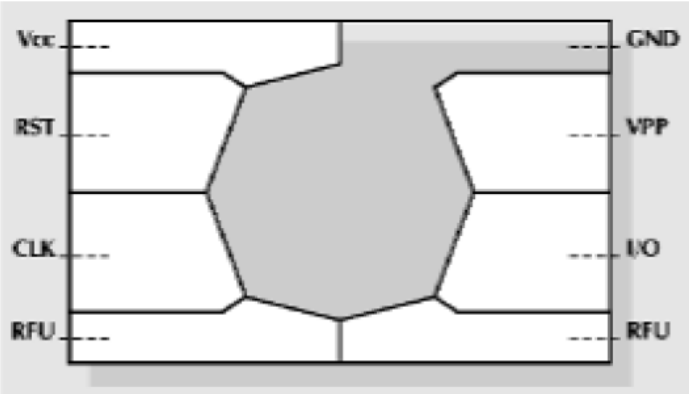


FIGURA 2. 2 Contactos de una tarjeta inteligente.[2]

- VCC.- Fuente de alimentación del chip.
- RST.- Reset del chip
- CLK. - Reloj.

---

[1] .http://www.latinoseguridad.com/LatinoSeguridad/Reps/TI.shtml

[2] Sandoval Juan D., Brito Ricardo, Mayor Juan C., 1999. "Tarjetas Inteligentes". España: Thomson Publishing Company

- RFU.- Contacto reservado para usos futuros.
- I/O.- Punto de entrada y salida de la información.
- VPP.- Voltaje externo que permite programar la memoria de la tarjeta.
- GND.- Tierra.

2.1.4.2 Tarjetas inteligentes sin contacto

Tienen una estructura y funcionalidad similar a las tarjetas inteligentes de contacto con la diferencia que éstas ya no utilizan contacto físico sino una interface inductiva (Figura Nº 3) es decir la comunicación se la realiza por medio de antenas por donde se transfiere toda la información entre el lector y la tarjeta, el tipo de interface utilizado implica que se utilicen otros protocolos de comunicación los mismos que se encuentran especificados en el estándar ISO 14443.

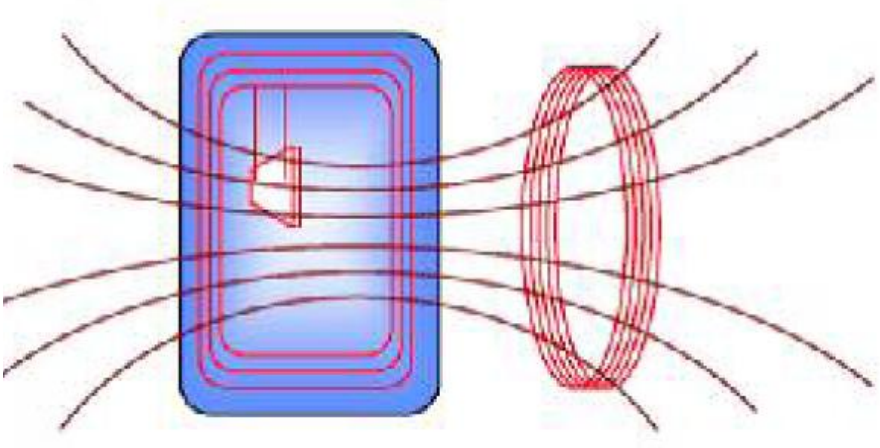


FIGURA 2. 3 Tarjeta inteligente sin contacto.[3]

Este tipo de tarjetas permiten tener una lectura mucho más rápida que una tarjeta de contacto ya que no es necesario hacer una inserción en el lector y además se evitan los problemas de fallos en la lectura por el deterioro en la superficie de los contactos o por residuos que impiden realizar una lectura correcta.

Estas tarjetas reciben su alimentación de energía ya sea por medio de una batería insertada junto al chip o por medio de un hilo metálico sobre el cual se induce una corriente eléctrica que es capaz de alimentar al resto de elementos del circuito.

[3] http://www.idensis.com/tecnologias_elementos.html

2.1.5 TIPOS DE LECTORES

El lector es un dispositivo que permite tener acceso a la información contenida en las tarjetas inteligentes, normalmente son dispositivos adaptadores que se incorporan al sistema de comunicaciones del ordenador generalmente por un puerto específico, se los puede dividir de la siguiente manera.

- *Lectores conectados a un ordenador*: Estos lectores son fabricados para ser usados conectándolos a un ordenador, esta conexión puede ser a través de un puerto serial, USB, PCMCIA, etc.
- *Lectores conectados a un equipo específico*: Son lectores que se pueden instalar en un aparato determinado para cumplir con una cierta función. Estos lectores se pueden instalar en cajeros automáticos, máquinas expendedoras, peajes, accesos a escenarios masivos, etc.
- *Lectores Portátiles*: Son equipos que no necesitan de otro aparato para cumplir su función. Estos lectores poseen los recursos integrados como baterías, memoria, etc.

2.1.6 VENTAJAS Y DESVENTAJAS

Entre las principales ventajas tenemos:

- Capacidad de almacenamiento y procesamiento seguro que otorga el microprocesador.
- Está sujeta a estándares internacionales lo que garantiza su uso universal.
- Tiempo de vida largo
- Los sistemas operativos de estas tarjetas soportan múltiples aplicaciones y políticas de seguridad independientes para almacenamiento de datos en una misma tarjeta.

Como desventajas tenemos las siguientes:

- El costo unitario y de gestión alto.
- La ausencia de infraestructura implica que se tenga que instalar lectores en los ordenadores implicados y en otros dispositivos que sean necesarios.
- Compatibilidad de los dispositivos y el software a pesar de la existencia de los

estándares.

- Ambigüedades legales relacionadas con la privacidad y confidencialidad del usuario.

2.1.7 SEGURIDAD EN TARJETAS INTELIGENTES

Se deben tener algunos criterios en la protección de la información expuesta en la seguridad de información, las tarjetas inteligentes las afrontan de la siguiente manera:

Confidencialidad. No se debe aplicar sólo a los datos almacenados en la tarjeta sino también a los datos almacenados en otros sistemas que pueden ser accedidos usando la tarjeta. Los controles de acceso y cifrado son las herramientas más usadas para proteger la confidencialidad y la privacidad.

Integridad. Los datos almacenados en la tarjeta o en otro sistema deberían estar protegidos contra alteraciones. Para ello las tareas de memoria pueden ser protegidas contra accesos no autorizados, o con memoria WORM (write once, read many times), que sólo puede ser escrita una vez.

No repudio. Ni el dueño de la tarjeta ni la entidad puedan repudiar la transacción o reclamar que nunca tuvo lugar.

"Los requerimientos del almacenamiento dependerían de si los datos deben ser portables o accedidos sin conexión, por lo que podrían ser almacenados en una tarjeta; o si no sería preferible almacenar los datos en el computador y usar la tarjeta para permitir el acceso a los datos".[4]

Según el nivel de confidencialidad requerido se tiene lo siguiente:

- Almacenar los datos en claro en una tarjeta con memoria o en un fichero del ordenador.
- Almacenar los datos en una tarjeta con memoria protegida o en un ordenador con control de acceso controlado por una contraseña o un sistema de tarjeta.

---

[4] http://www.tec-mex.com.mx/promos/bit/bit0703-msr.htm

- Cifrar los datos o almacenarlos en una tarjeta con memoria y circuitos de protección

Los datos se hacen confusos a personas no autorizadas a través de cifrado con clave secreta. También se debe comprobar que los datos almacenados no son alterados, y que no se pueden perder como resultado de un mal funcionamiento o fallo eléctrico.

Cuando los datos son transmitidos desde un sistema a otro, se debe asegurar que la información no es alterada, accidental o deliberadamente, en el camino. Si es confidencial, entonces se debe proteger el interfaz físicamente o con cifrado. Para comprobar la integridad de los mensajes se usan códigos de redundancia cíclica (CRCs, Cyclic Redundancy Checks), contadores de transacción y códigos de autenticación de mensajes (MACs, Message Authentication Code).

2.2 RFID (IDENTIFICACIÓN POR RADIO FRECUENCIA)

RFID es un sistema remoto de almacenamiento y recuperación de datos que usa dispositivos denominados etiquetas o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto mediante ondas de radio. [5]

Se ha sugerido que el primer dispositivo conocido similar a RFID pudo haber sido una herramienta de espionaje inventada por León Theremin para el gobierno soviético en 1945 y; según algunas fuentes, la tecnología usada en RFID habría existido desde 1920, desarrollada por el MIT [6]y usada extensivamente por los británicos en la Segunda Guerra Mundial.

2.2.1 COMPONENTES DE UN SISTEMA RFID

a) El tag o transponder de RFID consiste en un pequeño circuito, integrado con una pequeña antena, capaz de transmitir un número de serie único hacia un dispositivo de lectura.

[5] Weinstein, R., RFID: a technical overview and its application to the enterprise: 27- 33.
[6] MIT: Massachusetts Institute of Technology

b) El lector, (el cual puede ser de lectura o lectura/escritura) está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control.
c) Un controlador o un equipo anfitrión, comúnmente una PC o Workstation, en la cual corre una base de datos y algún software de control.

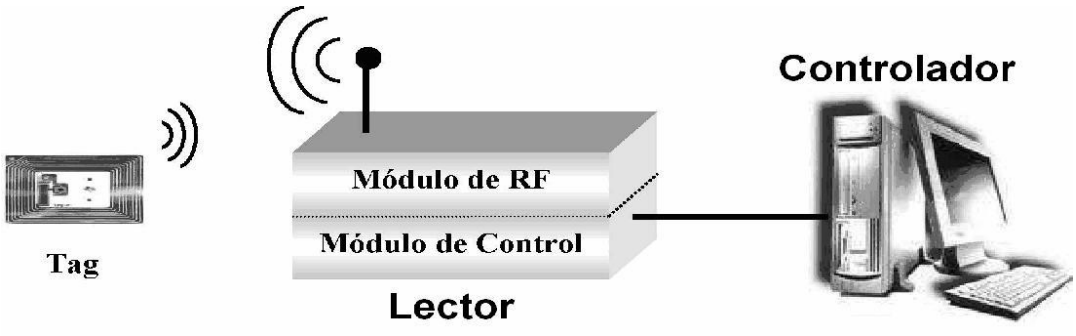


FIGURA 2. 4 Componentes de un sistema RFID; Funcionamiento de un *sistema RFID*

2.2.2 FUNCIONAMIENTO

El transponder y el módulo RFID (transpondedor + lector) trabajan juntos para proporcionar al usuario una solución que no requiere de contacto o línea visual para identificar personas, animales u objetos. [7]

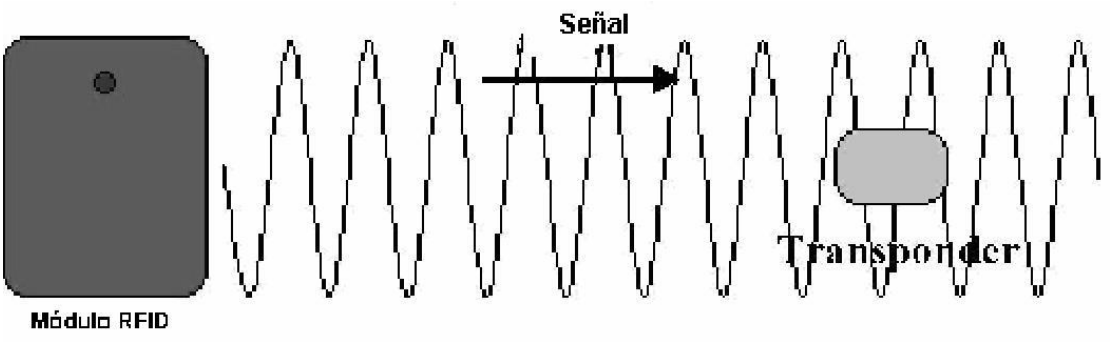


FIGURA 2. 5 Emisión de la señal de baja potencia del lector y entrada del transponder en el campo electromagnético

[7] http://www.kifer.eu/Recursos/Pdf/RFID.pdf

El módulo RFID emite una señal de radio frecuencia de baja potencia para crear un campo electromagnético. El campo electromagnético es emitido por el transceptor a través de una antena transmisora, típicamente en forma de bobina. Este campo electromagnético funciona como una señal “portadora” de potencia del lector hacia el transponder.

Un transponder contiene una antena, también en forma de bobina, y un circuito integrado. El circuito integrado requiere de una pequeña cantidad de energía eléctrica para poder funcionar.

La antena contenida en el transponder funciona como un medio para tomar la energía presente en el campo magnético producido por el módulo de RFID y la convierte en energía eléctrica para ser usada por el circuito integrado.

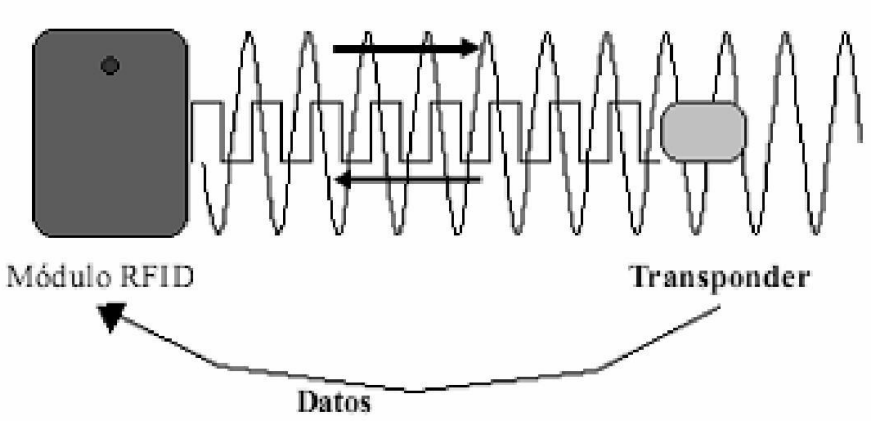


FIGURA 2. 6 Envío de datos por parte del transponder

Cuando un transponder se introduce en el campo electromagnético producido por el módulo de RFID, la energía captada permite que el circuito integrado del transponder funcione, los datos contenidos en su memoria son transmitidos.

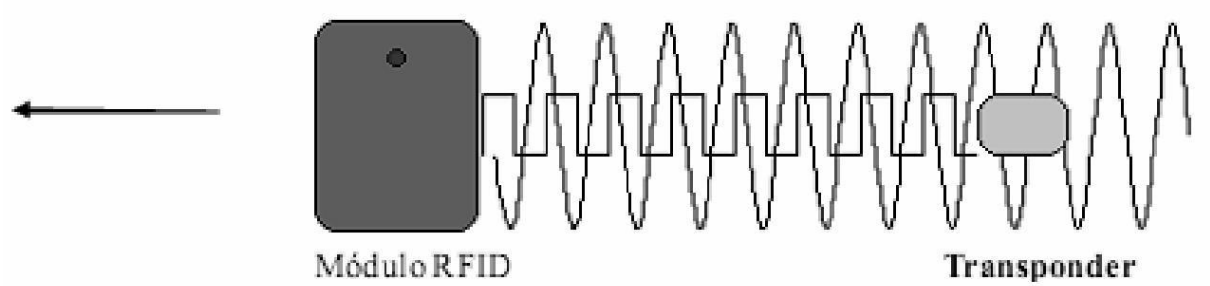


FIGURA 2. 7 Transmisión de los datos contenidos en la memoria del transponder

La señal electromagnética que proviene del transponder es recuperada por la antena receptora del módulo RFID y convertida a una señal eléctrica. El transceptor tiene un sistema de recepción que está diseñado para detectar y procesar esta "débil" señal proveniente del transponder, demodulando los datos originales almacenados en la memoria del circuito integrado contenido dentro del transponder. Una vez que los datos del transponder han sido demodulados, el módulo digital comprueba que los datos recibidos son correctos. Una vez que el lector verifica que no hay errores y valida la información recibida, los datos son decodificados y reestructurados para su transmisión como información en el formato requerido por el sistema al cual esté conectado el lector.

El rango de lectura, depende por lo general del tamaño de la antena del lector y del transponder utilizado. La etiqueta RFID, que contiene los datos de identificación del objeto al que se encuentra adherido, genera una señal de radiofrecuencia con dichos datos. Esta señal puede ser captada por un lector RFID, el cual se encarga de leer la información y pasársela, en formato digital, a la aplicación específica que utiliza RFID.

2.2.3 CONECTIVIDAD RFID[8]

Cuando se desarrolla un sistema de RFID la elección de la conectividad de red para los lectores de RFID, es una consideración importante:

[8] http://www.kimaldi.com/aplicaciones/control_de_presencia_asistencia_y_horarios/control_de_presencia_ acceso_y_recursos_con_rfid_activos

RS-232. Este protocolo provee sistemas de comunicación confiables de corto alcance. Tiene ciertas limitantes como una baja velocidad de comunicación, que va de 9600 bps a 115.2 Kbps. El largo del cable está limitado a 30 metros, no cuenta con un control de errores y su comunicación es punto a punto.

RS-485. El protocolo RS-485 es una mejora sobre RS-232, ya que permite longitudes de cables de hasta 1,200 metros. Alcanza velocidades de hasta 2.5 Mbps y es un protocolo de tipo bus lo cual permite a múltiples dispositivos estar conectados al mismo cable.

Ethernet. Se considera como una buena opción, ya que su velocidad es más que suficiente para los lectores de RFID. La confiabilidad del protocolo TCP/IP sobre Ethernet asegura la integridad de los datos enviados y finalmente al ser la infraestructura común para las redes.

Wireless 802.11: Se utiliza en la actualidad en los lectores de RFID móviles. Además de que esta solución reduce los requerimientos de cables y por lo tanto de costos.

USB: Pensando desde la tendiente desaparición del puerto serial en las computadoras, algunos proveedores de lectores RFID han habilitado sus equipos para poder comunicarse mediante el puerto USB.

Wiegand: Como todo protocolo de comunicaciones el Wiegand consta de dos partes fundamentales: Aquella que describe el modo en que físicamente se transmite la información digital y la forma de interpretar numéricamente dicha información. La transmisión de datos Wiegand usa tres hilos. La línea para enviar los unos lógicos o DATA1, la línea para los ceros lógicos o DATA0 y la línea de masa de referencia de ambos o GND. Los niveles que se usan son 0 ó Bajo, a nivel de GND, o Alto a +5V o VCC.

Con los avances tecnológicos actuales, se habla también que los datos generados por los dispositivos de RFID, puedan ser movilizados a través de la red de telefonía celular.

2.3. INMOVILIZADOR ELECTRÓNICO BASADO EN RFID

2.3.1 GENERALIDADES

Para aumentar la protección contra los intentos de robo, los automóviles están dotados de un sistema electrónico de trabado del motor, que se activa automáticamente al sacar la llave de arranque. En efecto, las llaves tienen un dispositivo que transmite una señal codificada a la central (MÓDULO INMOVILIZADOR), la cual, solamente si reconoce la señal, permite la puesta en marcha del motor.

2.3.2 COMPONENTES DEL SISTEMA:

1-Mòdulo lector o módulo inmovilizador.

2-Antena, en el tambor de contacto.

3-Unidad de control, computadora.

4-Señalizador luminoso.

5-Llave de usuario, contiene un transponder en su interior.

La llave del usuario es un elemento importante, ya que no es como las tradicionales. Además de la clave mecánica que posee y permite girar el tambor de arranque, contiene en su interior un componente que emite una señal electrónica codificada. Este componente se llama transponder. Esta señal es captada por una antena que se encuentra ubicada alrededor del tambor de arranque en forma de anillo. Esta antena envía la señal codificada emitida por la llave a un módulo antiarranque.

Este módulo puede ser exterior o estar incorporado dentro del módulo de gestión de motor o ECU. En el caso de los exteriores, si la señal enviada por la llave coincide con la que se encuentra en el módulo, envía otra señal a la ECU habilitando la puesta en marcha normal del vehículo.

Si el módulo de inyección no recibe señal o es distinta a la que se encuentra grabada en su memoria, inhibe la puesta en marcha del motor.

Generalmente un testigo luminoso en el tablero da cuenta de esta situación para poner de sobre aviso al usuario del estado del sistema.

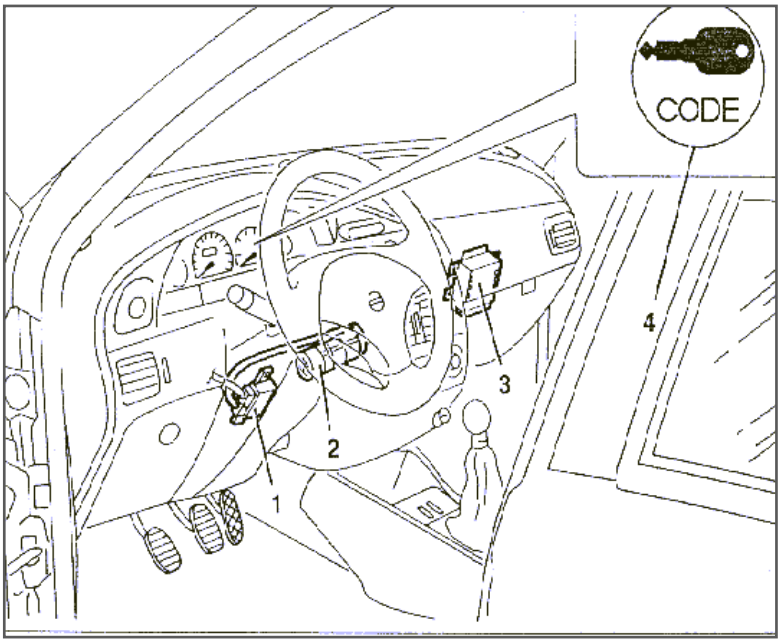


FIGURA 2. 8 Ubicación en el automóvil del sistema inmovilizador Fiat CODE [9]

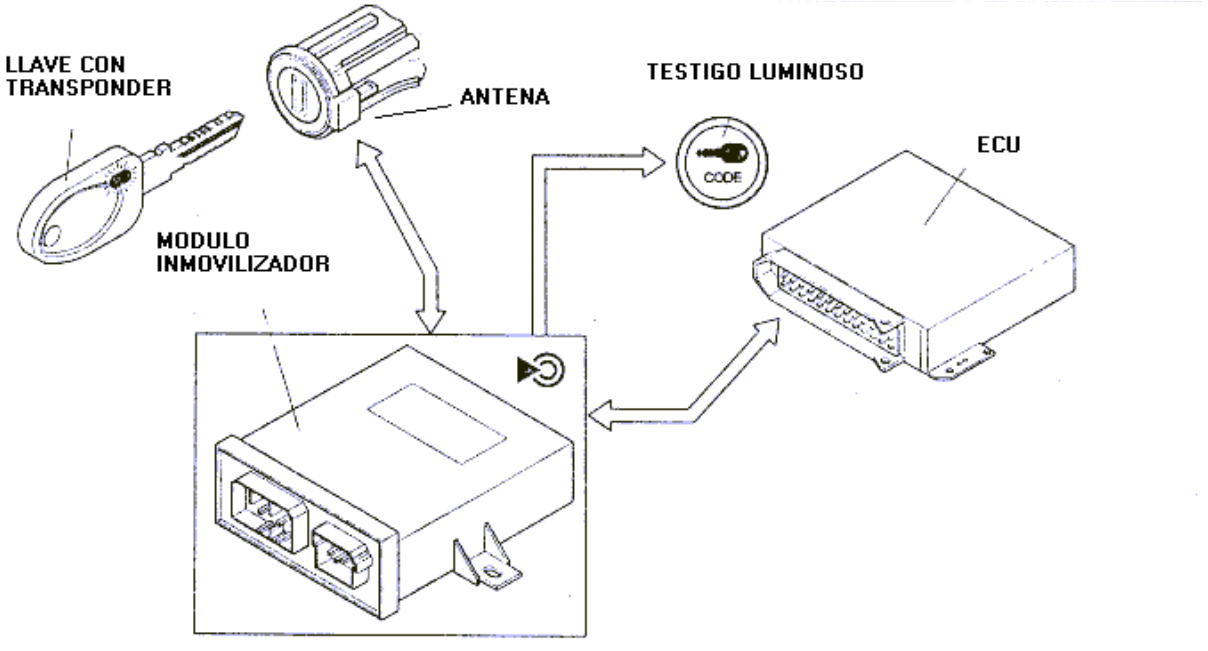


FIGURA 2. 9 Componentes del sistema inmovilizador[10]

[9] http://www.cise.com/Cursosdistancia/aula50/index2.htm
[10] http://www.cise.com/Cursosdistancia/aula50/index3.htm

2.3.3 FUNCIONAMIENTO

Al colocar la llave en el tambor el transponder es excitado por una corriente alterna que circula por la antena.

Al activarse el transponder emite una señal a modo de código que es leída por el módulo inmovilizador luego enviada a la computadora, donde ese código debe estar autorizado y ser válido.

El módulo inmovilizador esta comunicado con la ECU por una línea serie, la comunicación es bidireccional

2.3.4 TIPOS DE TRANSPONDERS

Transponder de código fijo

Cuando son excitados emiten un código fijo. Cada transponder tiene un único código en su interior. Estas llaves se pueden copiar, ya que el transponder es copiable.

Transponder de código Crypto

El transponder tiene una doble función. Por un lado existe un código de identificación y por otro lado un algoritmo de verificación. Estos transponder no son copiables.

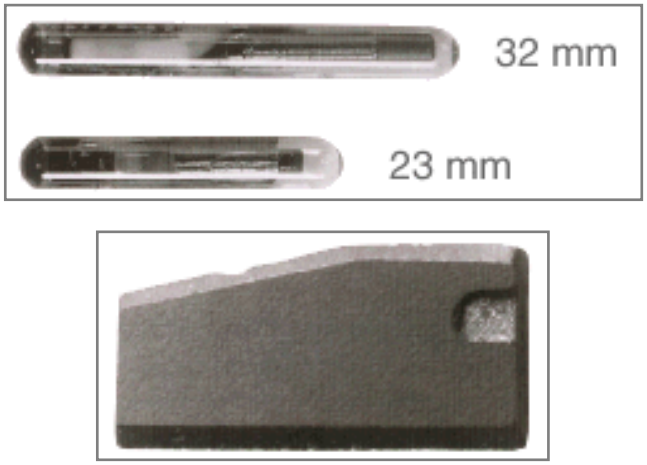


FIGURA 2. 10 Imágenes de trasponders[11]

[11] http://www.cise.com/Cursosdistancia/aula50/index4.htm

2.3.5 LAS LLAVES

Alguna persona podría realizar una copia Mecánica de la llave. Pero esta copia aunque realice perfectamente la apertura del contacto no lograra encender el motor, es mas en muchos casos el sistema INMOVILIZADOR inhibe el arranque y no solo la INYECCIÓN.

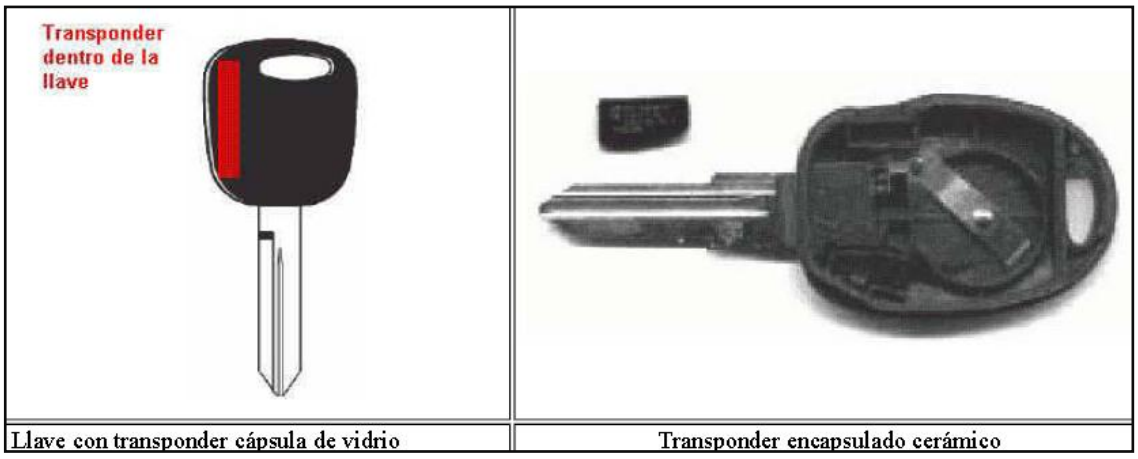


FIGURA 2. 11 Imágenes de llaves con transponder

TABLA 2. 1 ALGUNAS MARCAS DE TRANSPONDERS[12]

MAZDA	TEMIC
MITSUBISHI	TIRIS (TEXAS INSTRUMENTS)
NISSAN	PHILIPS TRANSPONDER
OPEL	PHILIPS TRANSPONDER
PEUGEOT	PHILIPS TRANSPONDER
PIAGGIO	TEMIC
PORSCHE	MEGAMOS
RENAULT	PHILIPS TRANSPONDER
SEAT	MEGAMOS
SEAT	PHILIPS TRANSPONDER

[12] http://www.cise.com/Cursosdistancia/aula50/index10.htm

2.3.6 TIPOS DE ANTENAS

La antena consta de una bobina arrollada en torno de un anillo plástico.

En los casos en que no tiene módulo lector, se le puede medir su resistencia. Según el modelo su resistencia es de menos de 100 Ohm.

La antena es energizada con una corriente alterna que excita el transponder de tal forma que se pueda emitir el código.

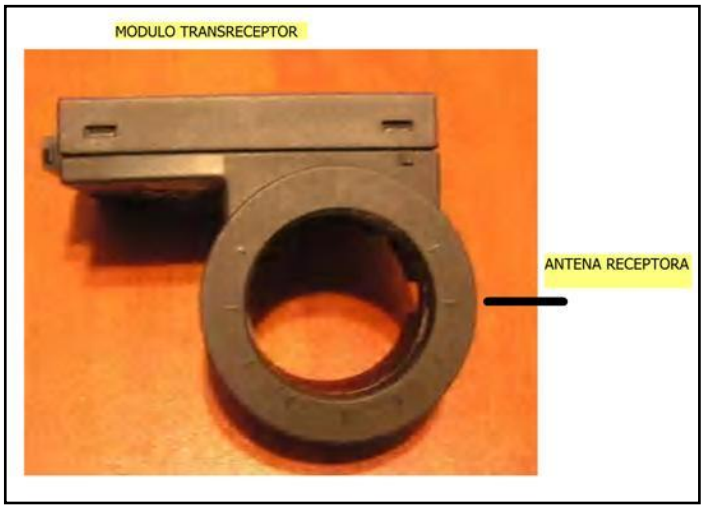


FIGURA 2. 12 Antena con módulo lector incorporado

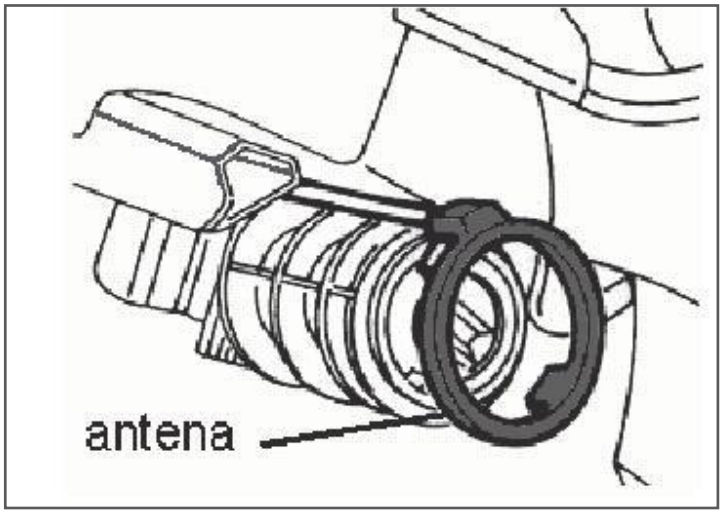


FIGURA1 2. 13 Antena sin módulo lector (solo bobina)[13]

[13] http://www.cise.com/Cursosdistancia/aula50/index9.htm

2.3.7 INMOVILIZADOR FIAT CODE I

Este sistema puede hallarse en las versiones Palio, Palio Weekend y Siena.

El sistema FIAT CODE activa el funcionamiento de la central de inyección del motor mediante un intercambio de códigos.

Cuando la llave está en MARCHA, la central de inyección/encendido del motor, pide a la central Fiat Code que le envíe el código, esta responde y solo envía un código secreto después de reconocer (mediante la antena) una llave electrónica conocida en el conmutador de arranque.

Una vez reconocido el código, la central de inyección del motor aprueba la puesta en marcha del motor. La central de inyección/encendido del motor puede memorizar el código secreto solo con un procedimiento específico.

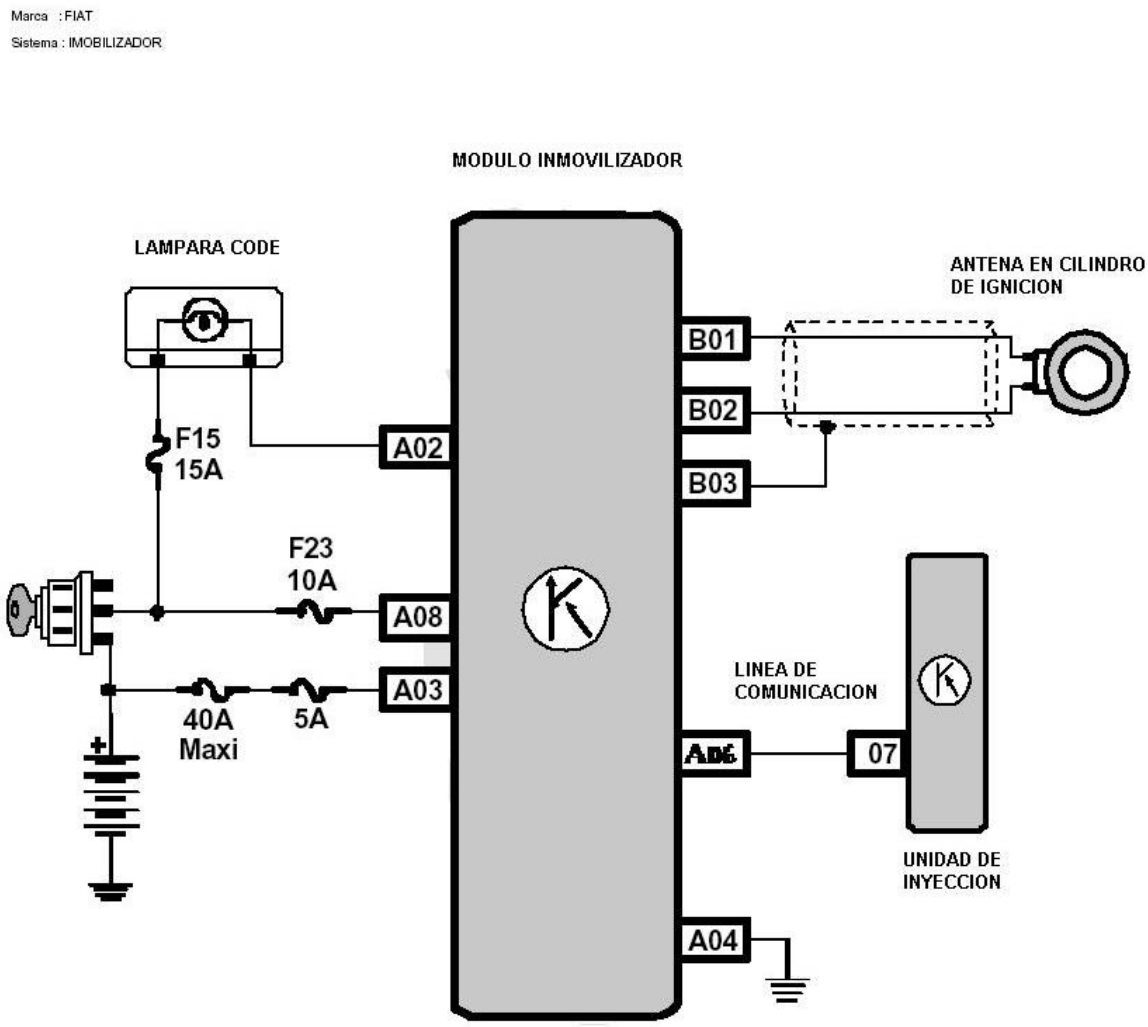


FIGURA 2. 14 DIAGRAMA ELECTRÓNICO DEL INMOVILIZADOR FIAT CODE

2.3.7.1 FUNCIONES DE LA CENTRAL DEL INMOVILIZADOR14

- Reconocer la introducción y la rotación de una llave en el conmutador de arranque.
- Emitir un campo electromagnético para dar potencia y activar el TRANSPONDER (emisor del código de la llave), y recibir el código de la llave.
- Memorizar como máximo una cantidad limitada de llaves con sus códigos secretos.

[14] http://www.cise.com/Cursosdistancia/aula50/index7.htm

- Gestionar los controles/elaboraciones de los códigos.
- Gestionar una comunicación serie bidireccional de un solo cable hacia la central de inyección (ECU).
- Gestionar un señalador luminoso de diagnosis, posicionado en el tablero de instrumentos.

2.3.8 SISTEMA DE SEGURIDAD PASIVA ANTI ROBO -PATS[15]

El sistema de seguridad Pasiva Anti Robo PATS está diseñado para generar seguridad contra el robo del automóvil sin que el cliente tenga que accionar ningún mecanismo.

Cada llave del sistema PATS (Llave del vehículo) contiene un elemento de seguridad llamado transponder, el cual es capaz de almacenar un código en su interior.

El Transponder es un elemento que se encuentra en el interior de la llave y no requiere baterías, no está relacionado para su funcionamiento con ningún tipo de alarma y es programado al momento de fabricación. Para que el transponder entregue su código es necesario alimentarlo y para esto se utiliza radio frecuencia.

El módulo PATS presenta varias ubicaciones, lo importante es que siempre debe contener el enlace con la antena colocada en el interruptor de encendido. Algunos módulos de generación siguiente cuentan con el TRANSRECEPTOR y antena incorporada en el mismo módulo.

[15] Cise Electrónica – José M. Bustillo 3243 – (1406) Capital Federal – Buenos Aires – Argentina 5411 4637-8381
Cise Electronics Corp. 12920 SW 128 th Street – Suite 4 – Miami – Florida 33186 – USA (786) 293-1094

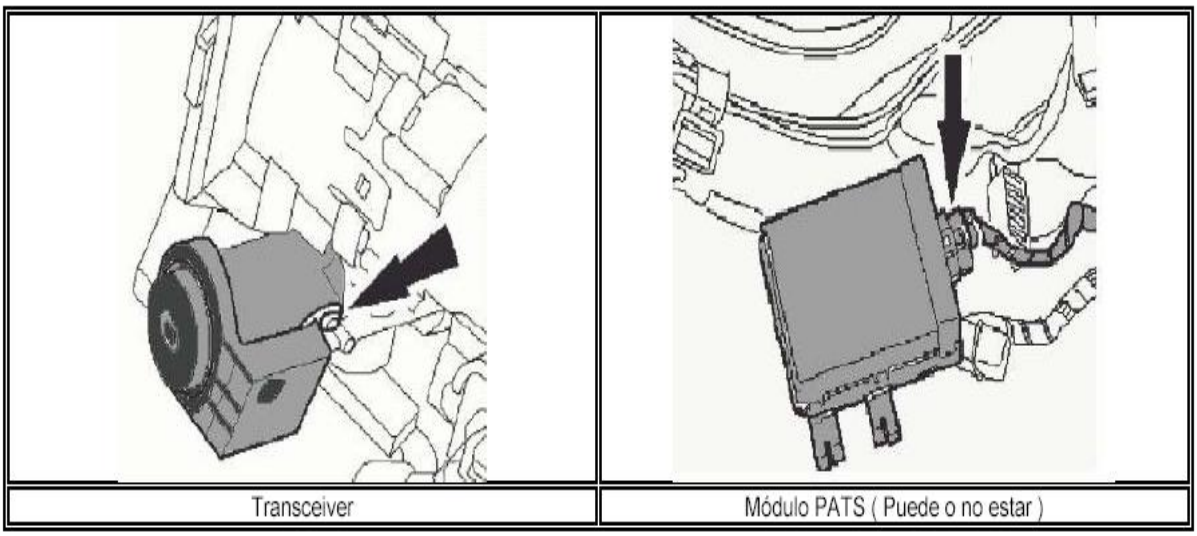


FIGURA 2. 15 UBICACIÓN DE LOS MÓDULOS DEL SISTEMA PATS

El PCM realiza el análisis de lo leído y contiene en su interior un Microprocesador y una memoria EEPROM (Borrable y programable eléctricamente).

Al tener el microprocesador los datos del código contenido en la llave procede a compararlos con alguno de los códigos que previamente fueron grabados en el proceso de programación.

Estos códigos se encuentran en la memoria no volátil del PCM y si existe correspondencia procederá a un arranque seguro, de no ser así puede tener las siguientes estrategias:

- No operar el arranque START (Relevador inhibidor del arranque).
- No accionar los inyectores después de unos segundos de encendido. (Almacena DTC P1260).
- Activar la luz de aviso Anti-robo. En el Tablero de instrumentos.

El sistema accionara la luz de advertencia de robo por aproximadamente un minuto y seguido de esto generara una serie de Códigos del tipo destello indicando el problema asociado.

Todo este proceso de identificación lo puede realizar al colocar la posición de contacto o start y se realiza de forma inmediata.

Dentro de los códigos almacenados al momento de la programación se pueden encontrar un mínimo de 2 códigos (2 llaves) y un máximo de 8 códigos (8 llaves), cada una de estas llaves al momento de la programación debe ser la correspondiente al sistema, es decir no se puede programar una llave de otra marca de vehículo aunque contenga una tecnología similar.

2.3.8.1 Pasos realizados por el pcm.

La siguiente es la secuencia realizada por el PCM para identificar si el código contenido en la llave es el correcto.

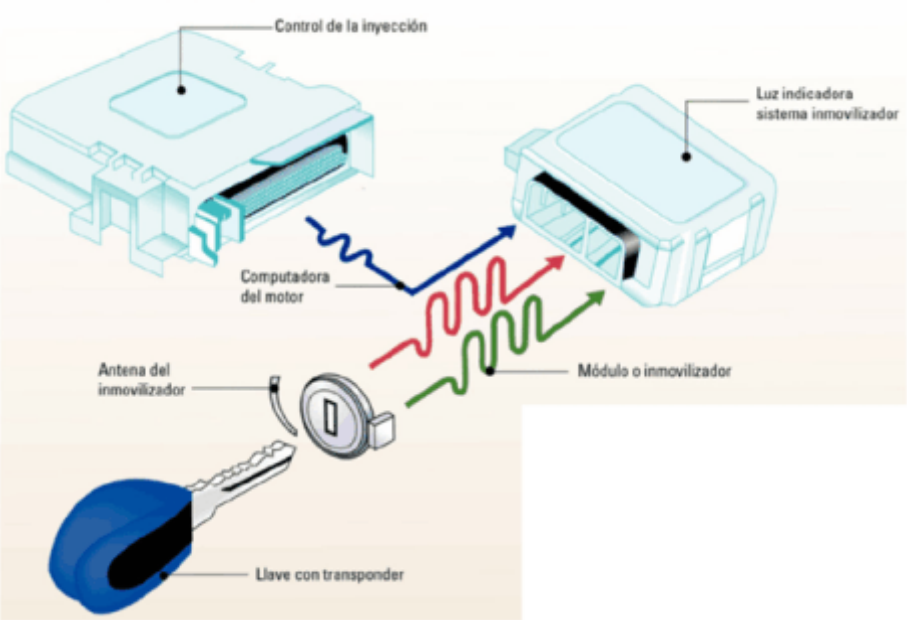


FIGURA 2. 16 ANÁLISIS DEL CÓDIGO DE LA LLAVE

1. Dispuesto el contacto de la posición 0 a II comienza la operación de verificación, en este momento tanto el PCM como el módulo Transeiver son alimentados.

2. El PCM genera un requerimiento de lectura de código al Transreceptor este a su vez envía una señal de radio frecuencia para extraer el código contenido en el transponder.

3. El transreceptor envía el código hacia el PCM, este lo analiza y compara con sus códigos programados.

4. Si el código corresponde a uno almacenado acciona el arranque y permite el encendido apagando la luz de destello de robo la cual se encuentra en el panel o tablero de instrumentos.

5. De no ser una de las llaves programadas inhibe el arranque genera un DTC P1260 (Robo de vehículo detectado) y gestiona por un minuto la luz anti robo.

Si es accionado el arranque externamente (Ejemplo by pass entre 30 y 87 del relevador), el motor de arranque girara pero no se podrá poner en marcha el motor.

En los primeros sistemas era entregada una llave maestra, la cual funcionaba como principal para programar llaves esclavas, en los sistemas más modernos es necesario programar mínimo 2 llaves adecuadas.

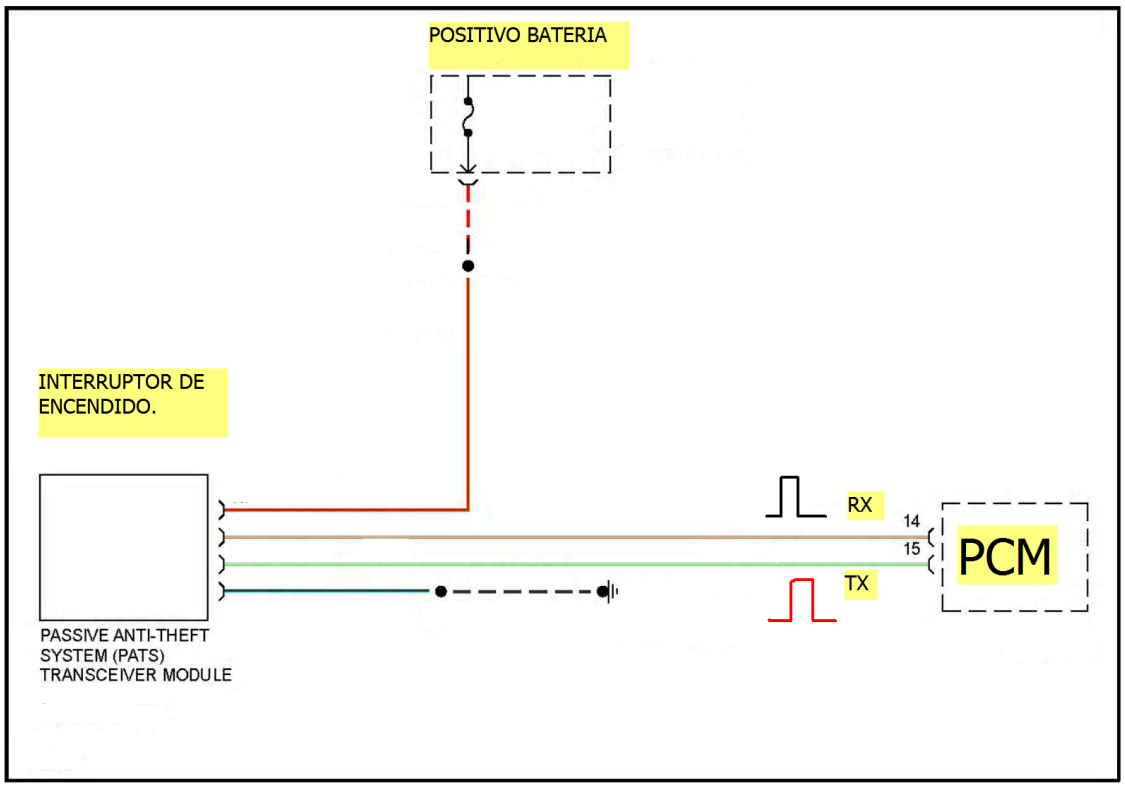


FIGURA 2. 17 CONEXIONADO ELÉCTRICO DEL SISTEMA.

En el esquema eléctrico se puede observar la conexión de un FORD ECONOLINE del año 97, en el cual el módulo TRANSRECEPTOR (Transeiver) se encuentra en el cilindro del interruptor de encendido, el Transreceptor está alimentado por positivo de Batería y cierra el circuito a masa en la carrocería, por otro lado está el PCM el cual comparte dos cables con el transreceptor TX y RX.[16]

Cuando se Dispone de la posición 0 a la II en el PCM, este envía una señal pulsante de 0 – 5 V por TX, seguida a esta señal el módulo transreceptor regresa la respuesta a la petición anterior.

Esta respuesta la genera por la línea RX, como respuesta enviara el código leído en la llave, el cual es analizado por el PCM y tomara la decisión respectiva. Todas estas comunicaciones son pulsantes, en valores 0 - 5 V.

Si alguna de estas señales se perdiera o los cableados se cortaran, se genera un DTC y el sistema queda inhabilitado.

El PCM también cuenta con sus respectivas alimentaciones y masas, según la distribución del cableado.

[16] Cise Electrónica – José M. Bustillo 3243 – (1406) Capital Federal – Buenos Aires – Argentina 5411 4637-8381
Cise Electronics Corp. 12920 SW 128 th Street – Suite 4 – Miami – Florida 33186 – USA (786) 293-1094

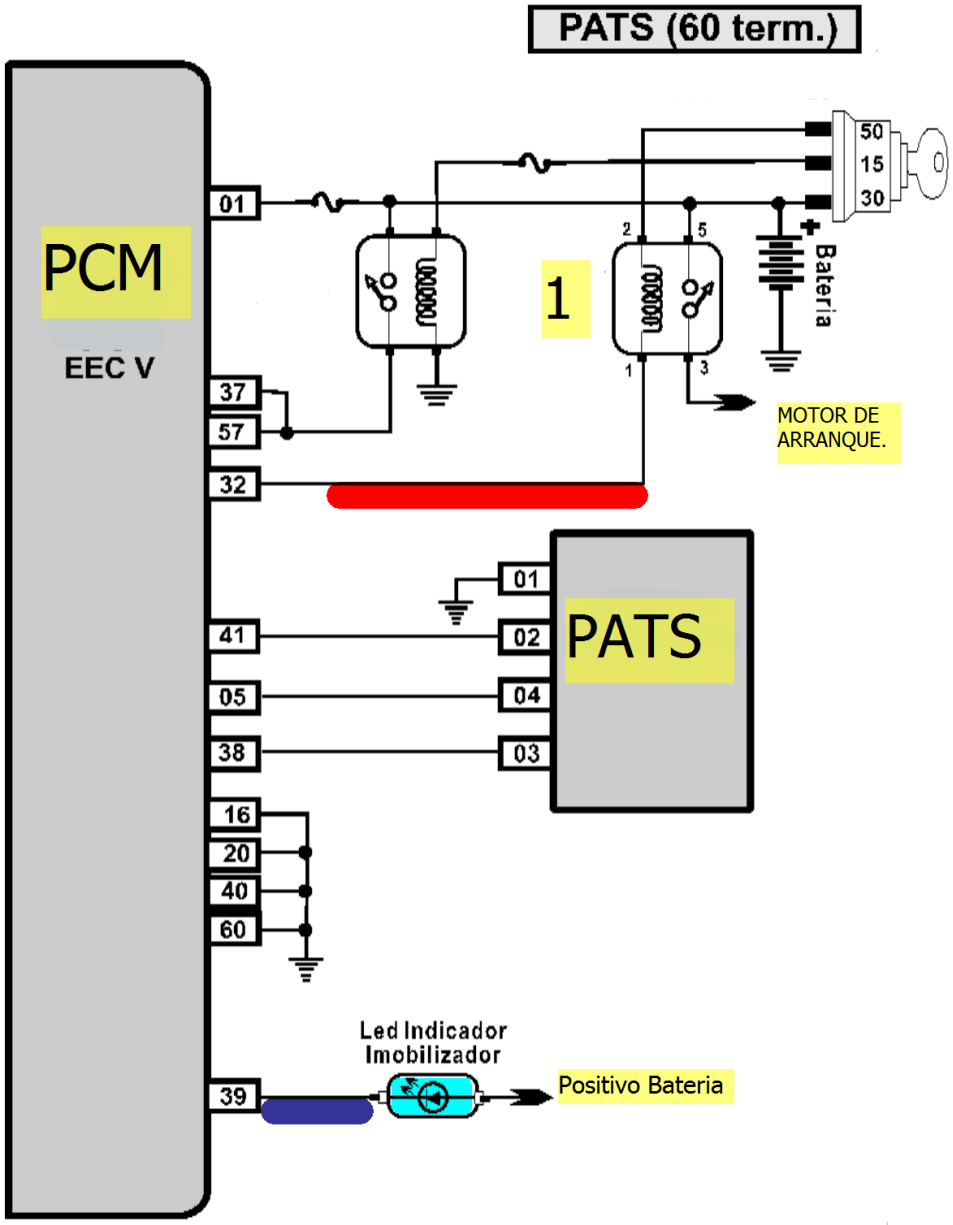


FIGURA 2. 18 En el esquema se aprecia la configuración de un FORD FIESTA.

En el esquema se puede analizar la conexión del PCM y el TRANSRECEPTOR (PATS).

La PCM está alimentada de Batería Pin 01 y Contacto 37 y 57; masas por 16, 20, 40 y 60.

El Transreceptor está conectado al PCM por 41, 05 y 38 donde tendrá uno de estos para la alimentación y, la masa estará en el pin 01 (PATS).

El indicador de robo está conectado a positivo y comandado por masa en el pin 39 del PCM como lo muestra la línea azul.

En el caso de tener la llave correcta al mover a la posición de arranque, el relevador 1 es accionado por el PCM a través de su pin 32, como lo indica la línea roja, de esta forma conmuta los contactos 3 y 5 colocando positivo al sistema de arranque (Motor de Arranque), si algo está mal en el sistema este relevador permanece inoperante y el testigo indicara el sistema activado (PATS).

2.4 SISTEMAS BIOMÉTRICOS

2.4.1 DEFINICIÓN

El término biometría proviene de los términos bio (vida) y metría (medida), estudia la identificación o verificación de individuos a partir de una característica física o del comportamiento de la persona. Esta tecnología se basa en que cada persona es única y posee rasgos distintivos que pueden ser utilizados para identificarla.

2.4.2 CARACTERÍSTICAS

Las principales características que debe cumplir un sistema biométrico para la identificación de personal son:

El desempeño: El sistema de debe ser rápido, exacto y robusto al momento de identificar a un individuo.

La aceptabilidad: El grado hasta el cual los usuarios están dispuestos a aceptar el sistema biométrico, el sistema debe proteger la integridad física de las personas y debe inspirar confianza ya que a veces en lugar de obtener información para validar un parámetro de acceso se puede estar profanando rasgos importantes del usuario.

La fiabilidad: Esta característica refleja cuán seguro es el sistema al momento de validar la información de acceso ya que en ocasiones se puede tratar de suplantar la identidad de una persona por medio de diferentes técnicas como por ejemplo crear dedos de látex, prótesis de ojos, grabaciones de voz, etc.

2.4.3 TIPOS DE SISTEMAS BIOMÉTRICOS

Entre los diferentes tipos de Sistemas Biométricos tenemos:

Rostro

Este sistema de reconocimiento es el más dable ya que el rostro es la manera directa para identificar familiares, amigos o conocidos. Los métodos utilizados en el reconocimiento de rostros van desde la correlación estadística de la geometría humana.

Iris

El método del iris del ojo es el método más raro para las personas ya que el humano no se reconoce por la apariencia del iris y también no es un método utilizado por la ley.

El método es como sigue: la imagen del iris se captura con una cámara de alta resolución y el sistema analiza dobleces y patrones, que son manejados para identificar a la persona, por lo general esto se hace acercando una cámara al ojo o mirando a través del lente de una cámara fija.

Este identificador es uno de los más precisos entre los sistemas biométricos.

Huellas digitales

Gracias a que los patrones de las huella digitales son únicos y se mantienen durante la vida de la persona, ésta es la primera técnica que se viene a la mente y de hecho es un método utilizado en diversos proyectos de muchos países para la construcción de bases de datos de huellas digitales para control y por otro lado la incorporación de la tecnología en diminutos aparatos tales como teléfonos móviles, ordenadores portátiles, teclados, tarjetas bancarias, armas de fuego, entre otros.

Firma

"La firma es un método de verificación de identidad de uso habitual, a diario las personas utilizan su firma para validar cheques o documentos importantes". Dependiendo del sistema ya sea la superficie donde se firma como el bolígrafo utilizado pueden contener varios sensores, que miden características mucho más allá que la forma o apariencia de la firma.

Voz

La voz es una característica que las personas utilizan para identificar a los demás y al igual que los sistemas basados en el rostro, goza de mucha aceptación entre sus usuarios. [17]

[17] http://www.microsoft.com/latam/technet/articulos/articulos_seguridad/NewsAbril06/abr06-01.mspx

Los sistemas de verificación mediante la voz “escuchan” mucho más allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que emitimos, estos sistemas también crean modelos de la anatomía de la tráquea, cuerdas vocales y cavidades.

En la siguiente tabla se pueden resumir las diferentes características de los sistemas biométricos.

TABLA 2. 2 TABLA COMPARATIVA DE SISTEMAS BIOMÉTRICOS

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Geometría de la mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

2.4.4 ARQUITECTURA

La arquitectura de un sistema biométrico está compuesta de dos módulos:

Módulo de inscripción.

Módulo de identificación.

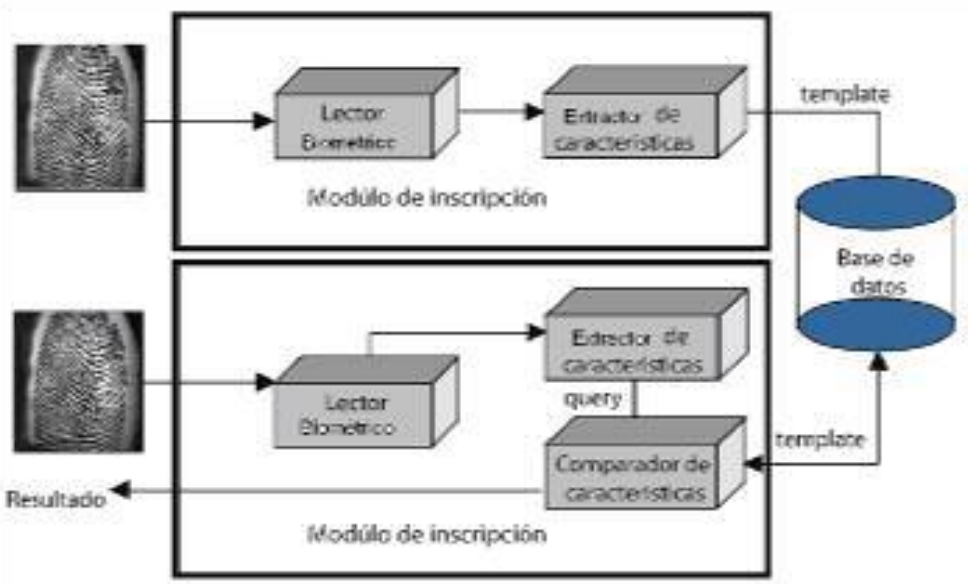


FIGURA 2. 19 Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares[18]

En el módulo de inscripción se obtiene la información proveniente de un lector biométrico elegido, luego se convierte esta información a formato digital para que luego el extractor de características produzca una representación compacta que será almacenada en la Base de Datos.

El módulo de identificación es el responsable del reconocimiento del individuo. Este proceso inicia cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de la información almacenada en la Base de Datos, esta representación es enviada al comparador de características el cual confronta con los respectivos registros almacenados en la Base de Datos para establecer la identidad.

2.4.5 FASE OPERACIONAL DE UN SISTEMA DE IDENTIFICACIÓN PERSONAL

La fase operacional en un sistema biométrico opera en 2 modos:

Modo de Verificación

[18] 6 http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

Modo de Identificación

En el modo de verificación un sistema biométrico acredita la identidad de un individuo comparando su característica con el template, así si una persona ingresa su nombre de usuario entonces no es necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino basta con comparar la información de entrada que esté asociada al usuario.

"Un sistema que esté operando en modo de identificación revela a un individuo mediante una búsqueda exhaustiva en la base de datos con los templates lo que conduce a una comparación de tipo uno a muchos para constituir la identidad del individuo". [19]

2.4.6 EXACTITUD EN LA IDENTIFICACIÓN: MEDIDAS DE DESEMPEÑO

Toda la información provista por los templates permiten particionar la base de datos conforme la presencia de ciertos patrones particulares para cada indicador biométrico. Una decisión tomada para un sistema biométrico distingue personal autorizado o impostor y para cada decisión existe dos posibles salidas de verdadero o falso, se tiene entonces cuatro posibles respuestas del sistema.

- Una persona autorizada es aceptada,
- Una persona autorizada es rechazada,
- Un impostor es rechazado,
- Un impostor es aceptado

El grado de confidencialidad asociado a las diferentes decisiones puede ser distinguido por la distribución estadística del número de personas autorizadas e impostores. Con las estadísticas anteriores se establecen dos tasas de errores:

Tasa de falsa aceptación (**FAR**: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado,

Tasa de falso rechazo (**FRR**: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor

[19] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

La **FAR** y la **FRR** son funciones del grado de seguridad anhelado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos

La FAR y la FRR están íntimamente relacionadas, efectivamente son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la figura 1.5

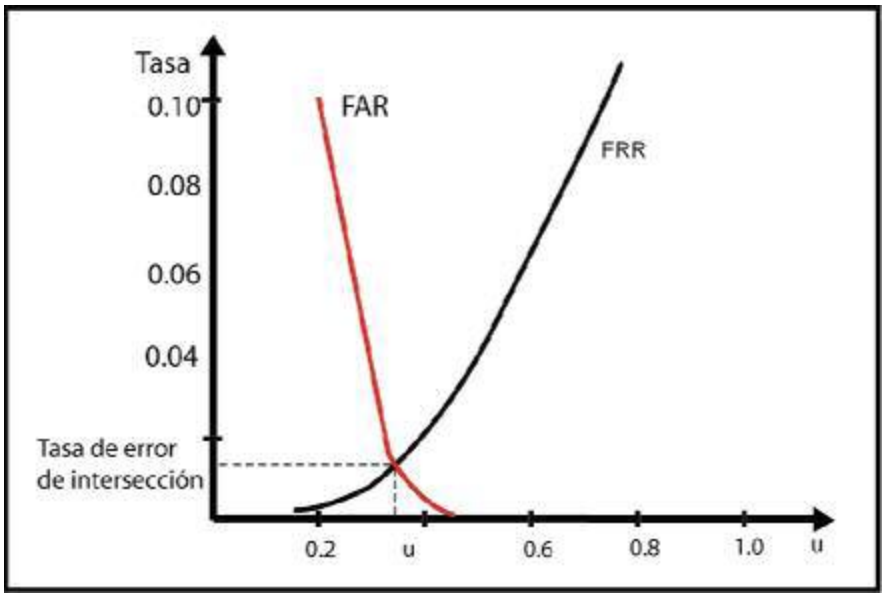


FIGURA 2. 20 Gráfica típica de FRR y de FAR como funciones del umbral de aceptación (u) para un sistema biométrico.[20]

[20] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

CAPITULO III

DISPOSITIVO BIOMÉTRICO FIM2030

En este capítulo se describe las características, el funcionamiento y el modo de utilización del dispositivo biométrico sobre el cual se desarrolla el presente trabajo. Para así crear una base solida de los alcances y limitaciones de la solución planteada en base a nuestro objetivo.

3.1 GENERALIDADES

FIM20 es un módulo de reconocimiento de huella digital autónomo compuesto por un sensor óptico y una placa de procesado. Ofrece una alta capacidad de reconocimiento y una gran velocidad para operaciones de identificación 1: N, y para la carga y descarga de datos, proporcionando las condiciones óptimas para su aplicación en sistemas de control de acceso.

Nitgen cumple con las normativas ISO9001 e ISO14001 (junio 2001)

De acuerdo a los objetivos específicos del desarrollo de este módulo de identificación biométrica, que es, realizar un sistema autónomo y versátil a la hora de crear soluciones de control de asistencia y acceso, principalmente, utilizando la huella dactilar como la herramienta de identificación. Para ello el módulo de identificación de huella dactilar FIM 2030 de NITGEN Co., Ltd. utiliza una arquitectura, basada en un DSP (Procesador Digital de Señales, en sus siglas en inglés), que permite la verificación e identificación interna de la huella dactilar, mediante sus algoritmos radicados en el propio procesador del equipo.[21]

En cuanto al desarrollo del sistema de identificación, es necesario integrar un microcontrolador de manera que el dispositivo FIM 2030 pueda ser controlado de acuerdo a las soluciones que se quiera brindar. Es decir, que en la configuración y programación del microcontrolador se basarán las soluciones, o más bien se controlarán los parámetros de funcionamiento de las soluciones que controlarán la asistencia, el acceso o la identificación biométrica para ser integrado en otros

[21] www.kimaldi.com

sistemas electrónicos que requieran de este nivel de seguridad.

El fabricante, del dispositivo FIM 2030, recomienda la utilización de un microcontrolador de la familia MSC-51 para su desarrollo. En este sentido se ha tomado el microcontrolador de marca Microchip modelo PIC16F877A, el cual nos permite alcanzar una óptima integración con este dispositivo biométrico.

El desarrollo y funcionamiento del sistema de identificación dependerá del tipo de producto que se quiera obtener, si bien es cierto que el método de identificación de un individuo realizado por el equipo biométrico no varía, la interfaz con el usuario puede cambiar, es decir, si se piensa en un equipo para controlar la asistencia se debe pensar en todos los dispositivos periféricos asociado a este tipo de solución, como son la incorporación de un visor que pueda mostrar la información que requiere y entrega el sistema, a su vez la incorporación de un teclado para la activación de las diferentes opciones e inclusive la posibilidad de integrar una impresora emisora de comprobantes de marcación. Todos estos periféricos deben ser controlados por el microcontrolador de manera de establecer un sistema totalmente autónomo de identificación. Por otro lado, para el caso de un control de acceso no sería necesario un visor o un teclado, para este caso sólo se necesitará integrar un sistema de led's luminosos que permitan brindar la información necesaria para la aceptación o rechazo de acceso a las funciones esenciales del vehículo. Bajo esta perspectiva el desarrollo de este proyecto se basa principalmente en el desarrollo del sistema de identificación biométrica, de manera que pueda ser fácilmente adaptable a este tipo de soluciones, es decir, que el resultado de este proyecto se obtendrá en el corazón del identificador biométrico de huella dactilar que luego se podrá adaptar con un mínimo de desarrollo a las distintas soluciones planteadas.

Para la integración del FIM 2030 con el microcontrolador, es necesario conocer y utilizar el leguaje propio del dispositivo FIM 2030, para ello se deben establecer la correcta comunicación bajo los parámetros y estructura de información que requiere el dispositivo FIM 2030. (Ver anexos A-E)

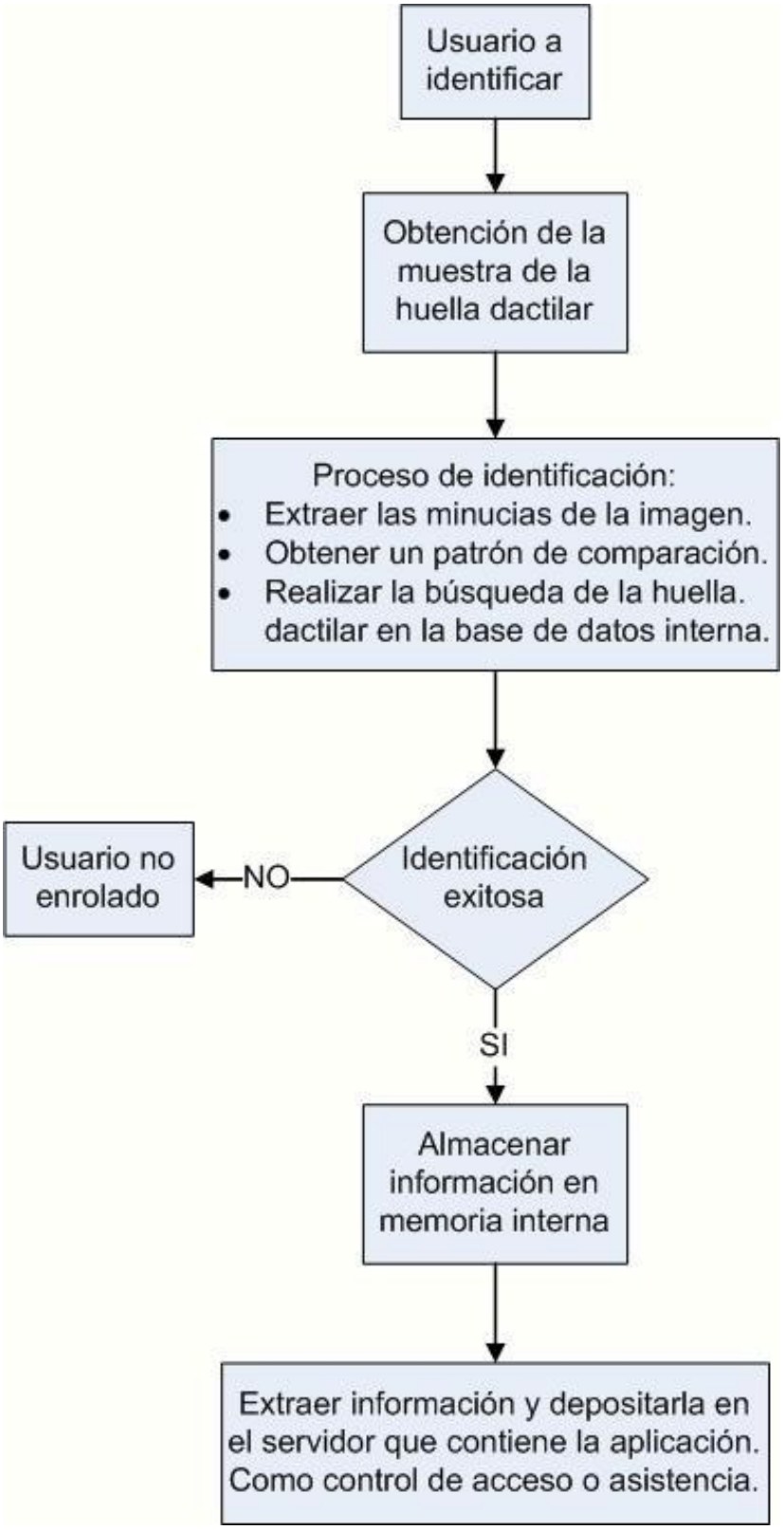


FIGURA 3. 1 Diagrama de funcionamiento del sistema biométrico

Fuente: Propia. (2010)

3.2 CUALIDADES DEL SENSOR

El mercado ofrece una gran gama de productos, los cuales permiten desarrollar sistemas basados en la biometría y precisamente en la huella dactilar. Donde se puede encontrar diversos tipos de tecnologías pudiendo ser adaptados en distintas aplicaciones. Entonces dentro de este marco global, el cual encierra muchos tipos de sensores, fue necesario analizar el tipo de aplicación que se requiere aplicar y decidir, bajo ciertos parámetros de carácter técnico, un sensor que cumple con las principales características para este desarrollo, entre las que destacan:

- **Excelente calidad de imagen:** el lector óptico permite obtener imágenes claras de la huella dactilar, libre de distorsión, generadas usando un avanzado y patentado método óptico de captura. Esta calidad de imagen brinda un mejor muestreo a la hora de extraer la información de las minucias.
- **Durabilidad:** las pruebas mecánicas de fuerza muestran alto grado de resistencia al impacto, descargas y ralladuras.
- **Software:** una de las principales características es que cuenta con un algoritmo de procesamiento rápido y preciso, lo que se traduce en un equipo eficiente y confiable.
- **Duración y versatilidad:** debido a la composición física del dispositivo y la alta calidad de sus componentes permiten su uso bajo condiciones extremas de uso y ambientales, considerando los parámetros adecuados de medición de estas condiciones y para estos tipos de dispositivos.
- **Diseño ergonométrico:** diseño compacto y modular de fácil integración en pequeños dispositivos, de fácil uso y su compatibilidad lo hace ideal para una amplia gama de usos.
- **Bajo costo:** el dispositivo es desarrollado para entregar un alto rendimiento, cero mantención y bajo costo de producción y desarrollo, muy conveniente para el uso general e industrial.

3.3 VENTAJAS DEL FIM2030 FRENTE A OTROS SENSORES ÓPTICOS

Debido a la diversidad de sensores existentes, estos se dividen en varios tipos de tecnologías para el reconocimiento de huella dactilar. Entre los que se encuentran la tecnología de sensores ópticos, los cuales a partir del contraste de la imagen obtenida del sensor, se pueden extraer las minucias para su análisis.

El equipo de desarrollo FIM 2030, corresponde a un sensor de tecnología óptica y presenta las siguientes ventajas frente a otros sensores ópticos:

- Módulo de reconocimiento de huella autónomo ideal para integradores tanto para aplicaciones on-line como off-line.
- La tecnología de escáner óptico ofrece máxima robustez, durabilidad, seguridad contra descargas, facilidad para el usuario y alta resolución en la captura de huellas.
- **Aplicaciones off-line:** Los usuarios se guardan en la memoria del equipo (hasta para 4.000 huellas) y se identifica usando el motor de búsqueda del algoritmo interno.
- **Aplicaciones on-line:** La huella dactilar que se pretende verificar (1:1) o identificar (1: N) se almacenan en la memoria no volátil del módulo, o se envían a partir del puerto RS-232 para que sean reconocidas por el equipo.
- Método único de captura de detalles finos, incluso desde piel seca.
- Muy baja distorsión de imagen.
- Materiales reforzados.
- Larga duración.
- De tamaño pequeño y atractivo.
- Fácil de integrar.
- Listo para su uso.
- Bajo costo con una vida más larga y sin requisitos de mantenimiento.
- Funcionalidad off-line y on-line incorporada

3.4 VENTAJAS DEL FIM 2030 FRENTE A SENSORES CAPACITIVOS.

Otro tipo de tecnología es la capacitiva, la cual funciona a través de las características electromagnéticas de la piel. Este tipo de sensor detecta la diferencia de capacidades entre la huella y el propio sensor.

Las ventajas del sensor FIM 2030 frente al sensor capacitivo son:

- Componentes no metálicos ni siliconosos permiten menos susceptibilidad a la corrosión cuando está expuesto a sales, al aceite y a la humedad de la piel y del ambiente.
- Las características superiores de tratamiento de la superficie eliminan la necesidad de realizar costosos procedimientos de capas superficiales.
- Gran robustez mecánica, resistencia y durabilidad.
- Una amplia gama de aplicaciones, especialmente para el uso en condiciones extremas de clima.
- Inmunidad a la descarga electroestática.
- Bajo costo con una larga vida de uso y sin requisitos de mantenimiento.
- Robustez del algoritmo y software.
- Algoritmo único de procesamiento de imagen, gran exactitud al extraer las minucias de la huella digital.
- Alta relación señal a ruido del algoritmo de procesamiento, elimina los factores falsos de identificación.
- Rápido proceso de extracción de la imagen de la huella para su comparación y verificación.
- Función de encriptación para proteger la privacidad del usuario.
- Compatibilidad con Laptop y PC’s.
- Fácil desarrollo de aplicaciones para variados propósitos.

3.5 DESCRIPCIÓN DEL DISPOSITIVO

FIM20 es un módulo de reconocimiento de huella digital autónomo compuesto por un sensor óptico y una placa de procesado.

Mediante la incorporación de una CPU de gran velocidad y un algoritmo de

reconocimiento de huella optimizado, el FIM20 ofrece una alta capacidad de reconocimiento y una gran velocidad para operaciones de identificación 1: N, y para la carga y descarga de datos, proporcionando las condiciones óptimas para su aplicación en sistemas de control de acceso. [22]

FIGURA 3. 2 Tarjeta controladora del dispositivo biométrico

FIGURA 3. 3 SENSOR BIOMÉTRICO

El FIM20 dispone de entradas digitales para registro de huellas, identificación, borrado parcial o completo y reset, de forma que no requiere conexión a un PC y

[22] www.kimaldi.com . (2010)

ofrece un entorno de desarrollo cómodo y seguro para aplicaciones off-line. [23]

En aplicaciones off-line habitualmente se guardan los usuarios en la memoria del equipo (para hasta 4000 huellas) y se identifica usando el motor de búsqueda del algoritmo interno. El módulo de reconocimiento biométrico de huella dactilar FIM20 también es ideal para aplicaciones on-line, pues admite comandos ASCII para controlar el equipo desde un host.

En las aplicaciones on-line, las huellas dactilares que se pretende verificar (1:1) o identificar (1: N) se almacenan en la memoria no volátil del módulo o se envían a partir del puerto RS-232 para que sean reconocidas por el equipo. Alternativamente, se usa el FIM20 únicamente como lector de huellas dactilares y se hace el reconocimiento en el PC usando las librerías de desarrollo de software SDK eNBSP.

3.5.1 PRINCIPALES CARACTERÍSTICAS

- Funcionalidad de identificación de huella dactilar on-line y off-line incorporada.
- Diseño optimizado para aplicaciones de control de acceso: tiempo de identificación reducido mediante algoritmo de reconocimiento 1:N.
- Alto grado de precisión en la identificación, incluso con huellas de pequeño tamaño, húmeda o seca
- Rápida adquisición de todo tipo de huellas prácticamente bajo cualquier condición
- Tasa de identificaciones muy elevada: FAR: 1/100.000 y FRR: 1/1.000
- Distintas configuraciones de usuarios (1.000 o 4.000) y carga y descarga remota de la información de las huellas de los usuarios
- Métodos de autentificación: verificación 1:1 y identificación 1:N.
- El acceso al dispositivo desde el host puede protegerse por huella o password
- Memorización de eventos: hasta 8.000 autenticaciones

[23] http://www.kimaldi.com/productos/sistemas_biometricos/biometricos_para_integracion/mòdulo_de_huella_dactilar_nitgen_fim30

- Ofrece un entorno de desarrollo cómodo sin necesidad de conexión a PC (aplicaciones off-line)
- Dos puertos de comunicaciones RS-232 para conexión a PC o host (aplicaciones on-line)
- Tamaño reducido, robustez y larga vida sin mantenimiento
- Protocolo de comunicaciones ASCII
- Tensión de alimentación de 5V
- Algoritmo y sensor óptico de elevada dureza (7 Moh)
- Compatible con normativa RoHS

3.5.2 MODELOS

Dos formatos de escáner óptico:

- Los modelos FIM2030 incluyen un módulo óptico más compacto de dimensiones más reducidas.
- Los modelos FIM2040 incluyen un módulo óptico compatible con el anterior modelo FIM01.
- Disponible cavidad para integrar el sensor óptico en una superficie plana para los dos modelos.
- Los dos modelos están disponibles con memoria para 1.000 y 4.000 usuarios. [24]

3.5.3 APLICACIONES

- Sistemas de control de acceso
- Sistemas de control de presencia
- Sistemas de gestión de asistencia laboral
- Cajeros automáticos
- Terminales de punto de venta
- Otras aplicaciones en las que se requiera identificación cómoda y segura para el usuario (sin posibilidad de suplantación de identidad)

[24] www.kimaldi.com / FIM2030 & FIM2040 DataSheet

3.5.4 REFERENCIAS DEL PRODUCTO

- Módulo FIM2030 - 1Mb (1.000 usuarios): 45FIM033

- Módulo FIM2030 - 1Mb + batería: 45FIM045

- Módulo FIM2030 - 4Mb (4.000 usuarios): 45FIM034

TABLA 3. 1 ESPECIFICACIONES DEL HARDWARE DE FIM 2030

ITEM		FIM20xx
Board Spec.	CPU	S2C2410 (ARM9)
	DRAM	8Mbyte SDRAM
	Flash ROM	Program Flash: 1Mbytes DB Flash: 1/2/4 Mbytes
Dimension		43 x 93 [mm^2]
Sensor		NITGEN OPP03 (in FIM2030) NITGEN OPP04 (in FIM2040)
Supply Voltage		5 ± 0.5 [V]
Current Consumption		Max. 300 [mA]
Operating Temperature		-20 ~ 60 [℃]
Humidity		5 ~ 95 [% RH]
ESD Tolerance		±8 [KV] (indirect)
Communication Channel		2 Port RS-232 Speed: 9600 ~ 115200 [bps]
External I/O		3 Input (for Demo Only) 2 Relay Output, 2 Reserved Input

TABLA 3. 2 ESPECIFICACIONES DE OPERACIÓN

ITEM	FIM20xx
Capture Speed	0.3(normal) / 1.1(secure) sec
Verification Speed	1.8 [sec] (Capture + Extract + Match)
Boot Up Time	Max. 0.7 [sec] for 100 users Max. 1.0 [sec] for 500 users Max .2.0 [sec] for 1000 users Max. 4.0 [sec] for 2000 users Max. 12.0 [sec] for 4000 users
Data Encryption Method	AES for saving data AES for DB communication

FUENTE: NITGEN - FIM20xx DataSheet

3.6 FUNCIONAMIENTO

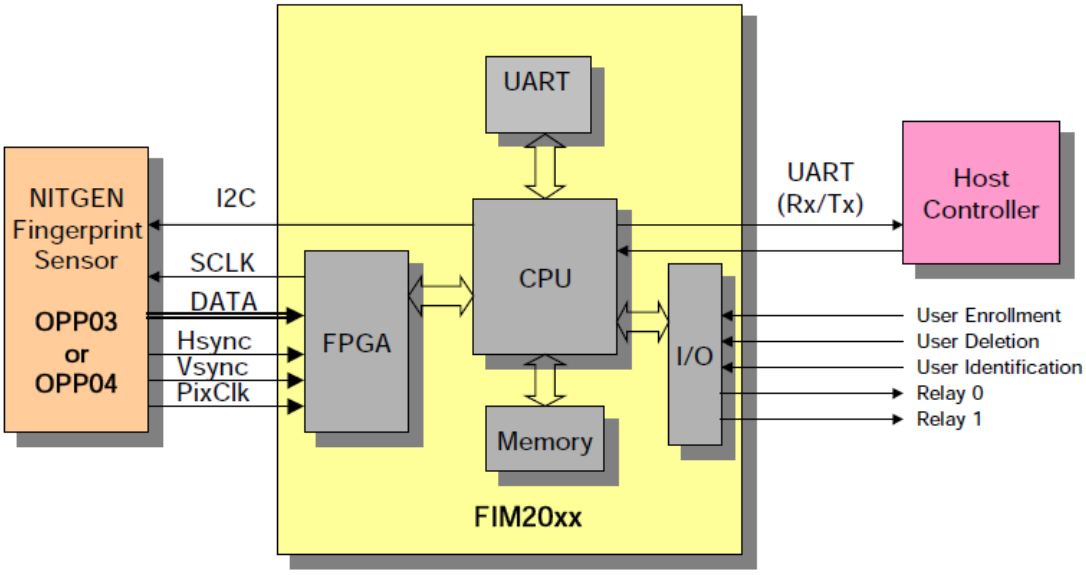


FIGURA 3. 4 Diagrama de bloques del FIM2030[25]

3.6.1 RESET

FIM20xx proporciona un puerto externo para la reinicialización a través de una señal de cero lógico. Poniendo en estado bajo al puerto de la reinicialización el módulo FIM20xx se inicializa. Entonces el puerto reset es internamente puesto a VCC.

Cuando el sistema se enciende, la CPU es automáticamente inicializada, sin embargo cuando algún error ocurre durante la operación será necesario realizar manualmente la inicialización del sistema (presionando el botón de reset). Para aplicaciones que requieran que la inicialización se realice por programa externo, se debe asegurar que la señal EX_RESET # esté conectada a tierra.

[25] NITGEN - FIM20xx DataSheet

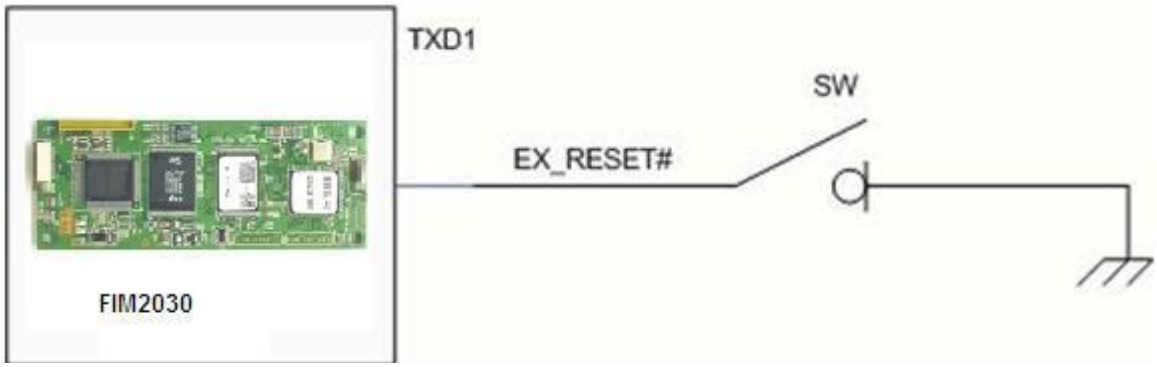


FIGURA 3. 5 Reset Externo

Fuente: Propia. (2010)

3.6.2 COMUNICACIÓN

FIM20xx tiene dos puertos de comunicación RS-232 a través de estos FIM20xx se comunica al mismo tiempo. Estos puertos soportan 6 modos de baudrate como son 9600, 14400, 19200, 38400, 57600, y 115200 bps.

FIM20xx sigue el protocolo de Comunicación Serial de NITGEN. (Ver anexos A-E)

3.6.3 ZONA DE DATOS DE USUARIO

FIM20xx proporciona 64 Kbytes de memoria flash. Usando esta memoria, el host (organizador) puede guardar los datos privados para su uso específico.

3.6.4 RELÉS DE SALIDA

FIM20xx tiene dos puertos de salida para señal de relé. Después de ejecutar las órdenes concordantes, tales como la Comprobación, Identificación, Emparejamiento y así sucesivamente, el resultado es el presentado en el puerto de RELAY_0.

Si el resultado es el deseado, el puerto es puesto en estado alto. La duración de estado alto es controlada por la tabla de configuración del sistema. Puede establecerse una señal en los puertos de salida del relé o puede restablecerse sin tener en cuenta el resultado concordante para varios usos.

3.6.5 TECLAS DE FUNCIÓN

FIM20xx soporta 3 teclas de función de entrada tales como Enroll_Key, Delete_Key, e Identify_Key. Usando estas teclas sin la comunicación serial, el registro, el borrado, el borrado total y las operaciones de identificación pueden ser ejecutados.

El siguiente diagrama de tiempo y la tabla muestran las condiciones de operación de las teclas de función.

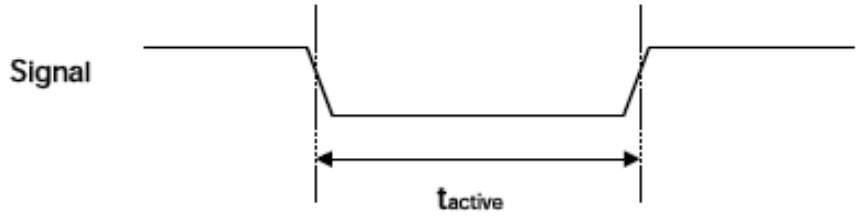


FIGURA 3. 6 Señal de tecla de función

TABLA 3. 3 SEÑAL DE TECLAS DE FUNCIÓN

Command	Signal Name	t_{active}	
		Minimum [ms]	Maximum [ms]
CMD_ENROLL	/ENROLL_KEY	30	
CMD_DELETE	/DELETE_KEY	30	3,000
CMD_IDENTIFY	/IDENTIFY_KEY	30	
CMD_DELETE_ALL	/DELETE_KEY	3,000	

3.6.6 CONTROLADOR PRINCIPAL

El controlador principal puede ser un microcontrolador convencional como es el 16F877a que cuenta con un puerto serial. El esquema de funcionamiento del sistema consiste en que el controlador principal envía el comando de acuerdo a un cierto protocolo definido y la unidad de proceso del FIM2030 analiza, procesa y realiza el comando definido. Esta comunicación es realizada a través del puerto serial entre los dos componentes.

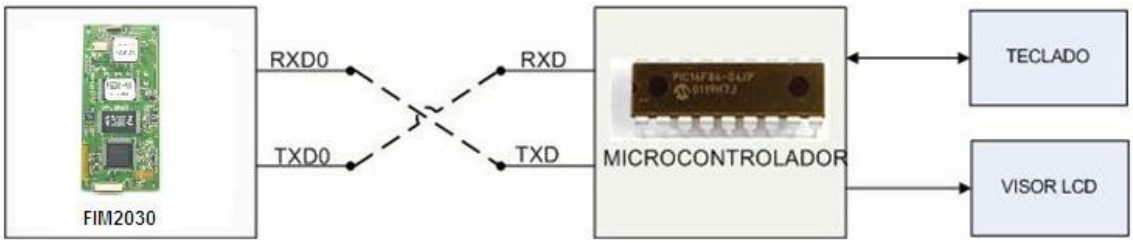


FIGURA 3. 7 Conexión entre el fim2030, un microcontrolador y dispositivos externos.

Fuente: Propia. (2010)

3.6.7 FUNCIONAMIENTO DEL SISTEMA DE RELÉ

La tarjeta controladora del FIM2030 lleva integrado un circuito conectado por **Open Collector**. La corriente eléctrica requerida para el funcionamiento del relé varía de acuerdo a la resistencia de la base del transistor, en este caso, la resistencia está seteada para 5 V y una corriente de 100 mA.

Este relé también debe ser operado por señales de comando generados desde el controlador principal, que en este caso corresponderá al microcontrolador. Es de gran importancia la configuración y utilización del relé a la hora de crear un equipo que sea capaz de generar señales para apertura de puertas, en caso de controlar accesos restringidos, o la activación de las funciones esenciales del vehículo cuando se requiera de la seguridad que brinda la identificación biométrica.

3.7 PROTOCOLO DE COMUNICACIÓN SERIAL[26]

La comunicación entre la CPU integrada en la tarjeta controladora del FIM2030 y el controlador principal es realizada a través del puerto serial. La velocidad de comunicación puede ser ajustada a 9600, 19200, 38400, 57600 o 115200 bps.

3.7.1 ESTRUCTURA DE PAQUETE

La comunicación entre la CPU del FIM2030 y el controlador principal es realizada usando dos tipos de paquetes de datos llamados “Paquete de Comando” y “Paquete

[26] EN-FIM-ComProtocol-v1.75

de respuesta". Tanto el controlador principal (Pic16F628A), como el FIM2030, deben recibir estos datos de acuerdo a la longitud especificada (8 bits), debido a que el valor del campo así lo indica.

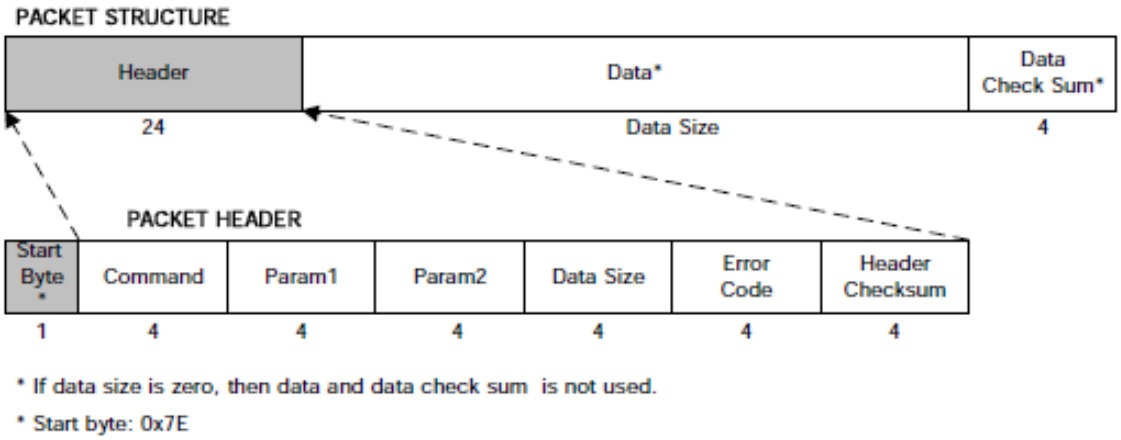


FIGURA 3. 8 Estructura del paquete de datos

La figura muestra la organización de un paquete. El paquete consiste en un byte de la partida "**start byte**", el encabezado "**header**", **data size** (optativo), y el control de datos "**Check Sum**" (optativo). El bloque de datos "**Data**" y el bloque de control de datos "**Check Sum**" sólo se envía si es necesario.

El tamaño máximo de un paquete de datos es de 64Kbytes.

Size (Start Byte) + Size (Header) + Size (Data) + Size (Data Checksum) ≤ 65,536

Si el tamaño de los datos es tan grande que el **host/device** (dispositivo controlador) no pueden llevar los datos en un solo paquete, el host/device divide los datos en pequeños bloques de datos y los envía encima de varios paquetes subsecuentes. Y el índice del paquete tiene el valor de 0 a 255.

3.7.2 DEFINICIÓN DE CAMPOS

Start byte: byte de partida.

Command: Campo de comando.

Param1: El primer parámetro donde la información es transmitida.

Param2: El segundo parámetro donde la información es transmitida.

Data Size: Tamaño de dato.

ErrorCode: Corresponde al resultado de ejecución del comando.

Checksum: Usado para la detección de errores de comunicación.

El campo **Command**, corresponde al comando que la unidad de procesos del FIM2030 ejecuta. Muchos comandos requieren parámetros para transmitir información, y en este caso, esto ocurre a través de Param1 y Param2.

3.7.3 CÓDIGO DE ERROR[27]

Si el **host** envía el paquete de comando, el dispositivo devuelve el paquete reconocido con el código de error del paquete. Si el Código de Error no es "**ERR_NONE**", el paquete de comando previamente enviado se ignora en el dispositivo. El host necesita verificar el código de error devuelto, y entonces reintenta o hace algo.

TABLA 3. 4 CÓDIGO DE ERRORES

LISTA DE CÓDIGO DE ERROR	
ERR_NONE	El paquete del comando se ejecutó con éxito
ERR_CHECKSUM_ERROR	Allí existe error del Checksum en el *header* o *data block*.
ERR_INVALID_CMD	El comando enviado al dispositivo no es válido.
ERR_UNSUPPORTED_CMD	El comando enviado al dispositivo no es soportado.

[27] EN-FIM-ComProtocol-v1.75

3.7.4 COMO SE UTILIZAN LOS PAQUETES

Todos los comandos son transmitidos desde el controlador principal, que, en este caso, se trata de un microcontrolador, al propio FIM2030. El FIM2030 por su parte replica todos los comandos con una respuesta usando el mismo formato que el paquete de comando al **host** principal. El FIM2030 envía los resultados del comando en el campo **ErrorCode** del ACK. Si la ejecución del comando se completa sin errores, el **ErrorCode** es 0 (**ERR_NONE**).

Ejemplo:

La siguiente representación muestra el paquete de comando, cuando se usa el comando CMD_FP_VERIFY (0x11) para verificar a un usuario cuyo ID es 1234. El comando es 0x11, Data es 0x1234.

TABLA 3. 5 EJEMPLO DE PAQUETE DE COMANDO

Command	0x00000011									
Param1	0x00000000									
Param2	0x00000000									
Data Size	0x0000000A									
Error Code	0x00000000									
Header Checksum	0x0000001B									
Data	0x31	0x32	0x33	0x34	0x00	0x00	0x00	0x00	0x00	0x00
Data Checksum	0x000000CA									

La siguiente la tabla muestra la sucesión de datos a ser transmitidos al dispositivo.

7E	00 00 00 11	00 00 00 00	00 00 00 00	00 00 00 0A	00 00 00 00	00 00 00 1B

31 32 33 34 00 00 00 00 00 00	00 00 00 CA

3.8 GUÍA DE DISEÑO MECÁNICO

3.8.1 MONTANDO EL MÓDULO ÓPTICO

En la figura Nº 30 se muestra la correcta posición del dedo sobre el lector biométrico.

El correcto posicionamiento del dedo requiere que la yema del dedo se extienda por sobre la ventana óptica por unos milímetros. La distancia de esta proyección está representada en la figura por la letra D, y varía dependiendo del tamaño del dedo de cada persona. Para este propósito, se puede decir que la distancia D es equivalente a 5 milímetros. Esto es debido, a que la información más importante usada por el lector de huella dactilar se encuentra en el cojinete más protuberante del dedo.

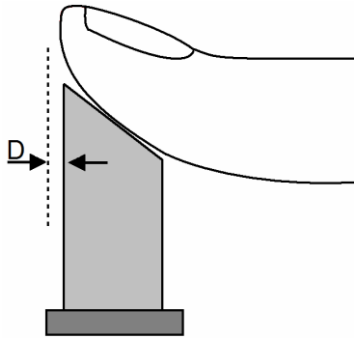


FIGURA 3. 9 Correcta posición del dedo

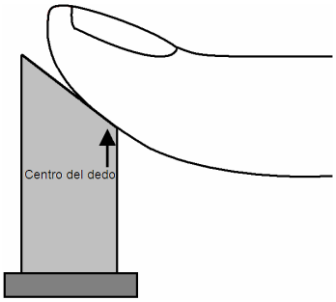


FIGURA 3. 10 Incorrecta posición del dedo

Fuente: Propia. (2010)

Para conseguir un buen desarrollo del producto se requiere de una carcasa o **housing** que permita un posicionamiento cómodo y óptimo para su correcta lectura. Es por esta razón que se detallan las características de dimensiones del lector con el cual se realizará el estudio de la estructura que sostendrá el dispositivo.

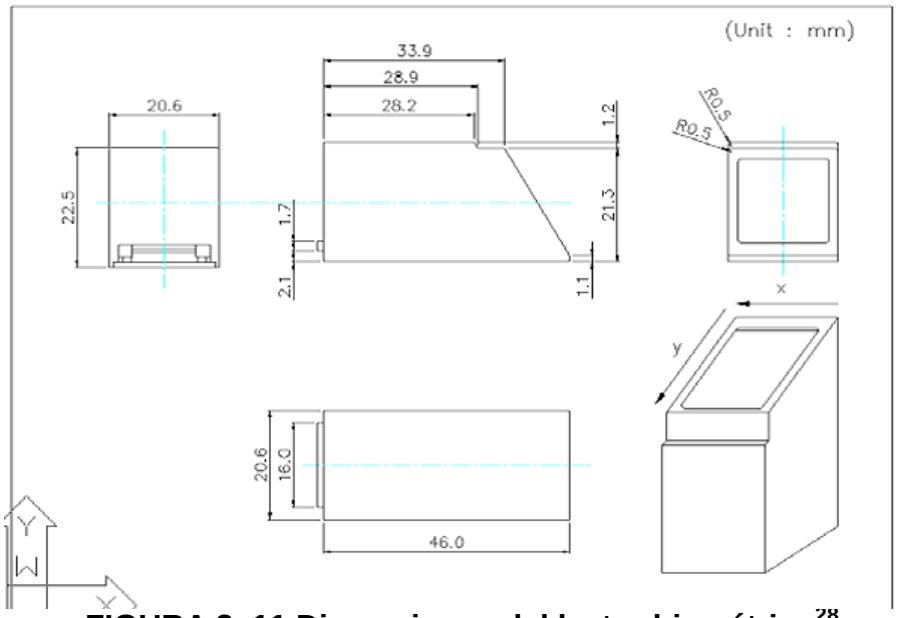


FIGURA 3. 11 Dimensiones del lector biométrico[28]

Para el caso de la placa que contiene el procesador del dispositivo es necesario utilizar pernos M3 para su montaje.

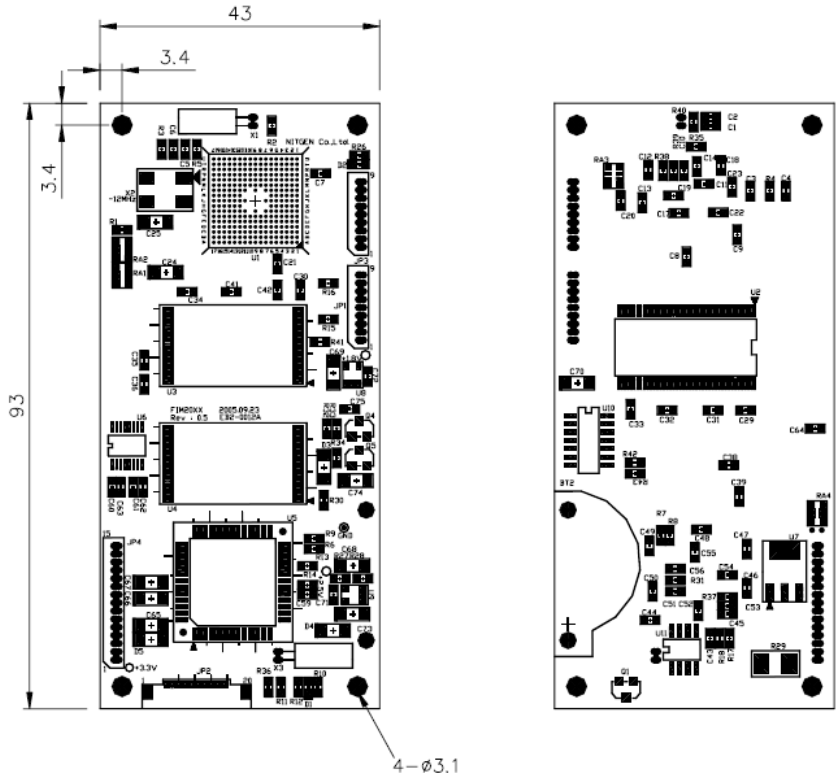


FIGURA 3. 12 Dimensiones de la tarjeta controladora del FIM2030

[28] FIM2030 DATASHEET. (2010)

3.8.2 CONSIDERACIONES ELÉCTRICAS.

Fuente de poder, en la tabla se muestra las especificaciones de energía del FIM2030. El dispositivo debe ser energizado por un adaptador de corriente continua de 5V, el cual alimentará indirectamente al módulo del sensor óptico, las fluctuaciones en la fuente de poder pueden afectar a la calidad de la imagen y el tiempo de procesamiento durante la captura de la huella dactilar.

Se debe considerar que al desarrollar e integrar dispositivos al FIM2030 que requieran largos consumos de energía, es recomendable usar fuentes de poder separadas para cada dispositivo, independientes al FIM2030.

TABLA 3. 6 ESPECIFICACIONES DE ENERGÍA

Parameter	MIN.	TPY.	MAX.	UINTS
Power				
Supply current			300	mA
Supply Voltage	4.5	5.0	5.5	V
RS-232				
Output Voltage Swing	±5.0	±5.4		V
Input Voltage Range	-15		+15	V
Input Threshold LOW	0.6	1.2		V
Input Threshold HIGH		1.5	2.4	V
Maximum data rate			115,200	BPS
Relay				
Output Voltage HIGH	2.4			V
Output Voltage LOW			0.4	V
Etc				
Reset pulse Width	1			ms

Fuente: FIM2030 DATASHEET. (2010)

3.8.3 DESCARGA ELECTROESTÁTICA

La figura 34 muestra los potenciales daños producidos por las descargas electroestáticas transferidas desde el metal al dispositivo, ya sea al lector óptico, o en la tarjeta de procesamiento. Estos componentes han sido testeados ante descargas electroestáticas a un nivel de ± 8.0 KV, es por esta razón, que es necesario un buen estudio de diseño para la carcasa del equipo, teniendo en cuenta

las distancias entre el case y los elementos que produzcan potenciales descargas.

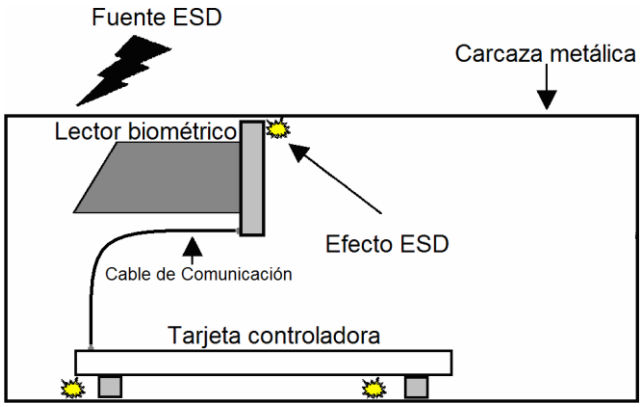


FIGURA 3. 13 El efecto de descarga electroestática[29]

3.8.4 INICIALIZACIÓN DEL PUERTO SERIAL

La comunicación serial del dispositivo FIM2030 está definida como RXD0 y RXD1 (para la recepción de la información) y TXD0 y TXD1 (para la transmisión de la información) sobre un conector de 15 pines. En la figura se muestra una señal de transmisión inesperada generada por el TXD1 del FIM2030 al encender el dispositivo. Esta es una posibilidad que los niveles de la señal puedan variar levemente y en forma uniforme entre las componentes hechas por el mismo fabricante, esto es importante para asegurarse que los buffers RX (de recepción) se encuentren limpios al inicializar para que este tipo de señales falsas no puedan causar un mal funcionamiento del dispositivo.

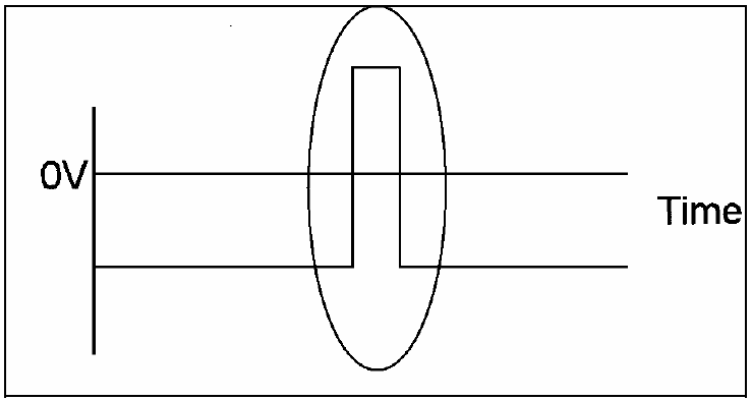


FIGURA 3. 14 Señal generada por la inicialización del CPU

[29] Aplication Design Guide.

3.8.5 CONSIDERACIONES AMBIENTALES

Al igual que todo componente electrónico, tienen algunas consideraciones del entorno donde se utilizará para su buen funcionamiento. En este caso se deben considerar, además, factores ambientales que determinarán el óptimo funcionamiento del equipo.

Temperatura Ambiental

La temperatura máxima de operación del dispositivo FIM2030 es de -20 ~ 60 [℃]

Luz exterior

La luz ambiental puede afectar la sensibilidad del sensor óptico del dispositivo FIM2030. Es por esta razón que se hace fundamental tener estos factores en conocimiento a la hora de realizar el estudio y evaluación de la carcasa del equipo, donde se debe considerar el efecto de la luz intensa y directa sobre el sensor.

Guía de enrolamiento de la huella dactilar.

Enrolamiento de la huella dactilar

3.8.6 COMO FUNCIONA

Cuando los usuarios colocan el dedo sobre el dispositivo de reconocimiento de huella dactilar por primera vez, el dispositivo toma y captura la imagen de la huella. Todas las huellas dactilares contienen un número de características físicas únicas, llamadas minucias, las cuales contienen aspectos y características visibles de la huella como son las crestas y valles, terminaciones y bifurcaciones. La mayoría de las minucias se encuentran en los puntos bases de la huella dactilar, y los mismos puntos bases se encuentran cerca del centro de la yema de los dedos en la protuberancia del dedo.

En la figura se muestra la posición de los puntos bases, en los distintos diseños de huella dactilar.

FIGURA 3. 15 Puntos bases en diversos patrones de la huella digital

3.8.6.1 Reconocimiento de huellas dactilares.[30]

Entre todas las técnicas biométricas, la identificación basada en las huellas dactilares es el método más viejo, el cual ha sido usado en numerosas aplicaciones. Una huella está formada por una serie de crestas y surcos localizados en la superficie del dedo. La singularidad de una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como el de detalles.

Existen dos técnicas para realizar la verificación de las huellas: [31]

Basada en Detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza está aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. Entre algunos detalles que podemos encontrar en una huella, tenemos:

FIGURA 3. 16 Detalles de las huellas digitales

[30] http://www.engr.sjsu.edu/biometrics/
[31] http://www.biometricpartners.com/Home/index.html

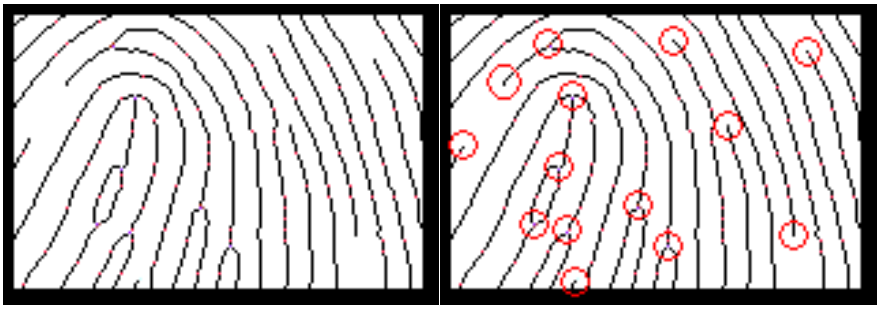


FIGURA 3. 17 Trazado del patrón de detalles.

Cada individuo posee uno y solo uno, arreglo de detalles. El mismo puede ser descrito por un modelo de probabilidad:

P(C)=P(N).P(M).P(A)

Donde: P(C) = f (Ley de Poisson)

P (M)= f (frecuencia de aparición del detalle)

P(A) = f (número de permutaciones posibles de detalles)

Basadas en correlación: Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, está técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

Una vez obtenida la huella digital es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto con la finalidad de reducir el tiempo de búsqueda. Los algoritmos existentes permiten clasificar la huella en cinco clases:

1. Anillo de Crestas.
2. Lazo Derecho.
3. Lazo Izquierdo.
4. Arco.
5. Arco de Carpa.

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0°,

45°, 90° y 135°) mediante un proceso de filtrado de la parte central de la huella

Dentro del proceso de reconocimiento es necesario emplear técnicas muy robustas que no se vean afectadas por algún ruido obtenido en la imagen además de incrementar la precisión en tiempo real. Un sistema comercial empleado para la identificación de huellas dactilares requiere de un muy bajo promedio de rechazos falsos (FRR)1 para un promedio de aceptación falso (FAR)2. Como por ejemplo:

Un dedo (FRR y FAR): 1:1000

Dos Dedos (FRR y FAR): 1:1000000

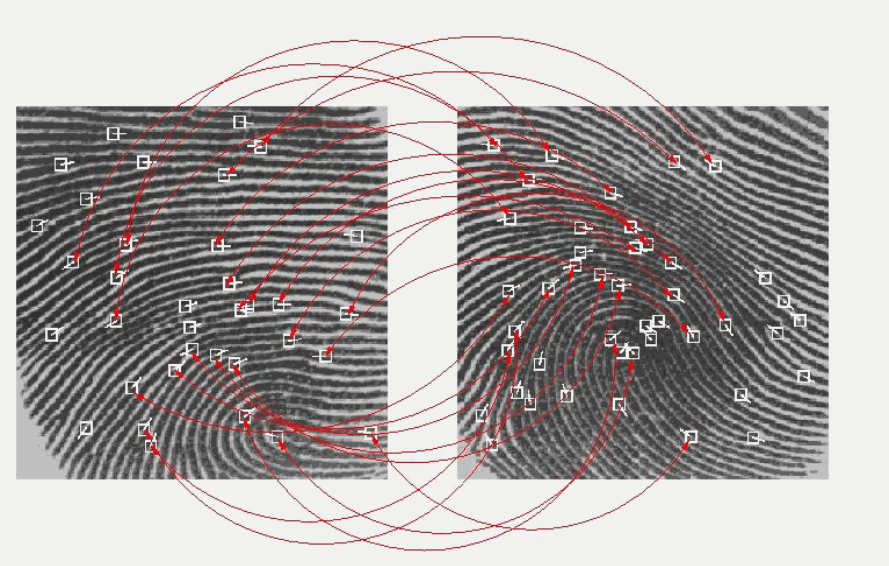


FIGURA 3. 18 Proceso de comparación.

El usuario es enrolado, o registrado, en la base de datos, luego de un algoritmo especial basado en la extracción de minucia. Las minucias dominantes desde la imagen obtenidas del lector biométrico, convierte los datos en un arreglo matemático único, comparable con una contraseña de 60 dígitos. Este arreglo único, es encriptado y almacenado, es importante notar que solo es almacenado este arreglo matemático o **template** basado en las minucias extraídas de la huella y no la imagen capturada. La próxima vez que se capture una huella por el sensor, se creará un nuevo **template** el cual será comparado con el almacenado en la base de datos para verificar la identidad del usuario.

3.8.7 CALIDAD DE IMAGEN DE LA HUELLA DACTILAR.

La calidad la huella digital es relativa al número de puntos de minucias capturados. Si el número y la posición de las minucias permanecen constantes cuando una huella de un individuo ha sido escaneada y capturada, esta imagen realiza una comparación exitosa con el template o arreglo matemático existente en la base de datos. La imagen de la huella que no posee un adecuado número de puntos de minucias puede llegar a ser inutilizable para su almacenamiento y autenticación, es por este motivo que reviste de gran importancia el proceso de enrolamiento, en el que se debe realizar una captura de la imagen de una muy buena calidad para que se puedan extraer de mejor forma la minucias y creación de **template**. En la figura se muestra una baja calidad de huella, caracterizada por manchas, decoloramiento, u otras distorsiones del área de la huella. Estas condiciones pueden ser causadas por una excesiva sequedad, humedad o marcas de cicatriz en la piel de la yema del dedo.

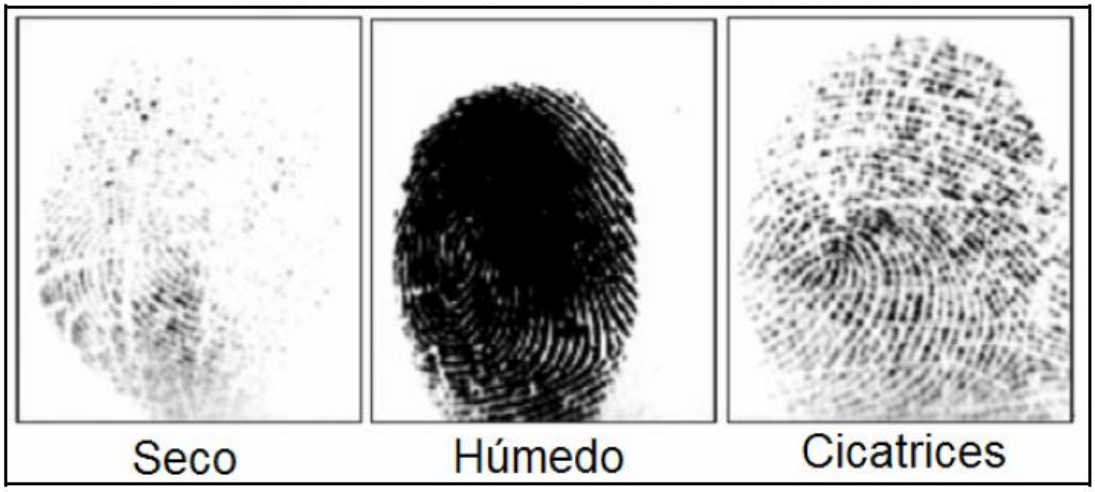


FIGURA 3. 19 Muestras de huellas con baja calidad

El algoritmo que realiza la comparación de la huella digital es capaz de extraer las minucias correctas incluso sin las ventajas de una impresión perfecta. Sin embargo, la posición del dedo o la relativa humedad o sequedad de la huella cuando es colocada sobre la ventana óptica del sensor, son dos factores importantes a la hora de realizar el reconocimiento de la identidad de un individuo.

3.8.7.1 Corrigiendo la imagen de la huella digital

Cuando la temperatura es baja, o luego de lavarse las manos, la huella está a menudo seca. En estos casos, el usuario puede humedecer sus dedos o simplemente respirando en ellos antes de colocarlo sobre el sensor. Si la huella se encuentra muy húmeda, la crestas y valles se vuelven indistinguibles. La carencia de datos, en cuanto a minucias, causan que las huellas dactilares húmedas sean rechazadas por el sistema al no poder reconocerlas. Para poder solucionar esta situación basta con secarse los dedos con una toalla limpia o con la propia ropa.

3.8.7.2 Posición de la huella dactilar

Para capturar la mayoría de las minucias se debe maximizar el área de exposición de la huella dactilar sobre el propio sensor óptico. La figura muestra el correcto posicionamiento de la huella dactilar sobre el sensor óptico, el cual contrasta con la siguiente figura que muestra los errores más comunes durante el período de enrolamiento.

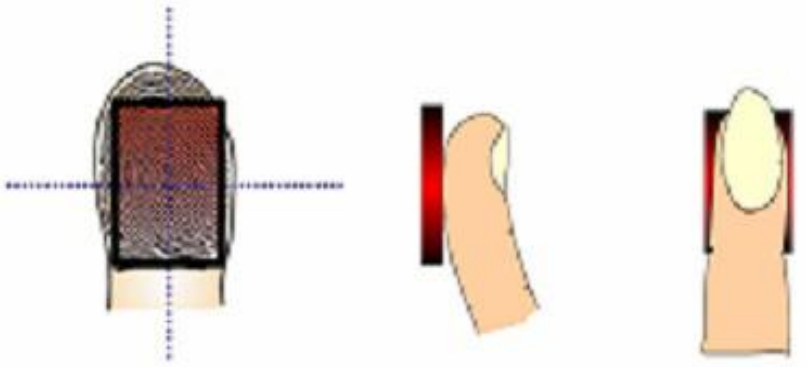


FIGURA 3. 20 Correcto posicionamiento del dedo sobre el lector biométrico

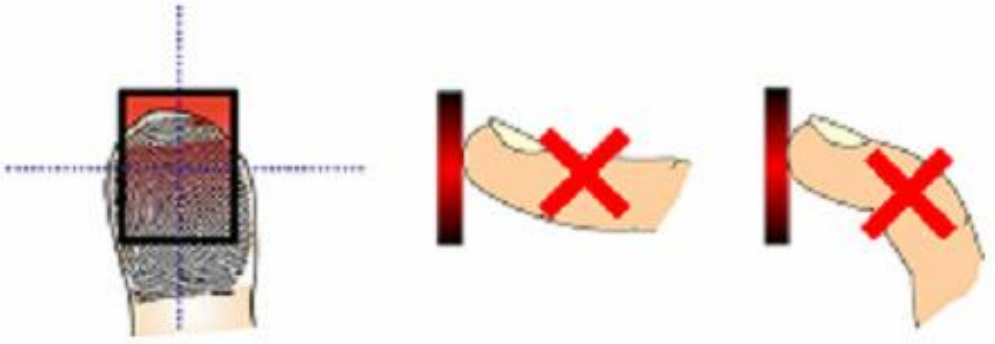


FIGURA 3. 21 Errores comunes

3.8.7.3 Angulo permitido para la rotación del dedo.

El sistema permite que el algoritmo pueda reconocer a un individuo que ha colocado la huella dactilar a 45º de rotación como máximo, tal como lo indica la figura.

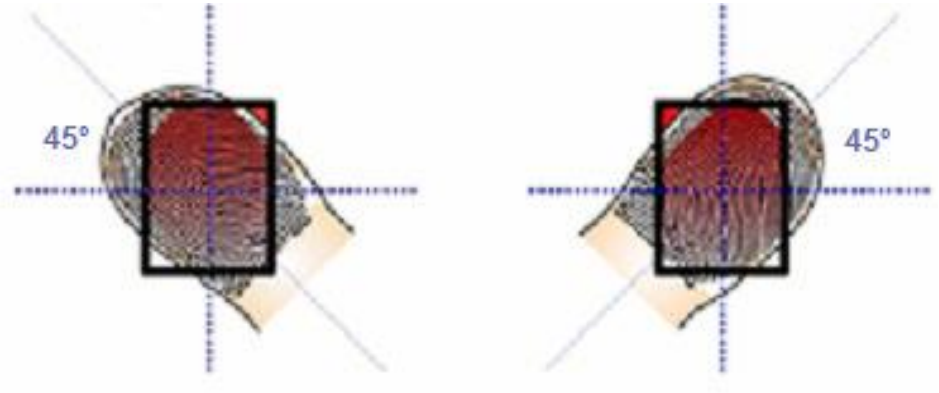


FIGURA 3. 22 ROTACIÓN PERMITIDA

3.8.7.4 Nivel de presión necesaria para obtener una buena calidad de huella dactilar

Si es demasiada la presión aplicada sobre el sensor, las crestas se juntan unas con otras y se hacen indistinguibles. En este caso, el efecto causado por este factor es similar a la dificultad de encontrar las minucias de una imagen de huella digital húmeda.

Por otra parte, si es poca la presión aplicada sobre el sensor el resultado de la imagen es similar al de una huella digital con piel seca.

3.8.7.5 Ajustar valores de exposición.

Ejemplos de exposición de imagen

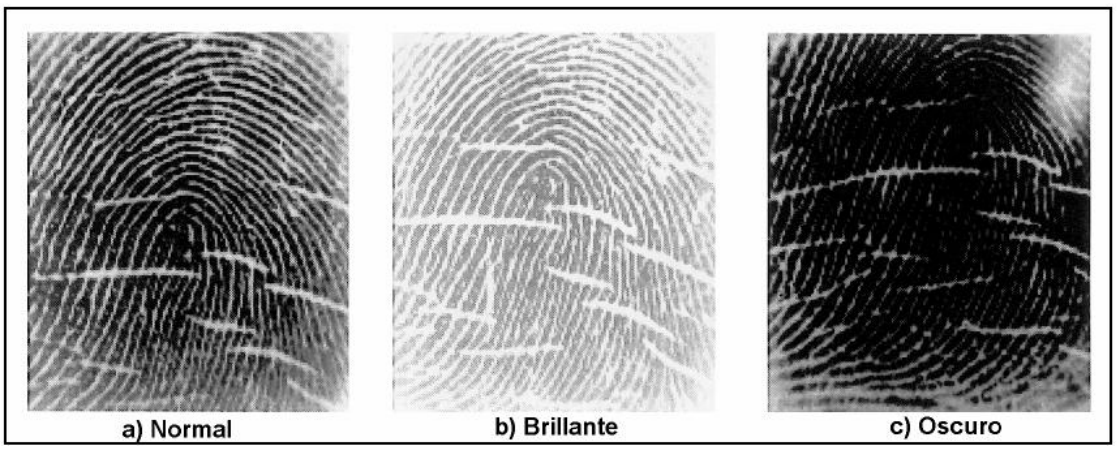


FIGURA 3. 23 EXPOSICIÓN DE LA IMAGEN

El FIM2030 captura las imágenes de la huella dactilar como se muestran en las imágenes anteriores. Estos valores pueden ser ajustados manualmente o usando el auto ajuste.

La imagen (a) de la figura es una buena imagen capturada, el claro contraste entre crestas y valles hacen que la extracción de la información de la huella dactilar sea confiable.

La imagen (b) tiene un poco más de brillo que la imagen (a), este ajuste es similar al de una huella digital con piel seca.

La imagen (c) es más oscura que la imagen (a), este nivel de exposición es similar al de una huella dactilar húmeda, lo cual produce información insuficiente de la minucia para una extracción confiable.

En cuanto al desarrollo del equipo se debe establecer una calidad óptima de la imagen a extraer, es por esta razón que es de gran importancia conocer y establecer los valores adecuados de ajuste para la extracción de imágenes.

Antiguos módulos ópticos utilizan prismas de tipo translúcidos, a diferencia de los nuevos módulos que usan prismas de tipo transparente. Esta diferencia radica en que todos los lados del prisma del tipo transparente, son cortados para crear superficies transparentes y suaves, duplicando la ganancia (amplitud de la señal). Los viejos modelos de prismas translúcidos consisten en sólo dos cortes en la superficie, con uno de los lados relativamente áspero, tiene un aspecto opaco si se observan por la ventana del sensor.

CAPITULO IV

OTROS DISPOSITIVOS RELACIONADOS AL DESARROLLO

4.1 MICROCONTROLADOR PIC 16F877A

Se denomina microcontrolador a un dispositivo programable capaz de realizar diferentes actividades que requieran del procesamiento de datos digitales y del control y comunicación digital de diferentes dispositivos.

Los microcontroladores poseen una memoria interna que almacena dos tipos de datos; las instrucciones, que corresponden al programa que se ejecuta, y los registros, es decir, los datos que el usuario maneja, así como registros especiales para el control de las diferentes funciones del microcontrolador.

Los microcontroladores se programan en Assembler y cada microcontrolador varía su conjunto de instrucciones de acuerdo a su fabricante y modelo. De acuerdo al número de instrucciones que el microcontrolador maneja se le denomina de arquitectura RISC (reducido) o CISC (complejo).

Los microcontroladores poseen principalmente una ALU (Unidad Lógico Aritmética), memoria del programa, memoria de registros, y pines I/O (entrada y/o salida). La ALU es la encargada de procesar los datos dependiendo de las instrucciones que se ejecuten (ADD, OR, AND), mientras que los pines son los que se encargan de comunicar al microcontrolador con el medio externo; la función de los pines puede ser de transmisión de datos, alimentación de corriente para el funcionamiento de este o pines de control especifico.

En este proyecto se utilizo el PIC16F877. Este microcontrolador es fabricado por MicroChip familia a la cual se le denomina PIC. El modelo 16F877 posee varias características que hacen a este microcontrolador un dispositivo muy versátil,

eficiente y práctico para ser empleado en la aplicación que posteriormente será detallada. [32]

Algunas de estas características se muestran a continuación:

- Soporta modo de comunicación serial, posee dos pines para ello.
- Amplia memoria para datos y programa.
- Memoria reprogramable: La memoria en este PIC es la que se denomina FLASH; este tipo de memoria se puede borrar electrónicamente (esto corresponde a la “F” en el modelo).
- Set de instrucciones, reducido (tipo RISC), pero con las instrucciones necesarias para facilitar su manejo.

FIGURA 4. 1 PIC 16F877a

4.1.1 LA FAMILIA DEL PIC16F877

El microcontrolador PIC16F877 de Microchip pertenece a una gran familia de microcontroladores de 8 bits (bus de datos) que tienen las siguientes características generales que los distinguen de otras familias:

- Arquitectura Harvard
- Tecnología RISC
- Tecnología CMOS

Estas características se conjugan para lograr un dispositivo altamente eficiente en

[32] lc.fie.umich.mx/~jrincon/apuntes%20intro%20PIC.pdf

el uso de la memoria de datos y programa y por lo tanto en la velocidad de ejecución. Microchip ha dividido sus microcontroladores en tres grandes subfamilias de acuerdo al número de bits de su bus de instrucciones:

TABLA 4. 1 **FAMILIA DEL PIC 16F877A**

Subfamilia	instrucciones	nomenclatura
Base - Line	33 instrucciones de12 bits	PIC12XXX y PIC14XXX
Mid – Range	35 instrucciones de 14 bits	PIC16XXX
High - End	58 instrucciones de 16 bits	PIC17XXX y PIC18XXX

4.1.2 CARACTERÍSTICAS GENERALES DEL PIC16F877

En siguiente tabla de pueden observar las características más relevantes del dispositivo:[33]

TABLA 4. 2 CARACTERÍSTICAS DEL PIC 16F877A

CARACTERÍSTICAS	16F877
Frecuencia máxima	DX-20MHz
Memoria de programa flash palabra de 14 bits	8KB
Posiciones RAM de datos	368
Posiciones EEPROM de datos	256
Puertos E/S	A, B, C, D, E
Número de pines	40
Interrupciones	14
Timers	3
Módulos CCP	2
Comunicaciones Serie	MSSP, USART
Comunicaciones paralelo	PSP
Líneas de entrada de CAD de 10 bits	8
Juego de instrucciones	35 Instrucciones
Longitud de la instrucción	14 bits
Arquitectura	Harvard
CPU	RISC
Canales Pwm	2

[33] http://www.monografias.com/trabajos18/descripcion-pic/descripcion-pic.shtml

La siguiente es una lista de las características que comparte el PIC16F877 con los dispositivos más cercanos de su familia:

PIC16F873	PIC16F874	PIC16F876	PIC16F877

CPU:

- Tecnología RISC

- Sólo 35 instrucciones que aprender

- Todas las instrucciones se ejecutan en un ciclo de reloj, excepto los saltos que requieren dos

- Frecuencia de operación de 0 a 20 MHz (200 nseg de ciclo de instrucción)

- Opciones de selección del oscilador

Memoria:

- Hasta 8k x 14 bits de memoria Flash de programa

- Hasta 368 bytes de memoria de datos (RAM)

- Hasta 256 bytes de memoria de datos EEPROM

- Lectura/escritura de la CPU a la memoria flash de programa

- Protección programable de código

- Stack de hardware de 8 niveles

Reset e interrupciones:

- Hasta 14 fuentes de interrupción

- Reset de encendido (POR)

- Timer de encendido (PWRT)

- Timer de arranque del oscilador (OST)

- Sistema de vigilancia Watchdog Timer.

Otros:

- Modo SLEEP de bajo consumo de energía

- Programación y depuración serie “In-Circuit” (ICSP) a través de dos patitas

- Rango de voltaje de operación de 2.0 a 5.5 volts

- Alta disipación de corriente de la fuente: 25mA

- Rangos de temperatura: Comercial, Industrial y Extendido

- Bajo consumo de potencia:

  - Menos de 0.6mA a 3V, 4 MHz
  - 20 µA a 3V, 32 KHz
  - menos de 1µA corriente de stand-by (modo SLEEP).

TABLA 4. 3 PERIFÉRICOS

Periférico	PIC16F873 PIC16F876	PIC16F874 PIC16F877	Características
3 a 5 Puertos paralelos	PortA,B,C	PortA, B,C,D,E	con líneas digitales programables individualmente
3 Timers	Timer0	Timer0	Contador/Temporizador de 8 bits con pre-escalador de 8 bits
	Timer1	Timer1	Contador/Temporizador de 16 bits con pre-escalador
	Timer2	Timer2	Contador/Temporizador de 8 bits con pre-escalador y post-escalador de 8 bits y registro de periodo
2 módulos CCP	Captura	Captura	16 bits, 1.5 nseg de resolución máxima
	Comparación	Comparación	16 bits, 200 nseg de resolución máxima
	PWM	PWM	10 bits
1 Convertidor A/D	AN0,...,AN4	AN0,...,AN7	de 10 bits, hasta 8 canales
Puertos Serie	SSP	SSP	Puerto Serie Síncrono
	USART/SCI	USART/SCI	Puerto Serie Universal
	ICSP	ICSP	Puerto serie para programación y depuración “in circuit”
Puerto Paralelo Esclavo	PSP	PSP	Puerto de 8 bits con líneas de protocolo

4.1.3 DESCRIPCIÓN DE LA CPU

La CPU es la responsable de la interpretación y ejecución de la información

(instrucciones) guardada en la memoria de programa. Muchas de estas instrucciones operan sobre la memoria de datos. Para operar sobre la memoria de datos además, si se van a realizar operaciones lógicas o aritméticas, requieren usar la Unidad de Lógica y Aritmética (ALU). La ALU controla los bits de estado (Registro STATUS), los bits de este registro se alteran dependiendo del resultado de algunas instrucciones.

Ciclo de instrucción

El registro Program Counter (PC) es gobernado por el ciclo de instrucción como se muestra en la siguiente figura. Cada ciclo de instrucción la CPU lee (ciclo Fetch) la instrucción guardada en la memoria de programa apuntada por PC y al mismo tiempo ejecuta la instrucción anterior, esto debido a una ***cola de instrucciones*** que le permite ejecutar una instrucción mientras lee la próxima:

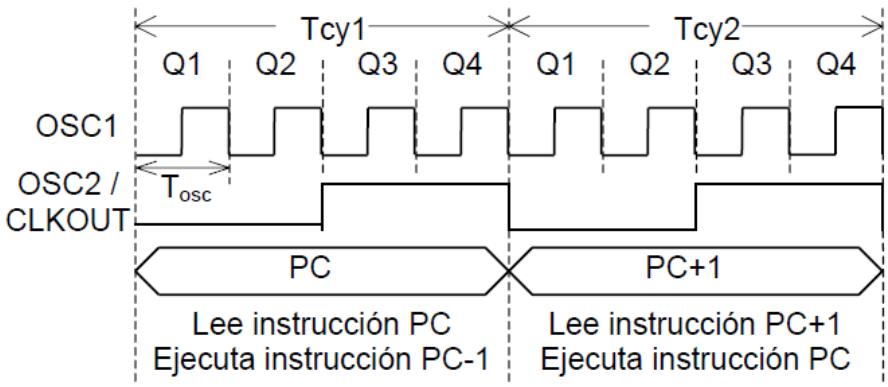


FIGURA 4. 2 Ciclo de instrucción

Como puede verse, cada ciclo de instrucción (Tcy = 4Tosc) se compone a su vez de cuatro ciclos del oscilador (Tosc= 1/Fosc)). Cada ciclo Q provee la sincronización para los siguientes eventos:

Q1: Decodificación de la instrucción

Q2: Lectura del dato (si lo hay)

Q3: Procesa el dato

Q4: Escribe el dato

Debido a esto cada ciclo de instrucción consume 4 ciclos de reloj, de manera que si la frecuencia de oscilación es Fosc, Tcy será 4/Fosc.

4.1.4 ORGANIZACIÓN DE LA MEMORIA DEL PIC

Los PIC tienen dos tipos de memoria: Memoria de Datos y Memoria de programa, cada bloque con su propio bus: Bus de datos y Bus de programa; por lo cual cada bloque puede ser accesado durante un mismo ciclo de oscilación.

La Memoria de datos a su vez se divide en:

- Memoria RAM de propósito general

- Archivo de Registros (Special Function Registers (SFR))

4.1.4.1 La Memoria de Programa

Los PIC de rango medio poseen un registro Contador del Programa (PC) de 13 bits, capaz de direccionar un espacio de 8K x 14, como todas las instrucciones son de 14 bits, esto significa un bloque de 8k instrucciones. El bloque total de 8K x 14 de memoria de programa está subdividido en 4 páginas de 2K x 14.

4.1.4.2. La Memoria de Datos

La memoria de datos consta de dos áreas mezcladas y destinadas a funciones distintas:

· Registros de Propósito Especial (SFR)

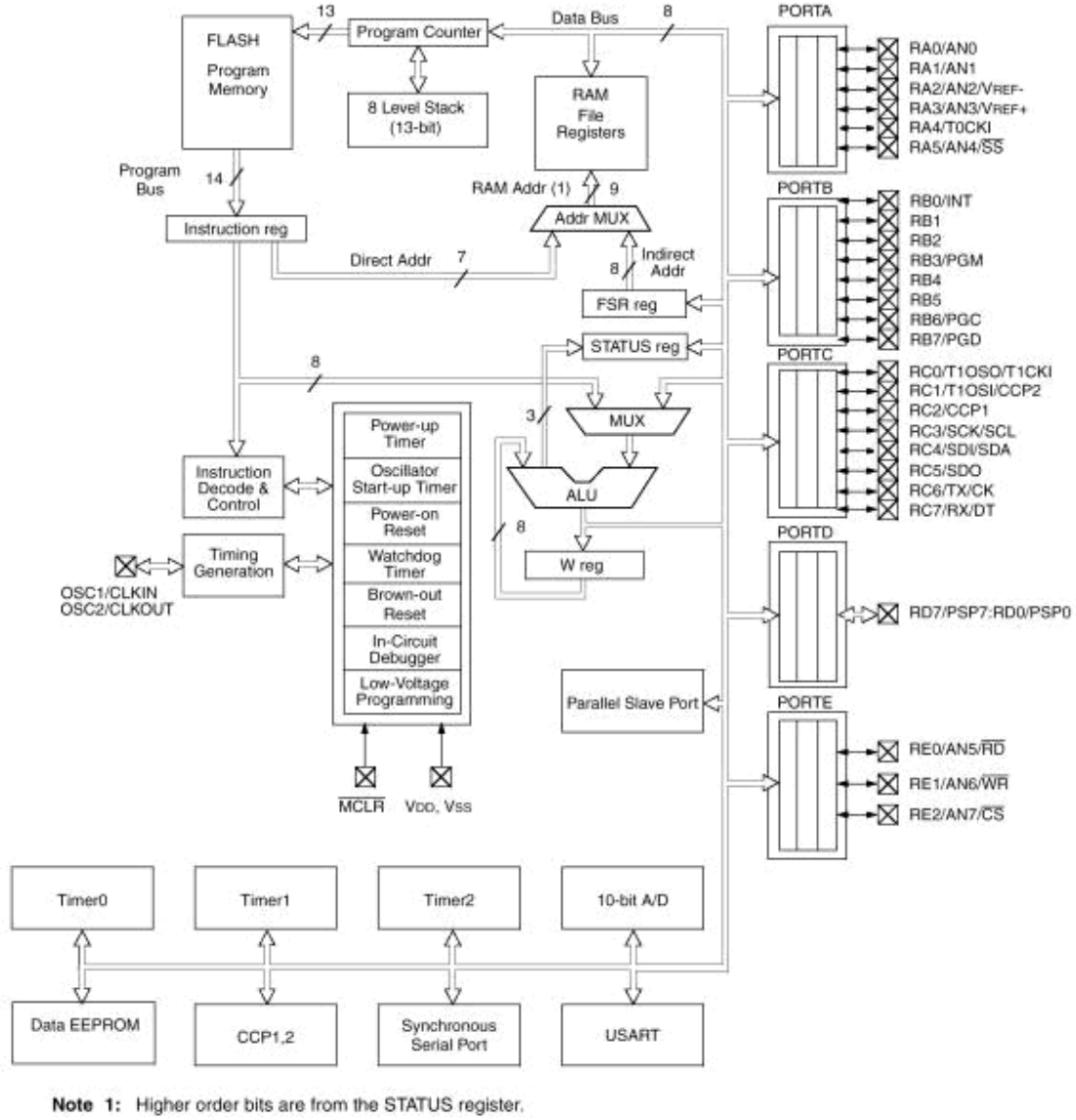
· Registro de Propósito General (GPR)

Los SFR son localidades asociadas específicamente a los diferentes periféricos y funciones de configuración del PIC y tienen un nombre específico asociado con su función. Mientras que los GPR son memoria RAM de uso general.

4.1.4.3. Diagrama de Bloques del PIC16F877[34]

En la siguiente figura se muestra a manera de bloques la organización interna del PIC16F877, Se muestra también junto a este diagrama su diagrama de patitas, para tener una visión conjunta del interior y exterior del Chip.

Device	Program FLASH	Data Memory	Data EEPROM
PIC16F874	4K	192 Bytes	128 Bytes
PIC16F877	8K	368 Bytes	256 Bytes



Note 1: Higher order bits are from the STATUS register.

FIGURA 4. 3 DIAGRAMA DE BLOQUES[35]

[34] http://www.monografias.com/trabajos18/descripcion-pic/descripcion-pic.shtml
[35] MicroChip PIC 16F877a Datasheet

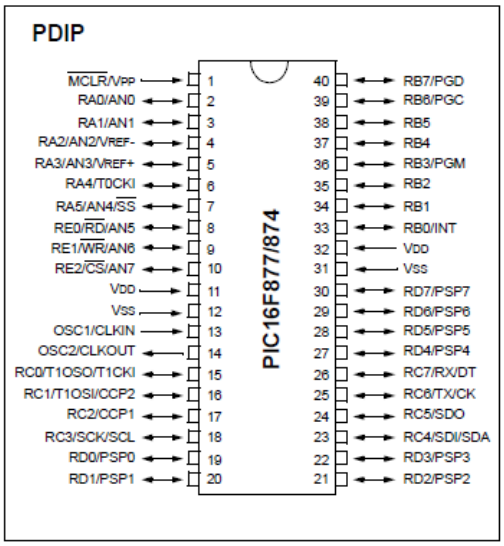


FIGURA 4. 4 DISTRIBUCIÓN DE PINES

TABLA 4. 4 DESCRIPCIÓN DE PINES DEL PIC16F877a[36]

NOMBRE DEL PIN	PIN	TIPO	TIPO DE BUFFER	DESCRIPCIÓN
OSC1/CLKIN	13	I	ST/MOS	Entrada del oscilador de cristal / Entrada de señal de reloj externa
OSC2/CLKOUT	14	O	-	Salida del oscilador de cristal
MCLR/Vpp/THV	1	I/P	ST	Entrada del Master clear (Reset) o entrada de voltaje de programación o modo de control high voltaje test
RA0/AN0 RA1/AN1 RA2/AN2/ Vref- RA3/AN3/Vref+ RA4/T0CKI RA5/SS/AN4	2 3 4 5 6 7	I/O I/O I/O I/O I/O I/O	TTL TTL TTL TTL ST TTL	PORTA es un puerto I/O bidireccional RAO: puede ser salida analógica 0 RA1: puede ser salida analógica 1 RA2: puede ser salida analógica 2 o referencia negativa de voltaje RA3: puede ser salida analógica 3 o referencia positiva de voltaje RA4: puede ser entrada de reloj el timer0. RA5: puede ser salida analógica 4 o el esclavo seleccionado por el puerto serial síncrono.

[36] http://www.monografias.com/trabajos18/descripcion-pic/descripcion-pic.shtml

RBO/INT RB1 RB2 RB3/PGM RB4 RB5 RB6/PGC RB7/PGD	33 34 35 36 37 38 39 40	I/O I/O I/O I/O I/O I/O I/O I/O	TTL/ST TTL TTL TTL TTL TTL TTL/ST TTL/ST	PORTB es un puerto I/O bidireccional. Puede ser programado todo como entradas RB0 puede ser pin de interrupción externo. RB3: puede ser la entada de programación de bajo voltaje Pin de interrupción Pin de interrupción Pin de interrupción. Reloj de programación serial
RCO/T1OSO/T1CKI RC1/T1OS1/CCP2 RC2/CCP1 RC3/SCK/SCL RC4/SD1/SDA RC5/SD0 RC6/Tx/CK RC7/RX/DT	15 16 17 18 23 24 25 26	I/O I/O I/O I/O I/O I/O I/O I/O	ST ST ST ST ST ST ST ST	PORTC es un puerto I/O bidireccional RCO puede ser la salida del oscilador timer1 o la entrada de reloj del timer1 RC1 puede ser la entrada del oscilador timer1 o salida PWM 2 RC2 puede ser una entrada de captura y comparación o salida PWM RC3 puede ser la entrada o salida serial de reloj síncrono para modos SPI e I2C RC4 puede ser la entrada de datos SPI y modo I2C RC5 puede ser la salida de datos SPI RC6 puede ser el transmisor asíncrono USART o el reloj síncrono. RC7 puede ser el receptor asíncrono USART o datos síncronos
RD0/PSP0 RD1/PSP1 RD2/PSP2 RD3/PSP3 RD4/PSP4 RD5/PSP5 RD6/PSP6 RD7/PSP7	19 20 21 22 27 28 29 30	I/O I/O I/O I/O I/O I/O I/O I/O	ST/TTL ST/TTL ST/TTL ST/TTL ST/TTL ST/TTL ST/TTL ST/TTL	PORTD es un puerto bidireccional paralelo
REO/RD/AN5 RE1/WR/AN RE2/CS/AN7	8 9 10	I/O I/O I/O	ST/TTL ST/TTL ST/TTL	PORTE es un puerto I/O bidireccional REO: puede ser control de lectura para el puerto esclavo paralelo o entrada analógica 5 RE1: puede ser escritura de control para el puerto paralelo esclavo o entrada analógica 6 RE2: puede ser el selector de control para el puerto paralelo esclavo o la entrada analógica 7.
Vss	12.31	P	-	Referencia de tierra para los pines lógicos y de I/O
Vdd	11.32	P	-	Fuente positiva para los pines lógicos y de I/O
NC	-	-	-	No está conectado internamente

4.1.5 OSCILADOR[37]

Los PIC de rango medio permiten hasta 8 diferentes modos para el oscilador. El usuario puede seleccionar alguno de estos 8 modos programando 2 bits de configuración del dispositivo denominados: FOSC1 y FOSC0, ubicados en un registro especial de configuración en la localidad 2007H de la memoria de programa:

Configuration word (2007H):

13	12	11	10	9	8	7	6	5	4	3	2	1	0
CP1	CP0	DEBUG	-	WRT	CPD	LVP	BODEN	CP1	CP0	$\overline{\text{PWRTE}}$	WDTE	**FOSC1**	**FOSC0**

En algunos de estos modos el usuario puede indicar que se genere o no una salida del oscilador (CLKOUT) a través de una patita de Entrada/Salida. Los modos de operación se muestran en la siguiente lista:

TABLA 4. 5 DESIGNACIÓN DEL OSCILADOR

FOSC1	FOSC0	Modo de operación del oscilador	
0	0	LP	Baja frecuencia (y bajo consumo de potencia)
0	1	XT	Cristal / Resonador cerámico externos, (Media frecuencia)
1	0	HS	Alta velocidad (y alta potencia) Cristal/resonador
1	1	RC	Resistencia / capacitor externos

- **Nota**: Algunos PIC's poseen un modo de oscilación que les permite usar una resistencia y un capacitor interno calibrados para 4 MHz

Los tres modos LP, XT y HS usan un cristal o resonador externo, la diferencia sin embargo es la ganancia de los drivers internos, lo cual se ve reflejado en el rango de frecuencia admitido y la potencia consumida. En la siguiente tabla se muestran los rangos de frecuencia así como los capacitores recomendados para un oscilador en base a cristal.

[37] http://lc.fie.umich.mx/~jrincon/apuntes%20intro%20PIC.pdf

TABLA 4. 6 CAPACITORES RECOMENDADOS SEGÚN LA FRECUENCIA DEL OSCILADOR[38]

Modo	Frecuencia típica	Capacitores recomendados	
		C1	C2
LP	32 khz 200 khz	68 a 100 pf 15 a 30 pf	68 a 100 pf 15 a 30 pf
XT	100 khz 2 Mhz 4 Mhz	68 a 150 pf 15 a 30 pf 15 a 30 pf	150 a 200 pf 15 a 30 pf 15 a 30 pf
HS	8 Mhz 10 Mhz 20 Mhz	15 a 30 pf 15 a 30 pf 15 a 30 pf	15 a 30 pf 15 a 30 pf 15 a 30 pf

Cristal externo: En los tres modos mostrados en la tabla anterior se puede usar un cristal o resonador cerámico externo. En la siguiente figura se muestra la conexión de un cristal a las patitas OSC1 y OS2 del PIC.

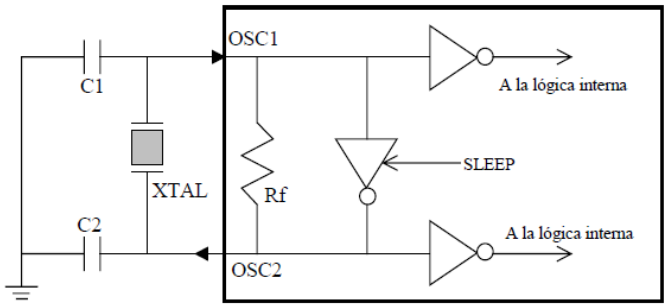


FIGURA 4. 5 Cristal externo

Circuito RC externo: En los modos RC y EXTRC el PIC puede generar su señal oscilatoria basada en un arreglo RC externo conectado a la patita OSC1 como se muestra en la siguiente figura:

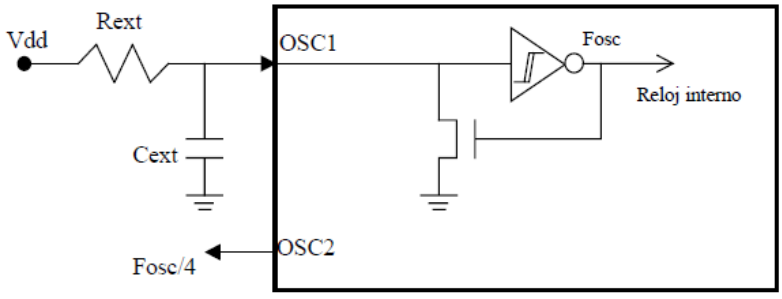


FIGURA 4. 6 Circuito RC externo

[38] http://lc.fie.umich.mx/~jrincon/apuntes%20intro%20PIC.pdf

Este modo sólo se recomienda cuando la aplicación no requiera una gran precisión en la medición de tiempos.

Rangos.- La frecuencia de oscilación depende no sólo de los valores de Rext y Cext, sino también del voltaje de la fuente Vdd. Los rangos admisibles para resistencia y capacitor son:

Rext: de 3 a 100 Kohm

Cext: mayor de 20 pf

Oscilador externo.- También es posible conectar una señal de reloj generada mediante un oscilador externo a la patita OSC1 del PIC. Para ello el PIC deberá estar en uno de los tres modos que admiten cristal (LP, XT o HS). La conexión se muestra en la siguiente figura:

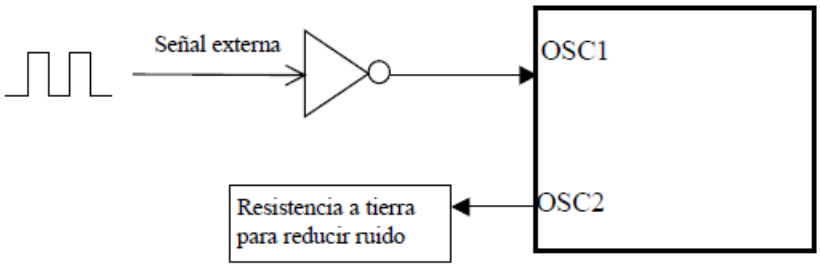


FIGURA 4. 7 Oscilador externo

Oscilador interno de 4Mhz.- En los PIC's que poseen este modo de oscilación, (modo INTRC) el PIC usa un arreglo RC interno que genera una frecuencia de 4 MHz con un rango de error calibrable de ± 1.5%. Para calibrar el error de oscilación se usan los bits CAL3, CAL2, CAL1 Y CAL0 del registro OSCCAL.

Calibración del oscilador interno.- El fabricante ha colocado un valor de calibración para estos bits en la última dirección de la memoria de programa. Este dato ha sido guardado en la forma de una instrucción RETLW XX. Si no se quiere perder este valor al borrar el PIC (en versiones EPROM con ventana) primero se deberá leer y copiar. Es una buena idea escribirlo en el empaquetado antes de borrar la memoria).

4.2 VISOR

Una de las características del dispositivo, que tiene que ver con un requerimiento indispensable para el desarrollo y uso del dispositivo, se trata del display o visor que sirve de interfaz, que permitirá comunicar al usuario la transacción realizada.

Se ha resuelto utilizar un visor de dos líneas con capacidad de 16 caracteres cada una, permitiendo desplegar la información necesaria para este sistema de identificación.

4.2.1 CARACTERÍSTICAS FÍSICAS [39]

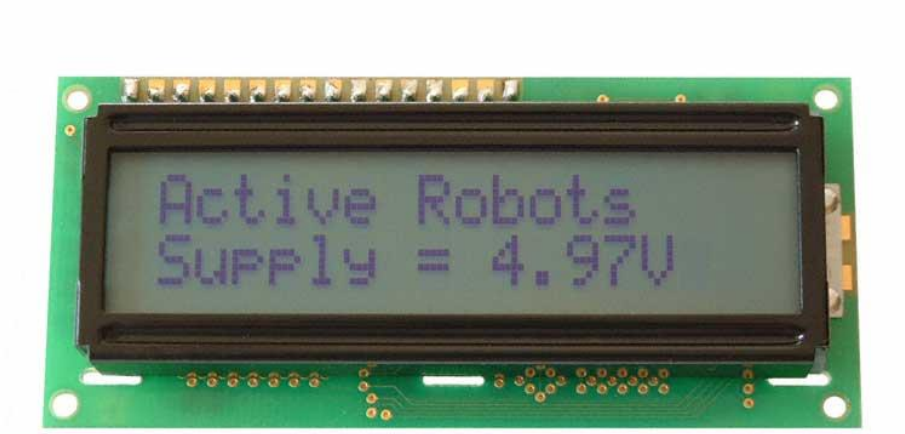


FIGURA 4. 8 Visor

[39] www.datasheetcatalog.org/datasheet/vishay/016m002b.pdf

TABLA 4. 7 DISTRIBUCIÓN DE PINES DEL LCD

PIN NUMBER	SYMBOL	FUNCTION
1	Vss	GND
2	Vdd	+ 3V or + 5V
3	Vo	Contrast Adjustment
4	RS	H/L Register Select Signal
5	R/$\overline{W}$	H/L Read/Write Signal
6	E	H →L Enable Signal
7	DB0	H/L Data Bus Line
8	DB1	H/L Data Bus Line
9	DB2	H/L Data Bus Line
10	DB3	H/L Data Bus Line
11	DB4	H/L Data Bus Line
12	DB5	H/L Data Bus Line
13	DB6	H/L Data Bus Line
14	DB7	H/L Data Bus Line
15	A/Vee	+ 4.2V for LED/Negative Voltage Output
16	K	Power Supply for B/L (OV)

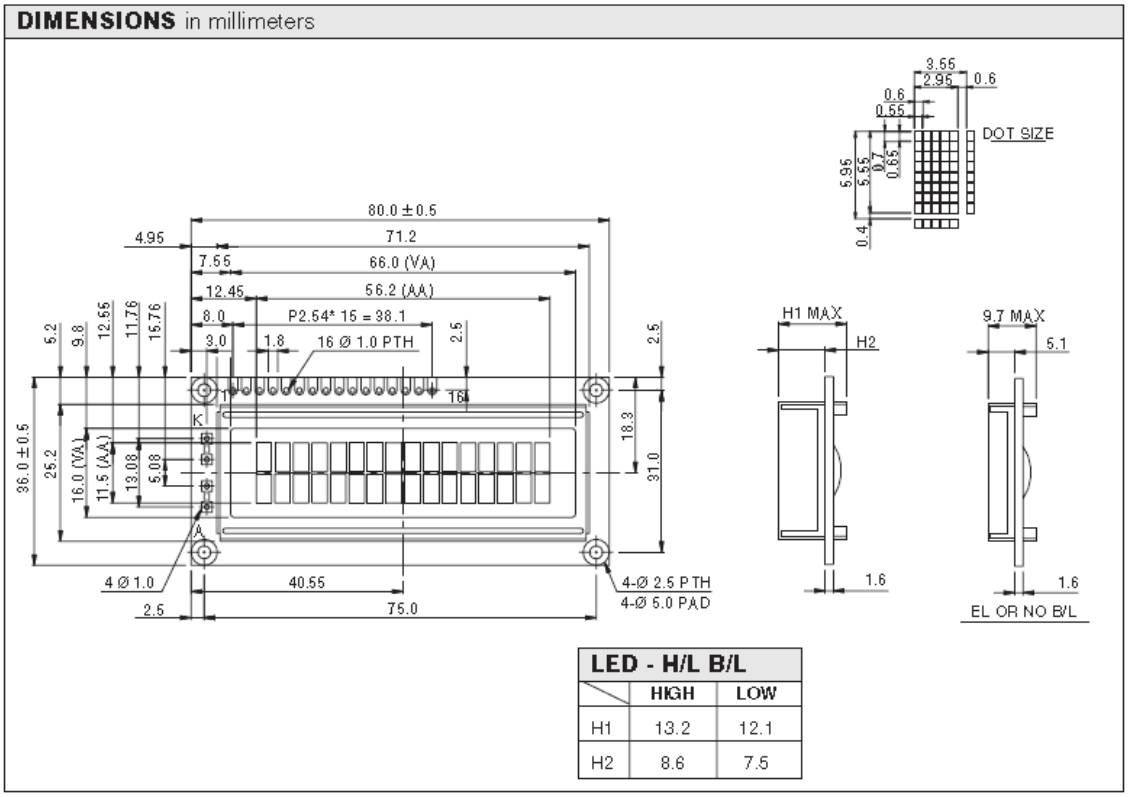


FIGURA 4. 9 Dimensiones del LCD

4.2.2 CARACTERÍSTICAS ELÉCTRICAS

Debido a la finalidad del dispositivo es necesario tener en cuenta las características eléctricas y de condición ambiental para establecer los parámetros de funcionamiento del dispositivo, para ello, es necesario describir las características propias del visor y considerar sus valores máximos y mínimos de funcionamiento.

TABLA 4. 8 CARACTERÍSTICAS ELÉCTRICAS DEL LCD DE 16X2

ELECTRICAL SPECIFICATIONS							
ITEM	SYMBOL	CONDITION		STANDARD VALUE			UNIT
				MIN.	TYP.	MAX.	
Input Voltage	VDD	VDD = + 5V		4.7	5.0	5.3	V
		VDD = + 3V		2.7	3.0	5.3	V
Supply Current	IDD	VDD = 5V		–	1.2	3.0	mA
Recommended LC Driving Voltage for Normal Temp. Version Module	VDD - V0	- 20 °C		–	–	–	V
		0°C		4.2	4.8	5.1	
		25°C		3.8	4.2	4.6	
		50°C		3.6	4.0	4.4	
		70°C		–	–	–	
LED Forward Voltage	VF	25°C		–	4.2	4.6	V
LED Forward Current	IF	25°C	Array	–	130	260	mA
			Edge	–	20	40	
EL Power Supply Current	IEL	Vel = 110VAC:400Hz		–	–	5.0	mA

CAPITULO V.

INTEGRACIÓN Y DESARROLLO

5.1 IMPLEMENTACIÓN DEL MICROCONTROLADOR

5.1.1 INTRODUCCIÓN

El desarrollo del microcontrolador es una etapa fundamental del proceso de desarrollo del equipo de identificación, proporcionará el manejo y control de todos los componentes que requiere el equipo de identificación. Su función principal, que es establecer el control y comunicación del dispositivo biométrico FIM2030, se realizará de acuerdo al protocolo establecido por el fabricante del dispositivo biométrico, ya que se debe establecer la estructura que este dispositivo requiere para su funcionamiento autónomo, es decir, cada proceso efectuado por el FIM2030 debe haber sido requerido por el microcontrolador dependiendo de la solución que se quiera brindar, ya sea por ejemplo, para el control de asistencia donde se debe ingresar un número por teclado que indique si el usuario se está registrando para su entrada o salida laboral, este indicador ingresado por un número permitirá al microcontrolador determinar y darle la instrucción al FIM2030 para que comience el proceso de obtención de la muestra de la huella dactilar para el procesamiento biométrico. De esta misma forma, el microcontrolador permitirá desplegar la información al usuario por medio del visor, permitiendo personalizar el contenido de la información de acuerdo a la solución generada por el sistema de identificación biométrico.

5.1.2 PROCESO DE IDENTIFICACIÓN

El proceso fundamental de este proyecto radica en implementar la identificación biométrica, a través de la huella dactilar, en este sentido se debe hacer funcionar el dispositivo FIM2030, implementando la configuración establecida con el microcontrolador. Para la implementación se debe dejar en claro la estructura de funcionamiento en base a las instrucciones que necesita el dispositivo biométrico FIM2030 para que pueda operar.

Teniendo en cuenta la estructura de datos con sus campos y registros, se debe

estructurar este mismo concepto pero a unos de los niveles de programación de más bajo nivel, como es el **Assembler**. Bajo este esquema, se deben interpretar cada una de las instrucciones que necesita el dispositivo FIM2030 por el microcontrolador, es decir, se debe manejar cada una de las instrucciones administrando los registros del microcontrolador y adaptar la información para que el FIM2030 pueda interpretarla.

Para entender de mejor forma los principales procesos de funcionamiento del equipo, es que se ha diseñado un diagrama de flujo que explica cual es la secuencia de tareas y pasos que el dispositivo realiza.

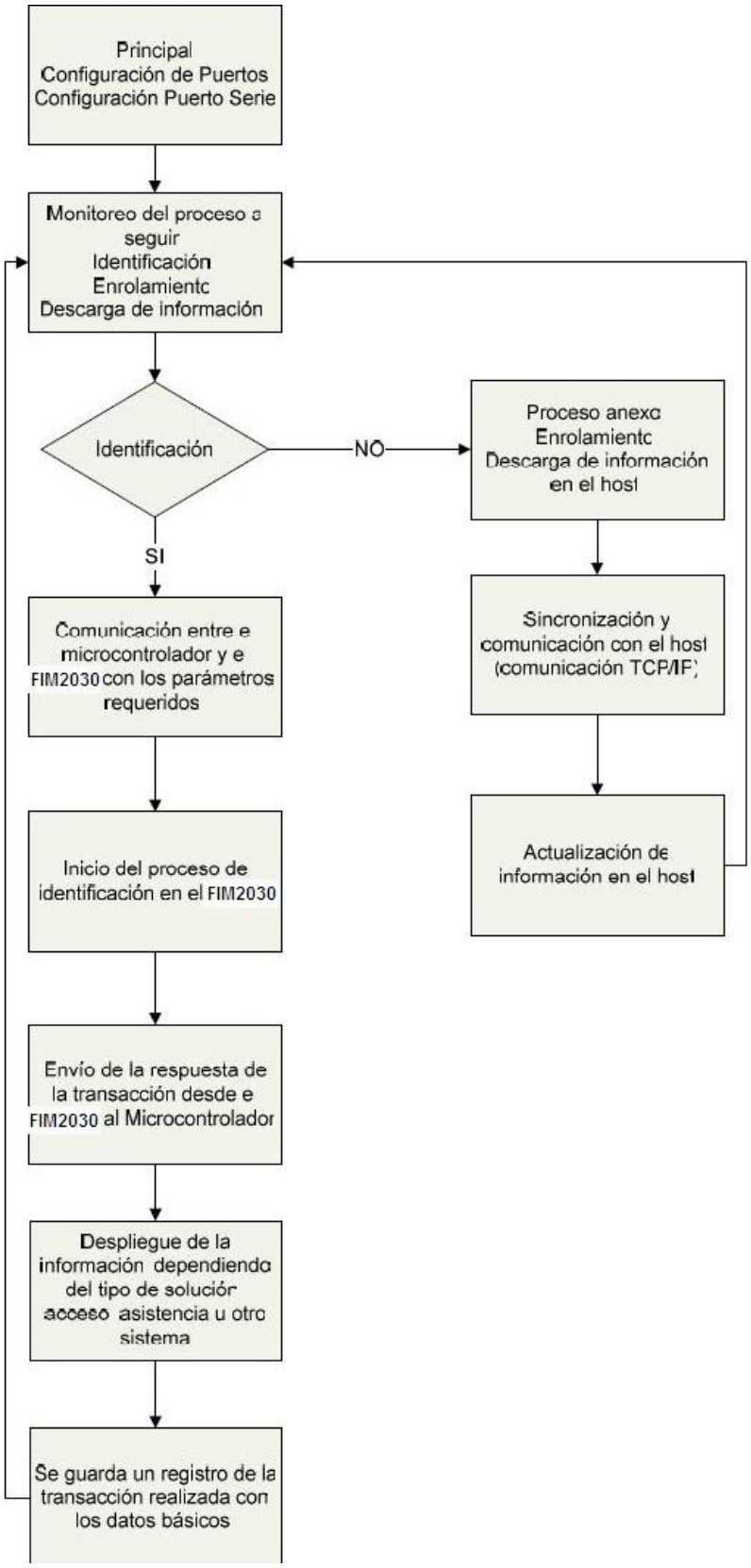


FIGURA 5. 1 Diagrama de flujo de operación del microcontrolador

Fuente: Propia. (2010)

Este diagrama se basa en el funcionamiento del microcontrolador, debido a que este, es el dispositivo principal de control de los dispositivos periféricos, entonces, desde esta perspectiva, el programa principal se inicia con la configuración de los puertos de E/S, en este caso se debe establecer que puertos serán utilizados para la comunicación de entrada y salida, por otro lado, en el puerto serie se debe configurar la velocidad de transmisión de la información y su nivel de seguridad de transmisión.

Luego de esta configuración, que se debe realizar una vez que se inicie el programa principal, se monitorea las opciones de procesos que el usuario quiera realizar con el FIM2030, es decir, que existirán como base en cada solución, las opciones principales como son la de identificación, enrolamiento y transferencia de información al **host** principal. Para cada una de estas opciones, el usuario deberá indicar por teclado, sensor o alguna instrucción, para el caso del administrador del sistema, que desee que realice el dispositivo biométrico. El programa principal estará censando cada una de las opciones a la espera de alguna petición. Debido a que la principal tarea del equipo es la identificación del usuario, el sistema pregunta si la opción deseada es la propia identificación biométrica, si es así, se inicia el proceso de comunicación del microprocesador con el FIM2030 con la instrucción de identificación, tanto en este proceso como en cualquier otro, es aquí donde el microcontrolador envía la instrucción al FIM2030 de acuerdo a la estructura de datos establecida. Una vez realizado este proceso, el FIM2030 comienza con el proceso de identificación; esto quiere decir que el dispositivo toma la instrucción, se inicializa la lectura biométrica y se toma la muestra de la huella dactilar, una vez obtenida la muestra, el propio FIM2030 procede a procesarla. Este procesamiento consiste en que bajo su propio algoritmo, el FIM2030 realiza la comparación de la huella obtenida con la almacenada en su propia base de datos. Si el dispositivo, al realizar el proceso de búsqueda, encuentra la huella, este devolverá como respuesta la identificación del individuo, enviándola directamente al microcontrolador para que pueda procesarla y enviarla a los periféricos relacionados, como son el despliegue de la información por el visor o el envío de una señal eléctrica para la apertura de una cerradura magnética o la activación de los respectivos relés que habilitaran las funciones esenciales del vehículo.

Luego del proceso de identificación, el sistema guarda un registro con la transacción realizada. Estos registros almacenarán los datos básicos del usuario registrado, para que luego esta información pueda ser descargada a un computador que sirva de administrador de la solución implementada, como es un control de asistencia o acceso centralizado.

Para el caso de que el proceso a seguir no sea el de la identificación, el programa principal contará con las opciones disponibles, indicadas como procesos anexos a la propia identificación, como son el enrolamiento o la descarga de la información al computador principal. Para estos casos será necesaria la comunicación con el host principal de manera de realizar la actualización de la información con los nuevos registros del sistema instalado, pudiendo ser el control de asistencia o acceso. Es conveniente decir que toda comunicación y sincronización entre dispositivos y el computador principal, se realiza bajo el protocolo TCP/IP.

5.2 DESARROLLO

5.2.1 CONFIGURACIÓN PUERTO SERIAL

La importancia del puerto serie radica en la comunicación que se establece entre el microcontrolador y los dispositivos externos. La comunicación se basa de acuerdo a sus parámetros de configuración, como son la velocidad de transmisión de datos, la paridad y el control de flujo de la transmisión.

Para este desarrollo, se han establecido los parámetros acordes a la comunicación que requiere el FIM2030 para obtener un buen funcionamiento. En este sentido se establecen dos parámetros fundamentales como son la velocidad de transmisión y el modo de comunicación serial del microcontrolador.

La velocidad de transmisión se ha establecido en 9600 bps y el modo de comunicación para el microcontrolador se ha establecido utilizar el modo 2, que consiste en una trama de 8 bits de datos, 1 de partida y uno de parada y un bit adicional que puede ser configurado por el usuario.

5.2.2 COMUNICACIÓN Y GENERACIÓN DE INSTRUCCIONES[40]

La comunicación entre el microcontrolador y el dispositivo FIM2030, se basa en la estructura establecida por el fabricante, en este caso se debe tener en cuenta la utilización de registros en el microcontrolador para formar la estructura de datos requerida.

De acuerdo a la estructura definida, se debe considerar la siguiente tabla para definir los registros necesarios.

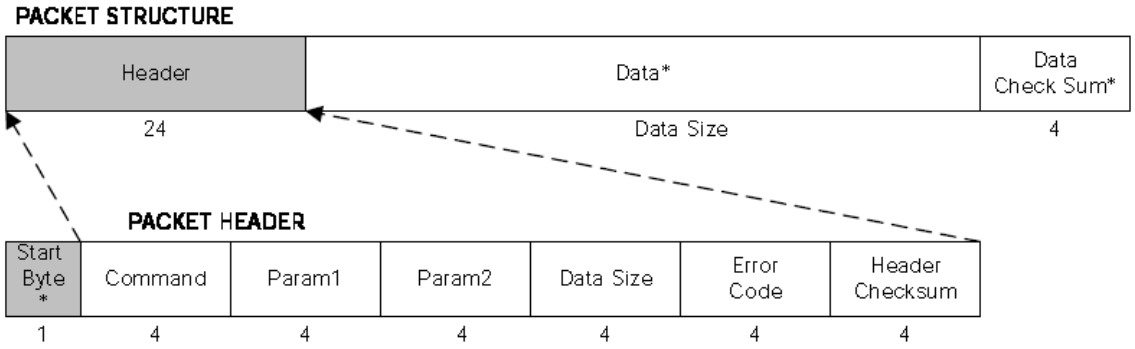


FIGURA 5. 2 Estructura del paquete de datos

En este caso, para el diseño de una solución general se ha creado un sistema de registro, que puede ser configurado para cualquiera de las soluciones definidas como objetivo para este dispositivo de identificación, como son el control de acceso, asistencia y para el control de identificación biométrica que pueda ser integrada en diferentes sistemas computacionales, principalmente.

Es decir, que la funcionalidad de la creación de instrucciones por parte del microcontrolador y su correspondiente envío al dispositivo FIM2030, no se verá afectado o cambiado de acuerdo a la finalidad del producto. En este caso, para el control de asistencia el dispositivo biométrico se activará según el comando o la opción definido en el teclado del equipo. En el control de acceso, dependerá de algún tipo de sensor o botón que active el sensor biométrico para que tome la muestra al usuario y en el caso de utilizar un computador como administrador del sistema biométrico, deberá enviar un comando de manera que el microcontrolador lo interprete y lo envíe como instrucción al dispositivo FIM2030.

[40] EN-FIM-ComProtocol-v1.75

Bajo esta noción, el desarrollo del programa del microcontrolador quedó abierto a los diferentes periféricos integrados para que puedan interactuar de una forma eficiente y eficaz con el dispositivo de identificación biométrica.

Esta sección aún corresponde al programa principal del microcontrolador, donde se encuentra monitoreando el proceso a seguir. En esta etapa, el programa se dedica a censar los periféricos que utiliza el microcontrolador. Entonces, al presionar uno de los botones del teclado el microcontrolador será capaz de capturar el dato y elaborar la instrucción de identificación para que el dispositivo biométrico FIM2030 inicie el proceso y el usuario pueda ingresar la huella dactilar para la captura de la muestra.

De acuerdo al desarrollo e implementación del dispositivo biométrico FIM2030 con el microcontrolador, se ha desarrollado el programa para el microcontrolador, el cual se explica su funcionamiento en el siguiente diagrama:

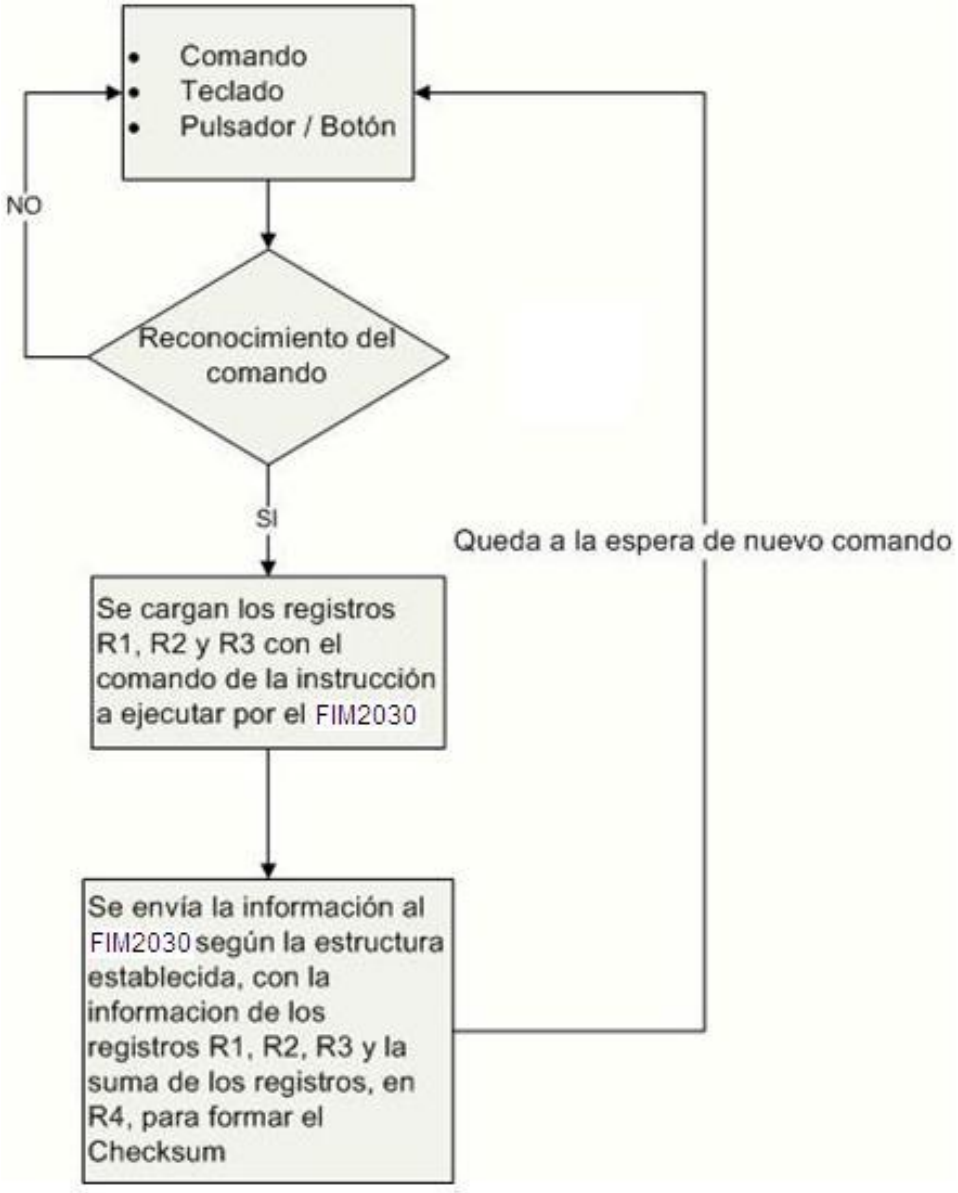


FIGURA 5. 3 Diagrama de reconocimiento del comando

Fuente Propia. (2010)

Se comienza con el ingreso del comando que el usuario quiera realizar sobre el dispositivo, este comando podrá ser ingresado de acuerdo a la configuración del equipo, pudiendo ser para control de acceso, asistencia o para un equipo administrado por un PC.

5.2.3 MODO DE USO DE LOS COMANDOS[41]

En este capítulo, se explica la estructura del bloque de datos a ser transmitido. El método de comunicación se explica con ejemplos.

5.2.4 PEDIR LA CONEXIÓN

Para verificar la conexión serial, use el comando “Request Connection”. Para la explicación de los datos reales del paquete, asuma que el dispositivo tiene 10 usuarios en DB. La siguiente figura muestra la sucesión de paquetes, y los contenidos de los paquetes.

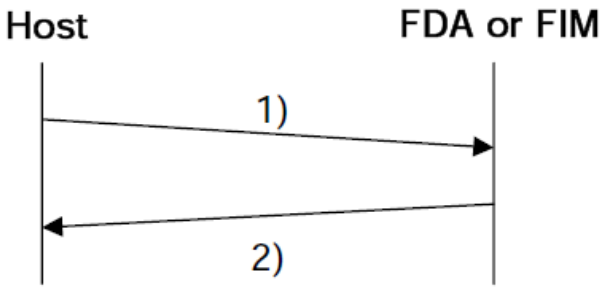


FIGURA 5. 4 Secuencia de petición de conexión

1) Estructura del paquete de comando CMD_REQUEST_CONNECTION

La siguiente la tabla muestra el paquete de comando hecho en el organizador (host).

TABLA 5. 1 PAQUETE DE COMANDO CMD_REQUEST_CONNECTION

Command	0x00000001
Param1	0x00000000
Param2	0x00000000
Data Size	0x00000000
Error Code	0x00000000
Header Checksum	0x00000001

La siguiente la tabla muestra la sucesión de datos a ser transmitidos al dispositivo.

7E	00 00 00 01	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 01

[41] EN-FIM-ComProtocol-v1.75

2) Paquete de reconocimiento

En contestación al paquete de CMD_REQUEST_CONNECTION del organizador, el dispositivo envía el paquete de reconocimiento, significando un éxito como lo siguiente.

TABLA 5. 2 PAQUETE DE RECONOCIMIENTO EXITOSO

Command	0x00000001
Param1	0x00000001
Param2	0x0000000A
Data Size	0x00000000
Error Code	0x00000000
Header Checksum	0x0000000C

Si el organizador obtiene el siguiente paquete, significa que la comunicación fue hecha con éxito.

7E	00 00 00 01	00 00 00 01	00 00 00 0A	00 00 00 00	00 00 00 00	00 00 00 0C

5.2.5 ENROLAMIENTO DEL USUARIO

Hay dos métodos para registrar al usuario. El primer método es el uso de CMD_ENTROLL_FP_STEP1 y CM_ENROLL_FP_STEP2. Y el segundo método es el uso de CMD_REGISTER_FP. El segundo sólo es soportado en FIM10, FIM01 y FIM20xx. El CMD_REGISTER_FP se recomienda porque CMD_ENROLL_FP_SETP1 y CMD_ENROLL_FP_STEP2 pueden estar obsoletos. En FIM01 y FIM20xx, CMD_REGISTER_FP_STEP1 y CMD_REGISTER_FP_STEP2 no son soportados.

Usando CMD_REGISTER_FP (Soportado en FIM10, FIM01 o series de FIM20xx)

Usando este único comando, El FIM10, FIM01 y FIM20xx soportan huella digital, contraseña, y del privilegio máster en el registro.

Precaución: Este ejemplo es para FIM10.

Enrolamiento de Usuario Normal

Asuma que un dispositivo tiene 10 usuarios en DB. La siguiente descripción explica la forma de registrar a un usuario normal con la IDENTIFICACIÓN “1234” y la contraseña “5678”.

1) Estructura del paquete de comando CMD_REGISTER_FP

La siguiente la tabla muestra el paquete de comando hecho en el organizador.

TABLA 5. 3 PAQUETE DE COMANDO CMD_REGISTER_FP

Command	0x00000033									
Param1	0x00000000									
Param2	0x00000000									
Data Size	0x0000001A									
Error Code	0x00000000									
Header Checksum	0x0000004D									
Data	0x31	0x32	0x33	0x34	0x00	0x00	0x00	0x00	0x00	0x00
	0x35	0x36	0x37	0x38	0x00	0x00	0x00	0x00	0x00	0x00
	0x00	0x00	0x00	0x00	0x00	0x00				
Data Checksum	0x000001A4									

La siguiente tabla muestra la sucesión de datos a ser transmitido al dispositivo.

7E	00 00 00 33	00 00 00 00	00 00 00 00	00 00 00 1A	00 00 00 00	00 00 00 4D

31 32 33 34 00 00 00 00 00 00 35 36 37 38 00 00 00 00 00 00 00 00 00 00 00 00	00 00 01 A4

2) Paquete de reconocimiento

En contestación al paquete de CMD_REGISTER_FP del organizador, el dispositivo envía el paquete de reconocimiento que significa un éxito. Si el organizador obtiene el siguiente paquete, significa que la comunicación fue hecha con éxito.

7E	00 00 00 33	00 00 00 01	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 34

3) Estructura del paquete de comando CMD_REGISTER_FP

Si el paquete de reconocimiento al primer CMD_REGISTER_FP ha vuelto con éxito, el organizador envía el segundo paquete de comando CMD_REGISTER_FP, como sigue.

7E	00 00 00 33	00 00 00 00	00 00 00 01	00 00 00 00	00 00 00 00	00 00 00 34

4) Paquete de reconocimiento

En contestación al paquete de CMD_REGISTER_FP del organizador, el dispositivo envía el paquete de reconocimiento siguiente, significando un éxito.

7E	00 00 00 33	00 00 00 01	00 00 00 0B	00 00 00 00	00 00 00 00	00 00 00 3F

5.3 PROGRAMA EN MICROCODE

El programa de control que se pretende grabar en el microcontrolador debe reunir características de eficiencia y eficacia, para que sirva como template para otras aplicaciones del dispositivo biométrico FIM2030. Pudiendo controlar un teclado, un visor LCD, un bip de audio a modo de alarma, realizar un control de potencia del sistema autónomo que manipulara las funciones esenciales del vehículo y principalmente el dispositivo FIM2030.

Para esto se debe configurar en el microcontrolador los protocolos de comunicación propios del Pic16F877a, que permitirán realizar el control local del dispositivo FIM2030, escribiendo la siguiente instrucción:

```
INCLUDE "modedefs.bas"          ; incluir los modos de comunicación
```

Posterior a esto se bebe definir el tamaño de bits para nuestros paquetes de comando y el tipo de oscilador que se ocupara en el ensamble del circuito:

```
DEFINE ADC_BITS 8               ; Fije número de BITS del resultado (5, 8, 10)
DEFINE ADC_CLOCK 10             ; Fije El Clock (10Mhz)
```

5.3.1 CONFIGURACIÓN PARA USO DEL LCD

En el caso del desarrollo de un reloj control, para el control de asistencia, el despliegue de información es un requisito indispensable, donde se pueda desplegar información de instrucciones de uso, la hora, fecha y la información de identificación de cada usuario. En cuanto al desarrollo, se ha establecido trabajar con el visor “ELECTROLITE QY-162A”

Entre sus principales características técnicas se encuentran:

La ventaja de este tipo de visor, consiste en su gran adaptabilidad de implementación a este tipo de desarrollos. Para la integración del visor en el microcontrolador, se debió reservar un puerto, del microcontrolador, exclusivamente para esta finalidad, ya que se deben considerar las conexiones para el bus de datos y de control.

Para comenzar con el despliegue de información por medio del visor, es necesario

crear una rutina de inicialización de la pantalla LCD con los comandos preestablecidos para modo de lectura de datos y del mismo modo, la configuración del visor y del cursor.

Así entonces, para el control del visor LCD se debe configurar los pines del microcontrolador sobre los cuales se enviaran los datos para desplegar los mensajes; debiendo escribir las siguientes sentencias:

```
DEFINE LCD_DREG PORTB       ; bit de datos del LCD empezando
DEFINE LCD_DBIT 0           ; por B.0, B.1, B.2, B.3
DEFINE LCD_RSREG PORTB      ; bit de registro del LCD conectar
DEFINE LCD_RSBIT 5          ; en el puerto B5
DEFINE LCD_EREG PORTB
DEFINE LCD_EBIT 4           ; bit de Enable conectar en el puerto B.4
```

5.3.2 MANEJO DE PUERTOS I/O Y DECLARACIÓN DE VARIABLES

En el manejo de los puertos I/O del microcontrolador pic16f877a debe especificarse la sentencia ADCON1, a través de la cual se puede digitalizar el puerto A y el puerto E para ser usados como entradas y salidas o a su vez como conversores análogo digitales.

```
adcon1=7
TRISC=%0
```

Dentro del programa es necesario declarar variables, para la utilización de formulas, sentencias de repeticiones y para censar algún puerto del microcontrolador, las cuales dependiendo de su uso deberá adquirir el tamaño **bit, byte o Word.**

5.3.3 INICIALIZACIÓN

Una vez declaradas todas las variables podemos iniciar a escribir el programa, para lo cual el primer lazo servirá únicamente para dar un aviso sonoro de que el PIC está trabajando. Si este lazo no se cumple una vez armado el circuito, es posible que el PIC no haya sido grabado correctamente. Aquí se hace uso de la sentencia **FOR** y de la primera variable (r **VAR BYTE**), la cual se designo para hacer repeticiones, quedando de la siguiente manera:

```
Inicio:
    FOR r=1 TO 2          ; dar dos pitidos para comprobar
    HIGH bip              ; que está funcionando
    PAUSE 1000
    LOW bip
    PAUSE 150
    NEXT
```

Después de inicializarse el PIC debemos inicializar el visor LCD, para lo cual mostraremos un mensaje de presentación en el cual incluirá datos como: nombre del producto y del fabricante. Generando la siguiente estructura:

```
    Presentación:
    HIGH LIGHT                ; encender el backlight
    PAUSE 500
    LCDOUT $FE, 1             ; limpia la pantalla
    LCDOUT $FE, $81, "IDENTIFICADOR"
    LCDOUT $FE, $C1, "BIOMÉTRICO A10"
    PAUSE 2000
```

5.3.4 MANEJO DE LA EEPROM

La manipulación de nuestro producto se hará bajo una contraseña de control de cuatro dígitos (1, 2, 3, 5), la cual, permitirá al usuario realizar configuraciones o ingresar a las funciones si este no tiene registrada su huella digital en la base de datos del dispositivo FIM2030, como es el caso en que el vehículo quede dispuesto en modo de servicio. Esta contraseña se guardara en la memoria EEPROM (Electrical Erasable Progamable Read Only Memory) del microcontrolador y podrá ser cambiada posteriormente por el usuario, si él lo desea. Si la nueva clave es olvidada, únicamente se podrá recuperar leyendo el microcontrolador, con ayuda del equipo programador. La estructura para grabar datos en esta memoria es la siguiente:

```
    EEPROM 0, [1, 2, 3, 5]    ; cargar la memoria EEPROM desde la posición 0 en adelante
```

Una vez cargada la memoria del microcontrolador procedemos a dar un aviso auditivo que indique que se ha reseteado el programa. Aquí se dará una secuencia de tres pitidos, durante este tiempo será sensado el teclado, y, si son presionadas dos teclas específicas (7 y C) se repetirá la secuencia de reset. Entonces la estructura queda así:

```
RESET:
        Y=0
        FOR R=1 TO 3
        HIGH bip: LOW LIGHT
        PAUSE 50
        LOW bip: HIGH LIGHT
        PAUSE 50
        HIGH A: HIGH B: LOW C: HIGH D                   ; sensar la fila C
        IF (CUATRO=0) AND (UNO=0) THEN RESET    ; corresponden a tecla 7 y c
        NEXT
```

Luego, se extraerá la contraseña grabada en la memoria EEPROM y se almacenaran en cuatro variables, usando la sentencia READ, que nos permite leer una a una las celdas de memoria del microcontrolador:

```
READ 0, SETPRIME        ; Leer el dato de la EEPROM 0 y guardar en SETPRIME
 READ 1, SETSEGUN       ; Leer el dato de la EEPROM 1 y guardar en SETSEGUN
 READ 2, SETERCER       ; Leer el dato de la EEPROM 2 y guardar en SETERCER
 READ 3, SETCUART       ; Leer el dato de la EEPROM 3 y guardar en SETCUART
```

5.3.5 CONSIDERACIONES PARA EL CONTROL DE ACCESO

El método de iniciar la identificación, de acuerdo al tipo de solución, corresponde para el control de acceso, donde se quiere acceder a las funciones esenciales del vehículo. En este caso, el usuario debe presionar algún botón, de manera que le indique al lector biométrico que se encienda para obtener la muestra biométrica. De otra forma, puede ser un sensor de corte que permita censar el acercamiento del dedo del usuario para que el lector pueda establecer automáticamente que debe iniciar el proceso de extracción de la muestra biométrica.

De cualquiera de estas dos formas, el sistema debe asociar el botón o la señal del sensor al envío de la instrucción. Es por esto que se debe programar al microcontrolador para que al momento de recibir esta información, pueda generar y enviar la instrucción correspondiente.

De acuerdo a lo anterior, se estableció usar un sensor ultrasonido para detectar el acercamiento de la mano del usuario al lector biométrico, así que, en cuanto a la generación de la instrucción, para iniciar el proceso de identificación se debe renombrar uno de los puertos del microcontrolador para recibir el dato del sensor, de

esta manera la rutina de detección de la señal queda de la siguiente forma:

```
ENTRADA:
LCDOUT $FE, 1
LCDOUT $FE, $81, "IDENTIFÍQUESE"
LCDOUT $FE, $C1, "EN EL SCANNER"
PAUSE 100
GOSUB BARRIDO: GOSUB PTECLA
IF numero=15 THEN Y=1: GOTO PASSWORD      ; corresponde a presionar la tecla #
IF sensor=0 THEN GOTO CONHUELLA           ; recibe la señal del sensor y vaya a
GOTO ENTRADA                              ; ejecutar las funciones
```

5.3.6 TRANSMISIÓN DE PAQUETES DE COMANDO

Una vez generada la instrucción, ésta debe ser enviada al dispositivo FIM2030 para que pueda procesarla y ejecutarla. Para este proceso el microcontrolador debe enviar la información de forma ordenada, considerando el mismo orden de la estructura de datos requerida.

El objetivo que se busca con este procedimiento es generar los bytes de información principales para armar la estructura de datos que necesita el FIM2030. Estos bytes corresponden al registro Command, generando la siguiente estructura para la transmisión en puerto serial:

```
TRANSMITIR:
    SEROUT TX,T9600,[IN,CMD,P1,P2,TDAT,ERR,HCHEK,DAT,DCHEK]
    PAUSE 25
    RETURN
;**********RECIBIR PAQUETES DE RESPUESTA**********
RECIBIR:
    SERIN RX,T9600,[X],RIN,RCMD,RP1,RP2,RTDAT,RERR,RHCHEK,RDAT,RDCHEK
    PAUSE 100
    RETURN
```

Es válido considerar, que para cada configuración del equipo, el procedimiento variará de acuerdo a este, es decir, que en el caso de considerar este desarrollo para un control de asistencia, el dispositivo deberá contemplar un teclado numérico que tendrá que ser configurado para que presionando un número, el sistema sea

capaz de generar la instrucción de identificación y/o cualquiera de las funciones de configuración del dispositivo FIM2030, a las que se accederá de acuerdo al procedimiento de uso del sistema biométrico.
Las distintas configuraciones del dispositivo FIM2030 se hacen a través su protocolo de comunicación serial, por tanto las instrucciones generadas son hechas sobre el protocolo RS232 de acuerdo a las instrucciones dadas por el fabricante del dispositivo FIM 2030 (Véase los Apéndices A - C).

5.3.7 ESTRUCTURA DE PAQUETES DE COMANDO

Se debe tener en cuenta que el último byte de la estructura de datos que necesita el FIM2030, corresponde al registro **Checksum**, el cual verifica que la estructura de datos se encuentre bien generada. La información de este registro consiste en la suma del valor de todos los registros de la estructura de datos, en este sentido, si la suma es correcta entonces es válida la instrucción. En este caso, el valor del **Checksum** se genera con la suma de los registros CMD, P1, P2, TDAT y ERR que contienen los valores de los comandos ingresados en la estructura de datos. Esta suma es finalmente almacenada en el registro HCHEK.

Debido a que los registros se nutren de la información del buffer del puerto serial, para el caso de que la comunicación se interrumpa, los registros se almacenarán con ceros, ya que no se actualizará el buffer, por lo tanto, se generará una instrucción no válida, la cual al ser verificada por el **Checksum**, el dispositivo FIM2030 no reaccionará y el programa del microcontrolador volverá a la rutina principal a la espera de otra instrucción.

En cuanto al desarrollo de la línea de código para el microcontrolador nos basamos en las tablas del Apéndice C, quedando de la siguiente manera:

```
CONECTAR:                    ; COMANDO REQUEST CONNECTION
    CMD=$01: P1=$00: P2=$00: TDAT=$00: ERR=$00: HCHEK=$01
    DAT=$00: DCHEK=$00
    RETURN
```

Siguiendo la misma estructura, basado en las tablas del Apéndice C, se generara cada uno de los comandos requeridos para el funcionamiento del dispositivo biométrico.

5.3.8 MANEJO DEL TECLADO

Para el desarrollo e integración del teclado al microcontrolador, se consideró un teclado matricial de 16 teclas. La característica de este teclado es que se puede configurar por medio de la identificación de sus filas y columnas. Entonces, para este desarrollo se estableció la siguiente rutina que permite al microcontrolador cifrar el teclado matricial, sensando una a una las teclas presionadas:

```
BARRIDO:
    LOW A                                   ; sensar la fila A
    IF UNO=0 THEN numero=1: RETURN ; tecla pulsada retorne cargada con 1
    IF dos=0 THEN numero=2: RETURN          ; tecla pulsada retorne cargada con 2
    IF TRES=0 THEN numero=3: RETURN         ; tecla pulsada retorne cargada con 3
    IF CUATRO=0 THEN numero=10: RETURN      ; tecla pulsada retorne cargada con 10
    HIGH A
    LOW B                               ;sensar la fila B
        ……
    HIGH B
    LOW C                               ; sensar la fila C
        ……..
    HIGH C
    LOW D                               ;sensar la fila D
        ……..
    HIGH D
    PAUSE 10
    GOTO BARRIDO
```

Consecuentemente, y, ya que la velocidad de lectura del microcontrolador es muy elevada, y considerando que el ser humano al presionar y levantar el dedo de cualquier botón requiere de un espacio de tiempo de aproximadamente 250 ms., mientras tanto el microcontrolador ya ha sensado 25 veces, como si se hubiera pulsado esa cantidad de veces dicho botón. Entonces es necesario redactar un programa que permita sensar de forma correcta el presionado de cada botón, a este programa se le llama antirrebote de teclas:

```
PTECLA:
    HIGH bip: PAUSE 100: LOW bip      ; genera sonido cada vez que se pulsa una tecla
ESPACIO:                              ; programa de antirrebote de teclas
    IF UNO=0 THEN ESPACIO             ; si la tecla sigue pulsada ir a ESPACIO
    IF DOS=0 THEN ESPACIO
    IF TRES=0 THEN ESPACIO
    IF CUATRO=0 THEN ESPACIO
    PAUSE 25
    RETURN
```

Una vez que se ha obtenido el cifrado de cada uno de los números del teclado, se asignan los números para el menú que activará la rutina correspondiente. Para este desarrollo, se ha optado por las siguientes opciones:

Para el caso de los usuarios que no puedan realizar las marcaciones a través de la huella dactilar, por problemas de definición y calidad de la muestra biométrica, deberán realizar estas marcaciones ingresando su número de identificación. Este número de identificación corresponde a una contraseña de cuatro dígitos que puede ser personalizado por el usuario.

Para estos casos, al sistema también se le deberá ingresar una instrucción que le permita interpretar que el usuario se registrará por medio de su número de identificación. Bajo esta premisa, se designara una tecla específica que le indique al microcontrolador que el usuario ingresará al sistema a través de su contraseña.

Todas estas indicaciones aparecerán en el equipo a modo de instructivo para su utilización, de todas formas, por la experiencia que se ha tenido en estos sistemas, se ha resuelto que este es un proceso de acostumbramiento, en cuanto a que los usuarios una vez que conocen el funcionamiento del sistema pueden realizar las marcaciones sin problemas, tanto para navegar en las distintas opciones hasta posicionar el dedo correctamente para obtener la muestra biométrica.

5.3.9 COMPARACIÓN DE CLAVES

El uso de una clave de acceso es en extremo necesario, puesto que el enrolamiento de nuevos usuarios así como el borrado de los mismos deberá hacerlo únicamente una persona autorizada. De acuerdo a esto, se usara la clave que fue guardada

anteriormente en la memoria EEPROM.

5.3.10 CAMBIO DE CLAVE Y ESCRITURA DE EEPROM

Una de las funciones de nuestro producto es la posibilidad de cambiar la contraseña cuantas veces sea necesario. Para ello se genero la siguiente rutina:

```
GRABAUNO:                          ; PROGRAMA PARA CAMBIAR LA CLAVE
    LCDOUT $FE, 1                  ; TECLA D PRESIONADA
    LCDOUT $FE, $85, "NUEVA"
    LCDOUT $FE, $C3, "CONTRASEÑA"
    GOSUB BARRIDO: GOSUB PTECLA    ; ir a BARRIDO y retorna a un antirrebote
    WRITE 0, numero                ; guardar en la EEPROM 0 el valor de número
    lcd=2: GOSUB MENSAJE
 GRABADOS:
    GOSUB BARRIDO: GOSUB PTECLA
    WRITE 1, numero
    lcd=3: GOSUB MENSAJE
 GRABATRES:
        ……..
 GRABACUATRO:
        ……
    GOTO RESET                     ; ir a reset para cargar el nuevo valor de las variables
```

5.3.11 MENÚ DE FUNCIONES

Las opciones a presentarse en el LCD, son definidas después de cumplir los requerimientos de identificación. Entonces el menú de funciones que permiten controlar el vehículo se describen en la siguiente rutina:

```
 LCDOUT $FE,1
LCDOUT $FE,$80, "A.START   B.IGN"
LCDOUT $FE,$C0, "C.ACCE   D.OFF"
```

5.3.12 CONTROL DE POTENCIA

El uso de relés es esencial en nuestro producto, ya que esa es la única forma de automatizar y suprimir las funciones mecánicas realizadas por el Switch de ignición del vehículo, así, entonces el control de los relés es realizado directamente desde el

microcontrolador una vez cumplidos los requerimientos de identificación de usuarios y habiendo elegido la función a ejecutarse. Entonces la rutina queda de la siguiente manera:

```
CONDICIÓN:
    GOSUB BARRIDO: GOSUB PTECLA
    IF numero=11 THEN GOTO CONTACT                          ; presionada la tecla B
    IF numero=12 THEN GOTO ACCESORIO                        ; presionada la tecla C
    IF numero=13 THEN GOSUB APAGADO                         ; presionada la tecla D
    IF numero=10 THEN GOSUB ENCENDIDO: GOTO TRABAJANDO      ; presionada la tecla A
    IF numero=15 THEN GRABAUNO          ; corresponde a la tecla # para ir a grabar
     GOTO CONDICIÓN                     ; mantener dentro de este lazo
CONTACT:
    ……..            ; Habilita todo el sistema eléctrico del vehículo
TRABAJANDO:
    ……..            ; Mantiene al microcontrolador y al dispositivo biométrico
    ……..            ; en un estado de espera y muestra un mensaje en el LCD
ENCENDIDO:
    ……..            ; Habilita todo el sistema eléctrico y activa el motor de arranque
    ……..            ; por un lapso corto de tiempo, suficiente para encender el motor C.I.
accesorio:
    ……..            ; Habilita únicamente los accesorios como el radio
APAGADO:
    ……..            ; Apaga el motor C.I., deshabilita el sistema eléctrico y resetea
    ……..            ; el dispositivo biométrico
```

5.4 INTEGRACIÓN ELECTRÓNICA

El desarrollo del equipo para la identificación biométrica, consta de la integración de diversos componentes electrónicos, que deben ser controlados bajo un sistema centralizado, es decir, un microcontrolador que deberá controlar a cada uno de los componentes, de manera de establecer un mismo lenguaje de comunicación entre ellos. En este caso, el microcontrolador, cumple una tarea de gran importancia a la hora de interpretar las distintas instrucciones de cada uno de los componentes y poder manejarlos de acuerdo al tipo de solución implementado.

Como ya se ha mencionado, se implementará el microcontrolador 16F877a, perteneciente a la familia PIC, los que básicamente tienen la misma configuración

de pines.

La gran oferta y disponibilidad de información de este tipo de microcontrolador y por otro lado su precio competitivo con respecto a otra marca y modelo, hacen de este microcontrolador una alternativa conveniente a la hora de realizar el estudio de factibilidad de este dispositivo.

Para la implementación del microcontrolador se ha considerado el siguiente esquema:

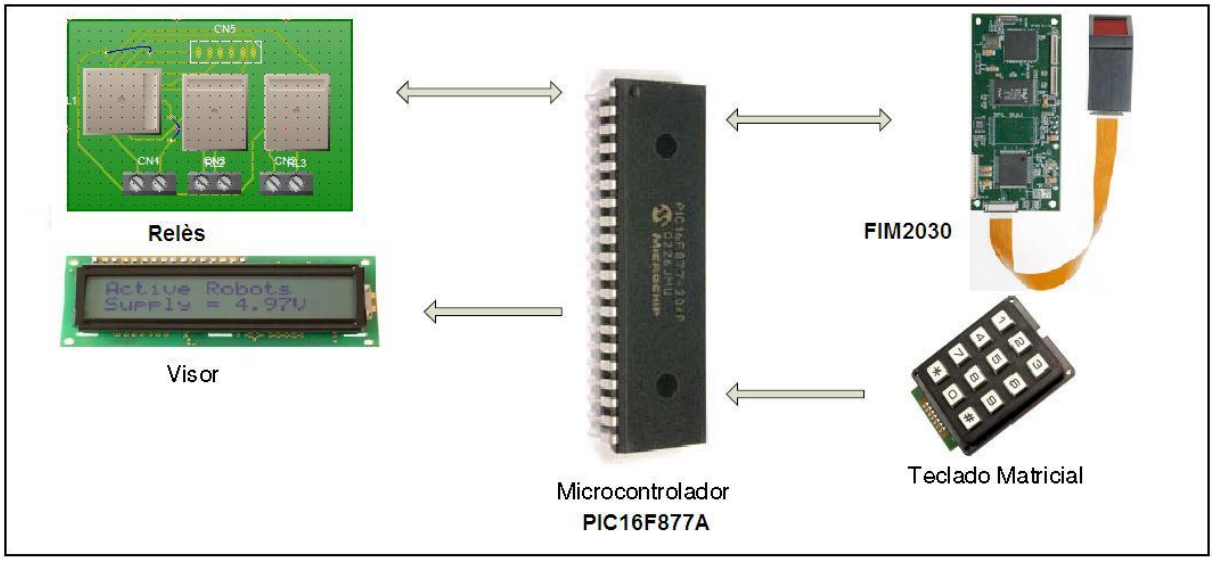


FIGURA 5. 5 Esquema de implementación

FUENTE: Propia (2010)

La integración electrónica también presenta una preocupación a la hora de administrar correctamente los pines que se utilizarán en el microcontrolador, sobre todo, por los puertos de comunicación a los que se deberán dar un uso exclusivo para cada componente.

5.4.1 INTEGRACIÓN DE COMPONENTES

5.4.1.1 Conversor Max232

El Max232 dispone internamente de 4 conversores de niveles TTL al bus estándar RS232 y viceversa, para la comunicación serial. El circuito integrado lleva

internamente 2 conversores de nivel de TTL a RS232 y otros 2 de RS232 a TTL con lo que en total se puede manejar hasta cuatro señales seriales, por lo general las más usadas son; TX, RX, RTS, CTS, estas dos últimas son las usadas para el protocolo **handshaking** pero no son imprescindibles. Para que este integrado, Max232, funcione correctamente se debe utilizar unos condensadores externos, como se muestra en la siguiente figura.

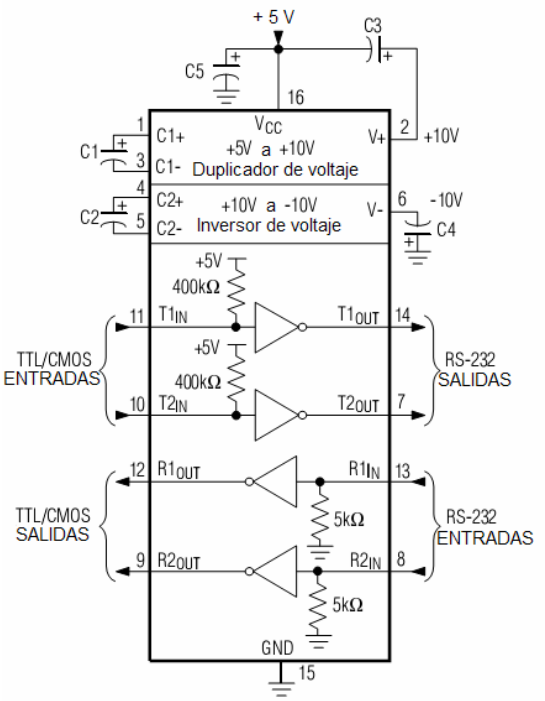


FIGURA 5. 6 Distribución de pines del circuito integrado max232[42]

Este circuito integrado permitirá, al microcontrolador, comunicarse bajo el protocolo serial con el dispositivo biométrico FIM2030 y los componentes que son necesarios para hacer una transmisión de datos. Con este sistema, el microcontrolador que se comunica con niveles TTL, puede convertirlos a niveles RS232 y trabajar bajo solo un mismo formato de comunicación.

Para integración de los demás componentes se debe pensar en la disponibilidad de puertos de comunicación del microcontrolador, desde este punto de vista y con el propósito de integrar cada uno de los componentes se ha diseñado una configuración que permita incluir todos los elementos necesarios para el funcionamiento del dispositivo de identificación biométrica.

[42] Max232_maxim_datasheet.pdf

Debido a que todos los dispositivos son controlados por el microcontrolador, éstos deben ser configurados desde el propio microcontrolador.

5.4.1.2 Conexión de Teclado

Comenzando por el teclado, se ha dispuesto la siguiente distribución de pines y conexionado, permitiendo reservar un puerto exclusivo para este fin. Con la finalidad de ilustrar esta distribución se ha desarrollado el siguiente esquema.

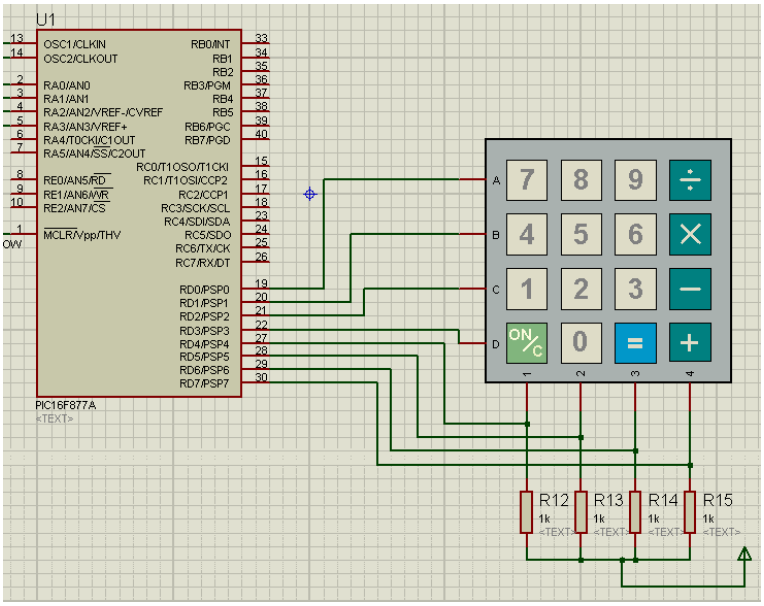


FIGURA 5. 7 Diagrama de conexión de teclado

Fuente: Propia “ISIS” (2010)

Para el teclado se ha destinado el puerto D del microcontrolador, es decir, que para obtener algún dato de teclado, la rutina de programación en el microcontrolador se programará este puerto sólo para el ingreso de datos.

Debido a que se trata de un teclado matricial, los datos ingresan por la combinación de filas y columnas para identificar el dato ingresado.

5.4.1.3 Conexión del Visor

Para la conexión del visor, se ha reservado y configurado el puerto B del microcontrolador, donde se designaron cuatro líneas de datos para el control del visor.

El diagrama esquemático de la conexión del visor, se muestra en la siguiente figura.

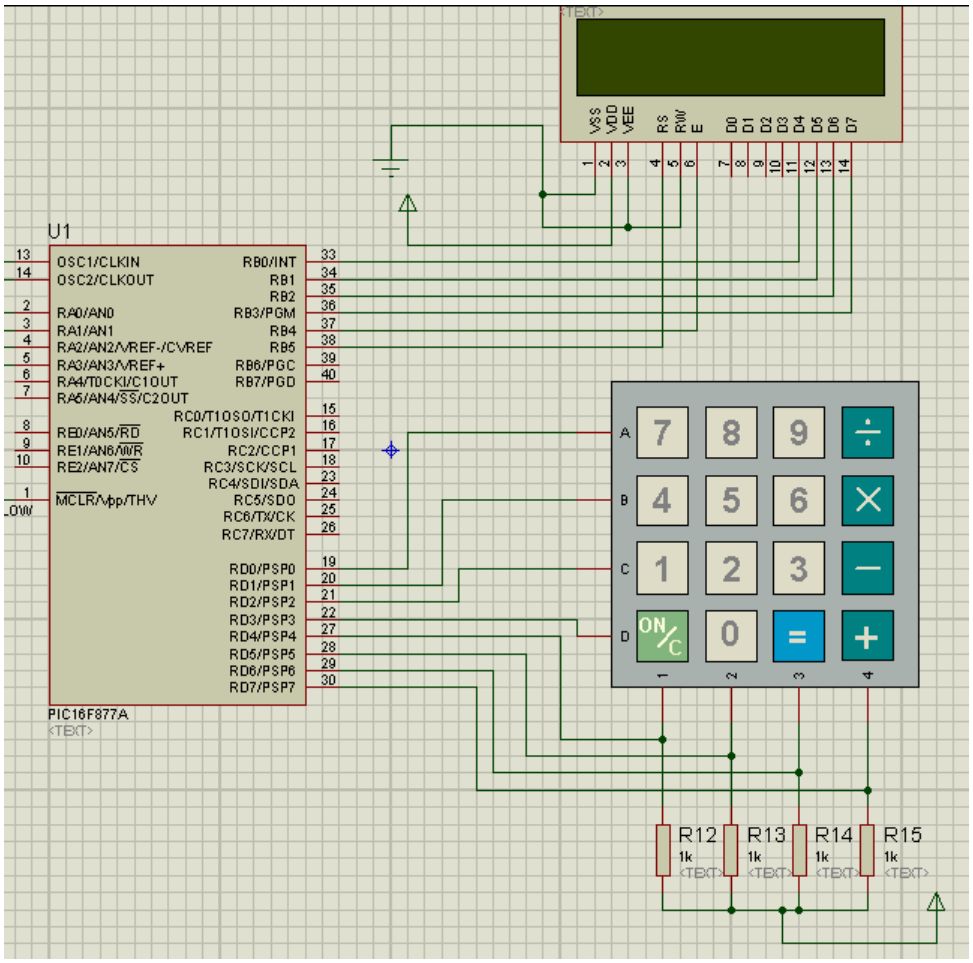


FIGURA 5. 8 Diagrama de conexión del visor

Fuente: Propia (2010)

Otro elemento indispensable para el desarrollo del dispositivo, es el sistema de comunicación. Este sistema consta de 3 etapas, el primero es la comunicación del propio microcontrolador, la que se realiza a niveles TTL. Para comunicar el microcontrolador con el FIM2030 se debe basar en el protocolo serial de comunicación.

La comunicación serial, funciona a niveles RS232, por lo tanto las instrucciones desde y hacia el microcontrolador se deben transformar de niveles TTL a RS232, por medio del circuito MAX232. Entonces, las instrucciones que emite el microcontrolador se deben dirigir directamente al FIM2030 para que puedan ser ejecutadas por el dispositivo biométrico.

Finalmente, la integración de cada uno de los dispositivos creará las bases de cada equipo de identificación biométrica, es decir, que dependiendo de la solución que se quiera implementar con este equipo, su configuración electrónica no variará demasiado.

Para el caso de necesitar implementar este equipo para una solución de control de asistencia, las características, en cuanto a integración electrónica, son las mismas descritas.

Para la producción del equipo de identificación biométrica, se debe crear una tarjeta con los circuitos integrados necesarios para su conexión y control del dispositivo biométrico.

Como requerimiento para producción en serie de estas tarjetas se ha establecido que las placas deben tener las siguientes características:

- Placa de Fibra.
- Pistas de doble faz.
- Perforaciones metalizadas en plomo de estaño.
- Máscara de soldadura serigráfica.
- Confección de guía de componentes.

Para el diseño y confección de las tarjetas, se desarrolló el siguiente plano esquemático con los circuitos integrados y conexiones necesarios para su funcionamiento.

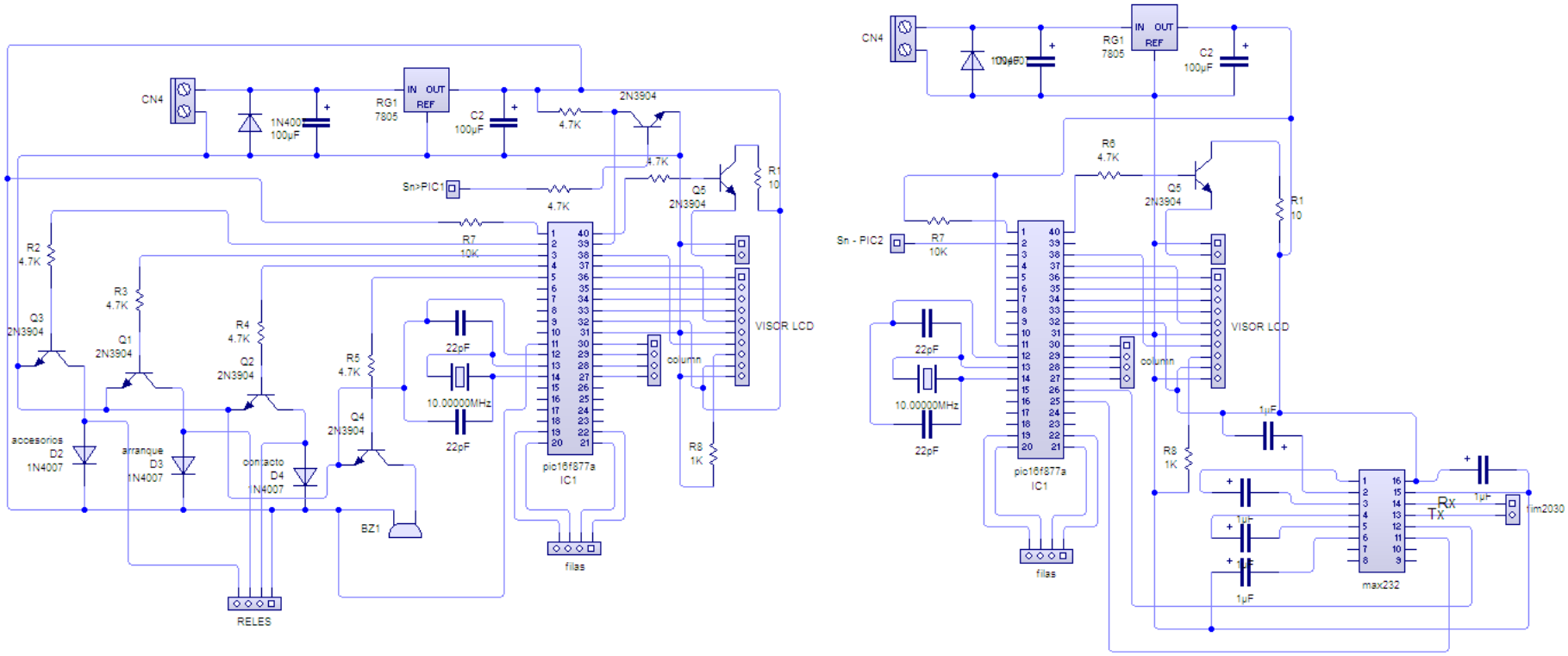


FIGURA 5. 9 Diagrama completo de conexión

Fuente: Propia LIVEWIRE (2010).

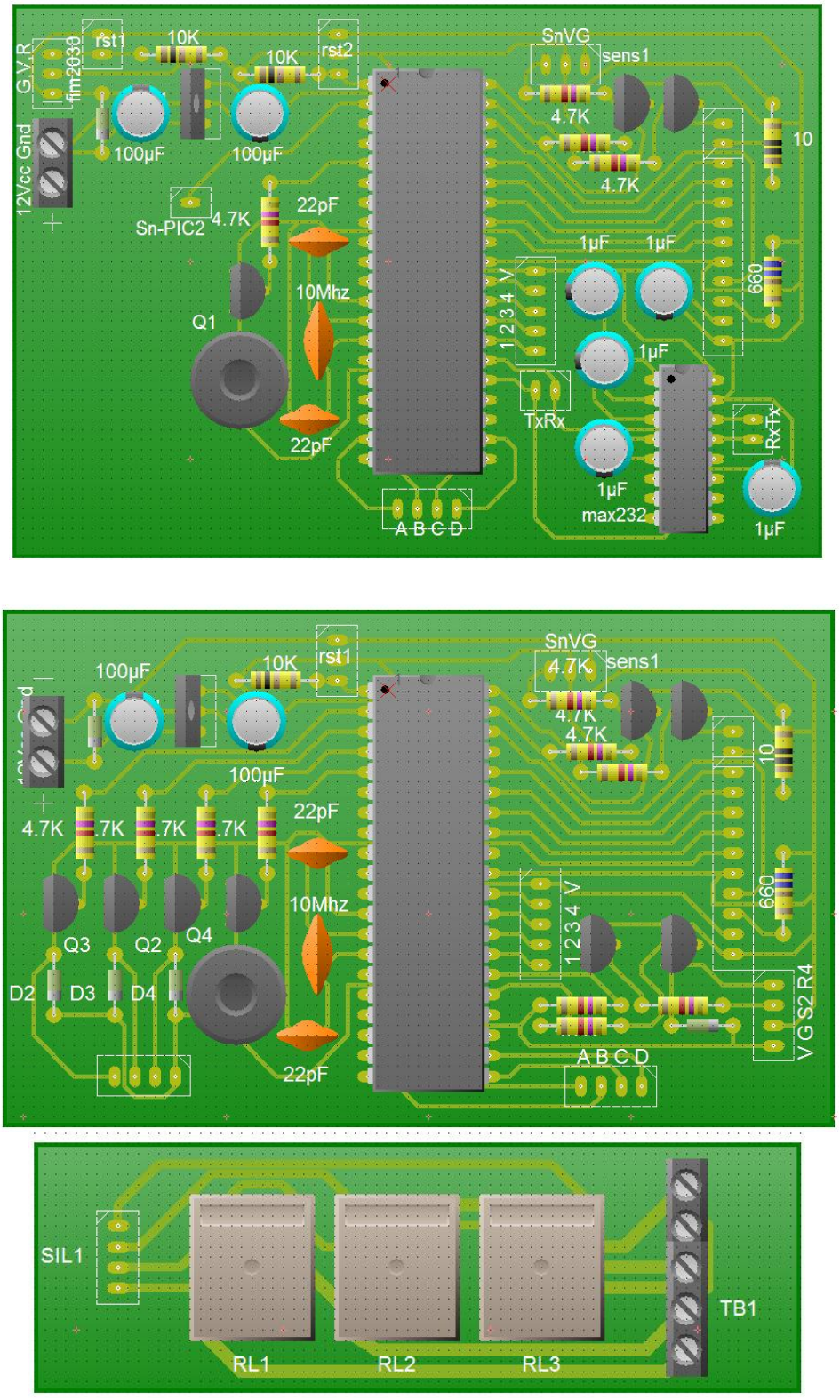


FIGURA 5. 10 Circuitos de control de dispositivos

Fuente propia PCB WIZARD (2010)

5.5 CONTROL DE APERTURA DE PUERTAS POR RFID

Debido al riesgo por mala manipulación y sensibilidad del lector biométrico, no se aprobó la factibilidad de instalar un scanner de huella digital en la puerta del vehículo, entonces, se planteo el uso del sistema de identificación por radio-frecuencia, ya que el objetivo del presente trabajo es tener acceso al vehículo a través de elementos de seguridad donde se pueda prescindir del uso de llaves.

Aunque este sistema requiere del uso de un transponder, es ideal para el cumplimiento de nuestro objetivo, ya que la identificación del usuario se realiza sin la necesidad del contacto físico entre el usuario y el vehículo, esto limitado por una cierta distancia de trabajo de 20 cm que es el rango dentro del cual el transponder recibe la señal electromagnética del transceptor para el emparejamiento de señales.[43]

5.5.1 METODOLOGÍA

Para el control de apertura de puertas del vehículo fue usado el lector RFID: ID-12; como una alternativa de uso del sistema RFID. Además, se hizo necesaria la utilización de un microcontrolador (PIC16F628A) a modo de host, el cual nos permitirá recoger la señal eléctrica de uno de los puertos de salida del dispositivo ID-12, la cual nos indicara que se ha identificado al usuario. Para luego procesar dicha señal y a través del microcontrolador lograr la apertura automática de los seguros de las puertas del vehículo.

FIGURA 5. 11 ID-12

[43] ID SERIES DATASHEET Mar 01, 2005

5.5.2 FUNCIONAMIENTO

El funcionamiento de este dispositivo de control se explicó en el capítulo II, por tanto en este capítulo se excluye dicha explicación.

El producto creado en base al dispositivo RFID: ID-12 controla el bloqueo y desbloqueo automático de las puertas del vehículo. Para ello el microcontrolador PIC16F628A recoge una señal de voltaje extraída del pin 10 del dispositivo ID-12, para luego comparar esta señal y realizar el control de potencia. A continuación se presenta el diagrama de conexión sugerido por el fabricante.

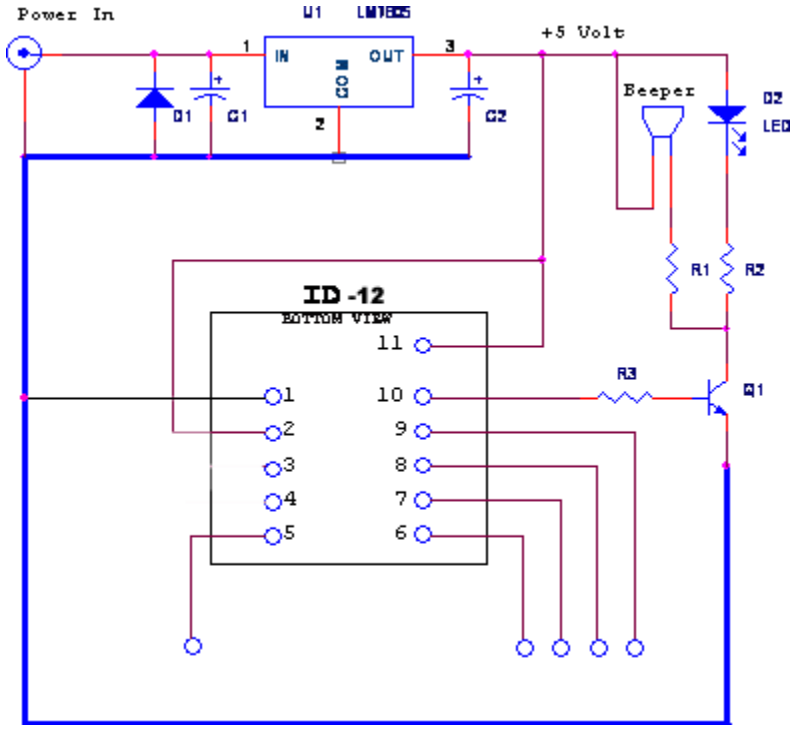


FIGURA 5. 12 Diagrama de conexión sugerido por ID-Series[44]

5.5.3 INTEGRACIÓN DE COMPONENTES

El acoplamiento del dispositivo ID-12 se hace a través del cumplimiento de los requerimientos eléctricos dados por el fabricante, principalmente lo que respecta a voltaje y corriente (5 VDC @ 30mA nominal).

[44] ID SERIES SR(2005-3-1) rev19

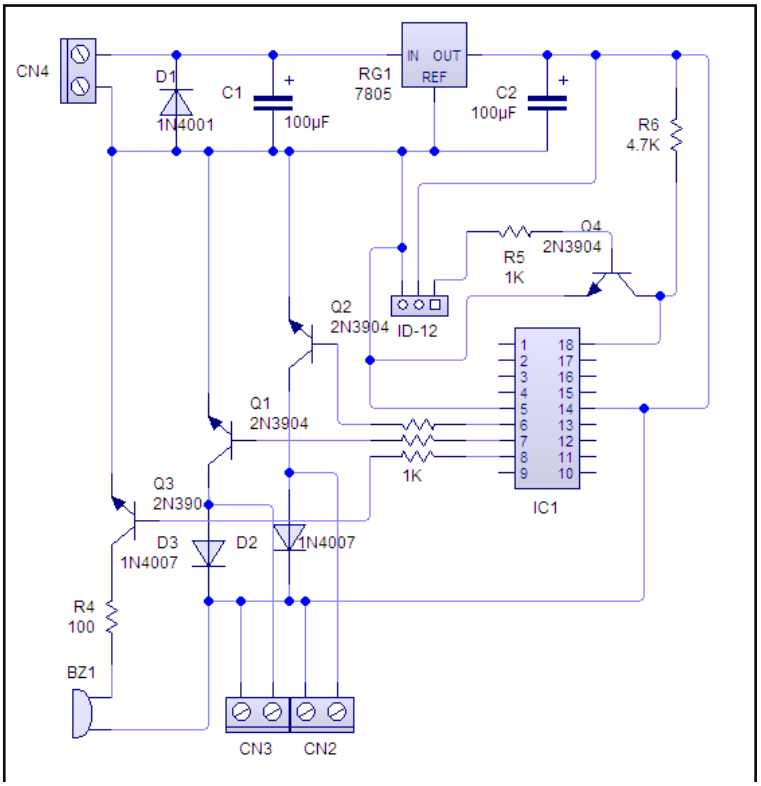


FIGURA 5. 13 Diagrama de conexión del control de apertura de puertas

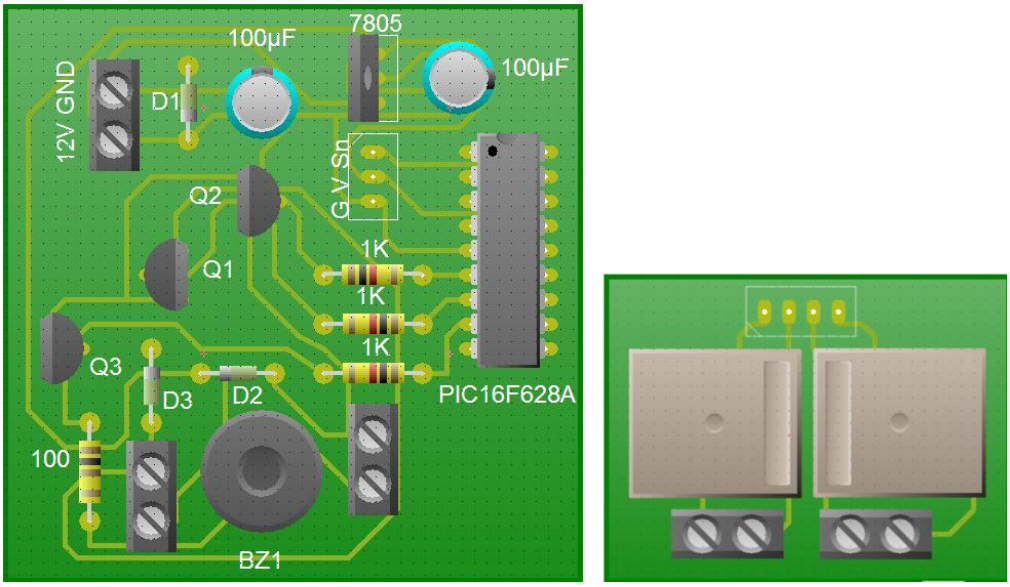


FIGURA 5. 14 Circuito de control de acceso con ID-12 y Pic16F628A

Fuente: Propia (2010)

Conforme al desarrollo del plano esquemático se elaboró la siguiente tabla de componentes.

TABLA 5. 4 LISTA DE COMPONENTES

DETALLE	CANTIDAD
Identificador biométrico FIM2030 NITGEN	**1**
Microcontrolador PIC16F877A	**2**
DISPLAY LCD 16x2	**2**
Teclado matricial 4x4	**2**
Relés de 5v, 15A	**5**
Identificador por radio frecuencia ID-12	**1**
Microcontrolador PIC16F628A	**1**
Regulador de voltaje 7805	**3**
Condensador de 100 uf	**6**
Condensador de 22 pf	**4**
Condensador de 1 uf	**5**
Diodo rectificador 1N4007	**8**
Transistor NPN 2N3904	**15**
Oscilador de 10Mhz	**2**
Resistencia de 1Kohm	**4**
Resistencia de 10Kohm	**3**
Resistencia de 4.7Kohm	**15**
Resistencia de 660ohm	**2**
Resistencia de 10ohm	**2**
Buzzer de 5v	**3**
Bloque de terminales	**9**

Conectores en simple línea	**17**
Cable IDE (Bus de datos)	**1**
Cable UTP 4 pares (metro)	**1**
Cable automotriz Nº 16 flexible (metro)	**6**
Placa de fibra 30x15 cm	**1**
Caja de proyectos (poliuretano)	**2**

Fuente: Propia (2010)

CAPITULO VI

PRODUCTOS

6.1 INTRODUCCIÓN

De acuerdo a los objetivos de este proyecto de generar productos rentables, versátiles y de bajo costo, se ha diseñado y desarrollado en base a la integración electrónica de partes y piezas junto con la integración e implementación de la programación necesaria para el funcionamiento del dispositivo de identificación biométrica. Hasta aquí se ha revisado y detallado cada uno de los pasos técnicos; precisamente, los aspectos técnicos del desarrollo del producto.

Una vez resuelto y desarrollado las bases teóricas, experimentales y los aspectos de integración electrónica de componentes, es preciso crear las bases para el propio desarrollo del producto, es decir, que la solución debe quedar paquetizada, de manera de crear un producto que pueda ser vendido.

Para este desarrollo se debe crear un dispositivo para que pueda ser manipulado y usado por un usuario, un equipo que esté destinado a una cierta tarea como puede ser el control de asistencia o acceso. En estos casos, se creará un producto para cada aplicación en particular de manera de crear estructuras de negocios para cada producto y poder rentabilizar el desarrollo realizado.

Este desarrollo de este proyecto consiste en el diseño, fabricación e implementación de un equipo para el control de asistencia y acceso para controlar las funciones eléctricas esenciales de un vehículo Jeep Grand Cherokee 5.2 Lt. Sin restricciones de que pueda ser instalado en cualquier otro vehículo independientemente de la marca y el modelo. Para ello, el equipo deberá contar con características técnicas específicas, de manera de fabricar un equipo de uso exclusivo a una aplicación determinada, que en nuestro caso se trata de permitir el arranque y puesta en marcha del vehículo en mención.

La fabricación de estos productos, permitirán desarrollar el plan de negocios para cada uno de ellos.

6.2 DESARROLLO DEL PRODUCTO

En base al desarrollo electrónico realizado para la identificación biométrica, se han establecido diversos parámetros para el diseño del producto final.

Teniendo estas especificaciones en cuenta y considerando los objetivos de este proyecto que se basan en la versatilidad y bajos costos, se creó una estructura del equipo que le permitiera ser los más flexible posible utilizando características modulares. Es decir, que dependiendo de la solución que se quiera producir y vender, dependerá de que componentes se incluyan permitiendo conservar la estructura principal del equipo, cambiando solamente los componentes de identificación y elementos opcionales.

Bajo esta estructura modular, es que se creó un equipo de carcasa plástica de 2 mm de espesor, que permite agregar dispositivos opcionales sin tener que variar su diseño.

Para el desarrollo de este equipo se ha pensado principalmente en brindar soluciones de asistencia, como reloj control y control de acceso que permite la conexión a un dispositivo eléctrico de control de relés para la puesta en contacto (ignición), puesta en marcha del motor de arranque y control de los accesorios eléctricos del vehículo.

6.2.1 COMPONENTES

Como componentes principales, que irán como elementos de serie independiente del tipo de solución son:

- Dispositivo Biométrico FIM2030
- Teclado
- Visor LCD

Los dispositivos opcionales generarán las características de cada equipo, que dependerá de la funcionalidad que se le quiera brindar.

6.2.2 DISEÑO

Para el diseño y fabricación del equipo se consideraron diversos requisitos, de manera de cumplir con todos los aspectos de modularidad que se desea obtener. En este aspecto, se consideraron los siguientes conceptos:

- Diseño de un equipo compacto y robusto.
- Diseño atractivo y moderno.
- Gama de colores personalizable. Permite crear un equipo con colores corporativos.
- Seguridad, tanto para los componentes electrónicos como también para los usuarios.
- Permite un alto tráfico de uso y condiciones adversas, tanto ambientales como de uso.
- Fácil acceso a mantención.

6.2.2.1 Concepto

La característica principal del producto radica en su simpleza, en este caso, se ha desarrollado un concepto simple tanto para el armado e integración de partes y piezas, como para la fabricación del equipo.

Este concepto se basa en 2 piezas que estructurarán el equipo.

- **Caja de componentes.**

En esta sección se anclará cada uno de los componentes electrónicos, sobre esta base se generarán las piezas de sujeción y sistema de ventilación.

- **Mascara.**

Corresponde al elemento estético del equipo, permitiendo además estructurar la posición de cada componente.

6.2.2.2 Diseño final

Luego de un desarrollo y análisis del diseño se realizaron mejoras, tanto en su estructura, como en la estética del equipo, siempre conservando el concepto básico de este desarrollo.

FIGURA 6. 1 Diseño final

Fuente: Propia (2010).

6.3 PRESENTACIÓN DEL PRODUCTO

Una vez obtenido el producto, como concepto y diseño en un prototipo, se pueden establecer en forma real y demostrando las características del equipo.

Por otro lado, sus prestaciones garantizan un óptimo funcionamiento en cuanto a la identificación y validación de la identidad de los usuarios registrados, cumpliendo con los principales requerimientos de control de acceso.

6.3.1 CARACTERÍSTICAS TÉCNICAS

Dimensiones: 220 mm. Alto

150 mm. Ancho.

50 mm. Profundidad.

Temperatura de funcionamiento: 0º C a 40º C

Rango de humedad de funcionamiento: < 90 % HR, no condensable.

Alimentación: 12 –14,6 V DC

1.5 – 2.5 A

6.3.2 ESPECIFICACIONES TÉCNICAS

*** Equipo con arquitectura Microcontrolador y FIM2030**

Microcontrolador de 8 bit y 8K Bytes de memoria flash

Operación: 0 - 20 MHz

FIM2030:

- CPU: S2C2410 (ARM9)
- SDRAM: 8MByte
- FLASH ROM: 1MByte Program Flash, 1/2/4MByte DB Flash

- Capacidad para enrolar a 500 usuarios.

- **Visor:**

  Tipo: LCD de 2 líneas y 16 caracteres.

  Área visible: 60 mm. × 18 mm.

  Backlight incorporado.

- **Teclado:**

  Tipo: Membrana de alto tráfico.

  Material: poliéster texturizado.

  16 teclas; pad numérico y 4 funciones de menú.

  Vida Útil: > 1.000.000 operaciones por tecla.

- **Sensor Biométrico:**

  NITGEN OPP03

  Resolución de la Imagen: 500 DPI ± 0.2%

  Tamaño de la imagen: 260 × 300

  Área efectiva de detección: 13 mm. × 15 mm.

  Escala de grises imagen: niveles de grises de 8-bits

  Distorsión: < 0.1%

  Fuente de luz: LED rojo

  Duración (típica) del sensor: 60.000 horas.

  Condiciones de luz ambiental: sobre los 5.000 LUX.

6.4 FUNCIONAMIENTO

El producto creado lleva incorporado dos display LCD y dos teclados matriciales de 4 x 4, como interfaz para el usuario. Los requerimientos del equipo se presentan a modo de mensajes en el LCD y el teclado ha sido configurado para responder a los menús presentados. Generando, así, un producto de fácil manipulación y alta confiabilidad.

6.4.1 PROCESO DE IDENTIFICACIÓN

Para el proceso de identificación se diseñó un sistema que permite, sólo utilizando la huella dactilar, iniciar el proceso de validación de la identidad del usuario en el propio equipo, o sea, buscando en la base de datos propia del equipo, para luego, solo enviar los reportes de las marcaciones realizadas.

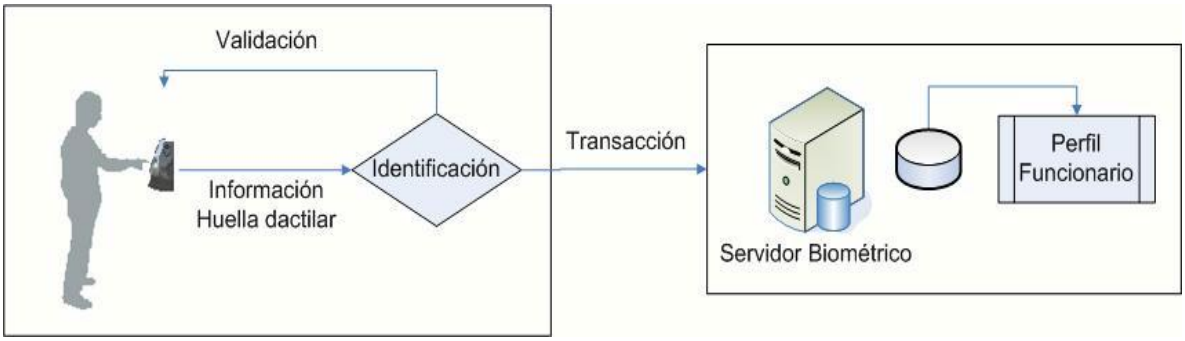


FIGURA 6. 2 Proceso de identificación

Fuente: Propia. (2010)

Para iniciar la configuración del equipo el usuario debe poseer el privilegio de usuario máster, es decir, debe conocer la contraseña de acceso para acceder al modo de configuración. La contraseña o PIN es un número de 6 dígitos que inicialmente es la serie 1, 2, 3, 4, 5, 6 que debe ser cambiada en la primera configuración del dispositivo.

Para el registro de nuevos usuarios el dispositivo solicitará un número de identificación personal, en este campo deberá ingresarse el número de cédula del nuevo usuario. Debe establecerse también el tipo de usuario (ordinario o VIP), el nivel de seguridad al cual será sometido (rango de 1 - 4) y el espacio de la base de

datos que ocupará. Todos estos requerimientos aparecen en el LCD, facilitando al usuario el proceso de configuración.

Una vez configurado el equipo puede empezar verificando las huellas grabadas. El dispositivo escaneará automáticamente la identidad del usuario, una vez que éste posicione su dedo sobre el sensor biométrico. Si la identidad del usuario es validada se encenderá un led verde indicando que el usuario se encuentra registrado, caso contrario se encenderá un led rojo.

6.4.2 CONTROL DE PUESTA EN MARCHA DEL VEHÍCULO

Una vez inicializado el sistema de identificación biométrica se presenta en el LCD (en modo de espera) el nombre y la versión del proyecto “IDENTIFICADOR BIOMÉTRICO LC.01”, en ese momento el dispositivo biométrico puede ser configurado, pudiendo realizar operaciones de registro de nuevos usuarios, borrado de la base de datos y reconocimiento de usuarios sin que el motor de combustión se ponga en marcha.

Para iniciar el proceso de control de acceso el usuario deberá presionar un botón del teclado (numero “0”) para indicarle al equipo que valide su identidad y proceda a arrancar el vehículo. En ese instante y por razones de seguridad el usuario dispone de 10 segundos para identificarse antes de que el equipo vuelva a modo de espera. Dentro de esos 10 segundos el usuario puede presionar el botón “#” para arrancar el motor a través del reconocimiento de una contraseña de cuatro dígitos. Una vez identificado el usuario el dispositivo inicia el control de los sistemas del vehículo, allí, el equipo se reserva un espacio de 3 segundos antes de arrancar automáticamente el motor de combustión; dentro de estos 3 segundos el usuario puede acceder al menú de control del vehículo presionando el botón “*”; el menú presenta cuatro opciones:

Puesta en marcha del motor de combustión	presionar “A”
Conexión de los sistemas eléctricos	presionar “B”
Habilitar únicamente accesorios	presionar “C”

Salir/Apagar presionar “D”

Una opción adicional corresponde a ir a grabar una nueva contraseña, para ello el usuario deberá presionar el botón “#”. Una vez cambiada la contraseña el equipo se reiniciará y el usuario deberá identificarse de nuevo.

Una vez puesto en marcha el motor de combustión o habiendo elegido una de las funciones del menú, el equipo ingresa a un segundo modo de espera, donde sensará al teclado esperando que el usuario presione el botón “D” para apagar el motor o desconectar los sistemas eléctricos. Después de confirmar el apagado, el usuario dispondrá de 3 segundos para volver al menú, presionando el botón “*”, caso contrario el sistema vuelve al modo de espera y el usuario deberá identificarse de nuevo.

6.4.3 OTRAS SOLUCIONES

Utilizando el desarrollo de la identificación autónoma, con el microcontrolador y el dispositivo biométrico FIM2030, se puede realizar una diversidad de aplicaciones. Debido a su arquitectura y configuración se puede desarrollar un equipo autónomo que sólo necesite integrarse a algún equipo con conexión serial o TCP/IP para brindar un grado de control y seguridad a cualquiera de estos sistemas.

CAPITULO VII

GESTIÓN DE MERCADO

7.1 VALOR DISTINTIVO

Este nuevo equipo, para el control de acceso biométrico, está destinado principalmente a satisfacer las necesidades de medianas y grandes empresas o usuarios particulares que requieran de sistemas de control seguros, donde exista un elevado flujo de usuario y sea necesaria una autenticación segura y eficiente o como una opción de personalización, para el área de Tuning Car. Los diseños de las soluciones serán flexibles para la adaptación en los distintos sistemas que tengan los clientes.

En estos momentos la oferta actual ofrece diversos dispositivos que contienen elementos biométricos para el control de personas, y el mercado tiene un comportamiento que, poco a poco, ha ido incorporando estas tecnologías. Este comportamiento ha ido evolucionando desde la desconfianza o el temor que dispositivos biométricos, como la lectura del iris, que puedan causar algún tipo de daño a la salud hasta la necesidad de incorporar sistemas de control seguros y con bajas tasas de error. Durante esta evolución a un mayor acercamiento de este tipo de tecnologías es necesario contar con elementos que realicen una interfaz amigable entre la tecnología, en este caso, el dispositivo de control y el usuario. Es por estas razones, que se hace necesario crear un vínculo cercano con el usuario, para ello, se ha creado un equipo con un diseño atractivo y de uso intuitivo, ayudado con una interfaz desplegada en el visor, que por medio de un menú pueda ser personalizada, en cuanto al nivel de información que se desee entregar al usuario del equipo.

7.2 ANÁLISIS DE MERCADO

7.2.1 COMPETENCIA

Actualmente existen diversas empresas que comercializan dispositivos de control biométrico para el control de acceso y asistencia, con productos que van desde soluciones creadas sobre arquitectura PC, hasta equipos integrados con tecnología

propietaria de reconocimiento de huella dactilar.

Sin, embargo las soluciones que las empresas especializadas en biometría ofertan están enfocadas únicamente a empresas industriales o bancarias. Hasta hoy no existe en el mercado productos de identificación biométrica que puedan ser implementados en vehículos. Por esta razón se puede especular sobre la acogida que puede darse a nuestro producto. Ya que podemos considerarlo como un producto completamente nuevo, de innovación tecnológica.

7.2.2 ESTRATEGIA DE VENTA

En esencia, se debe vender la compañía, no sólo el producto. De esta forma, no basta con realizar una transacción con el cliente o sólo vender un dispositivo con tecnología biométrica. Se deben vender soluciones a la medida de cada cliente junto con sus servicios asociados, o sea, identificar, analizar y satisfacer las necesidades del cliente.

No basta con sólo realizar una transacción con el cliente, se debe buscar una relación a largo plazo, destacando la importancia de la relación para ambas partes.

El desarrollo de un dispositivo requerirá establecer estrategias para generar soluciones, que al llegar el momento de producir deben ser eficientes y que garanticen el cumplimiento de los requerimientos, tanto en lo técnico, como en los plazos requeridos.

TABLA 7. 1 GENERACIÓN DE PLAZOS DE RESPUESTA

ETAPA	PROCESO	TIEMPO
Generación del requerimiento	Recepción, análisis y diseño de la propuesta.	1 a 2 semanas dependiendo de la complejidad del requerimiento
Implementación de la solución	Integración del dispositivo, desarrollo de la propuesta, prueba e implementación del sistema.	1 a 2 semanas según el tipo de proyecto.

Puesta en marcha	Instalación, Capacitación y evaluación en terreno	1 semana.

Fuente: Propia (2010)

La venta de los equipos tiene mucha relación con el enfoque de la empresa, en este sentido, la empresa, al no tener una fuerza de venta desarrollada, tiene que crear una estrategia de venta avalado por un socio comercial, es decir, traspasar las expectativas de venta a una empresa que tenga la fuerza y recursos para estructurar una estrategia exitosa. En este caso, al no ocuparse la inversión en recursos de ventas, se desarrolla un plan de proveedor de equipos y soluciones, principalmente enfatizando en realizar una estrategia comercial con grandes empresas ya consolidadas que permitan sustentar el financiamiento de la venta.

7.2.3 ENFATIZAR LAS ACTIVIDADES DE SERVICIO Y APOYO

Como otro elemento diferenciador, se realizarán actividades que respalden al producto, en este sentido, el producto se compone de una serie de elementos que generan finalmente la solución que requiere el cliente. Para ello, se debe realizar una oferta de servicios asociados como son;

- Servicios de instalación.
- Servicios de mantención.
- Capacitación.

7.2.4 ESTRATEGIA DE PROMOCIÓN

Se establecerá una estrategia principal a la hora de alcanzar nuevos clientes, de esta manera se buscará realizar publicidad en periódicos y en banners de portales dirigidos a nuestro mercado objetivo.

De esta forma, se deberán construir elementos que permitan el apoyo de la publicidad del producto con sus soluciones y servicios asociados, en este sentido, se hablará de folletos de ventas y catálogo de productos. En este sentido, se creará servicios de correo directo con clientes y potenciales clientes con información

actualizada de las diversas alternativas que ofreceremos, las actualizaciones y mejoras generadas con toda la información del producto, sus soluciones y servicios de apoyo.

7.2.5 ESTRATEGIA DE FIJACIÓN DE PRECIOS

Para la correcta planificación de los precios hay que tener en cuenta los objetivos planteados para este proyecto, es decir, se quiere introducir un dispositivo de bajo costo y generar soluciones integrales. Es por eso, que independiente del precio de venta del dispositivo se debe enfatizar en cobrar precios competitivos en la creación de soluciones y la obtención de los buenos resultados que se ofrecerán. Para ello, es esencial crear una estructura coincidente y balanceada entre los costos y la estructura de salarios, que permitan y aseguren buenos servicios de apoyo asociados a la creación de soluciones.

Por lo tanto, se deben establecer los parámetros que se utilizarán para cobrar los servicios de apoyo como son; los servicios de instalación, servicios de mantención, capacitación y apoyo de redes de trabajo, asegurando disponibilidad y un precio de venta que permitan generar ganancias.

Entre los principales factores que influyen en la fijación de precios se consideraron los siguientes:

- Factores internos y externos que afectaron la decisión de fijar el precio de cada producto.
- Estrategias de fijación de precios.
- Ventajas y desventajas.
- Contextos apropiados de aplicación.

7.2.5.1 Factores internos

1. Objetivos de marketing: antes de fijar los precios, se debió decidir qué estrategia seguirá el producto. Para esto se debió desarrollar los principales objetivos para el marketing:

- Supervivencia.
- Maximización de las utilidades actuales.
- Liderazgo en participación del mercado.
- Liderazgo en calidad del producto.

Para coordinar las decisiones de fijación de precios se deben considerar con las decisiones en cuanto al diseño del producto, su distribución y promoción para formar un programa de marketing, coherente y eficaz.

2. Costos: los costos establecerán el límite inferior para la fijación del precio. Nuestra compañía quiere cobrar un precio que cubra todos sus costos de: producir, distribuir y vender el producto y también genere un rendimiento justo por los esfuerzos y los riesgos considerados.

3. Consideraciones de organización: por un lado, la gerencia debe decidir quién de la organización fijara los precios. En este caso, por ser una empresa pequeña, la alta gerencia manejarán los precios.

7.2.5.2 Factores externos

• Naturaleza del mercado y la demanda: debido a que los costos establecerán el límite inferior del precio a fijar, el mercado y la demanda establecerán el límite superior. El mercado, en este caso, puede ser de varios tipos, si bien el análisis más profundo de cada uno nos desviaría del objetivo central de este proyecto, es conveniente nombrar las características principales del mercado al que se requiere apuntar.

7.2.5.3 Estrategias Generales para fijar precios

• Fijación de precios basada en el costo: Se ha utilizado el método más simple de las estrategias para la fijación del precio, se trata de establecer el costo del producto y asignarle un margen de venta. Este margen dependerá del tipo de solución y producto, en el caso de realizar proyectos de una gran envergadura se utilizará una

estrategia de fijación de precios por utilidades meta, que consiste en fijar un precio con el fin de obtener cierta utilidad que es establecida como meta u objetivo.

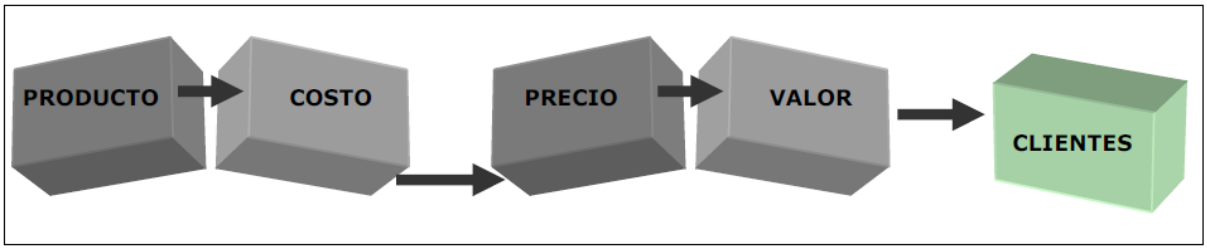


FIGURA 7. 1 Fijación de precios basada en el costo

Fuente: Propia. (2010)

7.2.6 PRODUCTO NUEVO

En base a la estrategia de fijar los precios de acuerdo a los costos asociados, es necesario también considerar la necesidad de la empresa de innovar con este nuevo producto e insertarse en el mercado con una estrategia para penetrar en el mercado.

Bajo este concepto, se fija un precio bajo, con el fin de atraer la mayor cantidad de compradores posibles y así lograr una importante participación en el mercado, que se irá desarrollando de acuerdo a la maduración del producto. Al alcanzar, entonces, un elevado volumen de ventas, los costos, por ende, serán inferiores, lo que puede permitir bajar más aún el precio, generando economías de escalas.

7.2.7 CÓMO RESPONDER A LOS CAMBIOS DE PRECIO

Debido a la fuerte relación que existe entre los precios de los componentes que conforman el dispositivo y el desarrollo de nuevas tecnologías, es necesario estar atento y anticiparse ante el cambio tecnológico para enfrentar de mejor forma la maduración del producto. Si bien es cierto, este dispositivo representa un desarrollo que permitirá generar un producto comercialmente rentable, es necesario investigar el mercado, tanto nacional como internacional, que permita establecer los pasos a seguir, de acuerdo al desarrollo de nuevos productos que realicen las mismas tareas a un costo menor. En este sentido, la respuesta de la empresa ante los

cambios de precio es un factor de gran importancia a la hora de generar y desarrollar un plan de negocios viable para un producto, tomando en cuenta todas las variables que se involucran y anticipándose a los cambios generados por el mercado.

Se debe tener en cuenta, cómo los consumidores reaccionan a los cambios, debido al propio ciclo de vida del producto y, por otro lado, desde el punto de vista de la empresa, cuál es la importancia del producto dentro de la variedad de productos que conforman la cartera.

De manera de graficar y al mismo tiempo de detallar el flujo lógico que se deberá considerar al momento de resolver los distintos factores que pueden afectar al cambio de precio del producto, se muestra en el esquema de la siguiente figura:

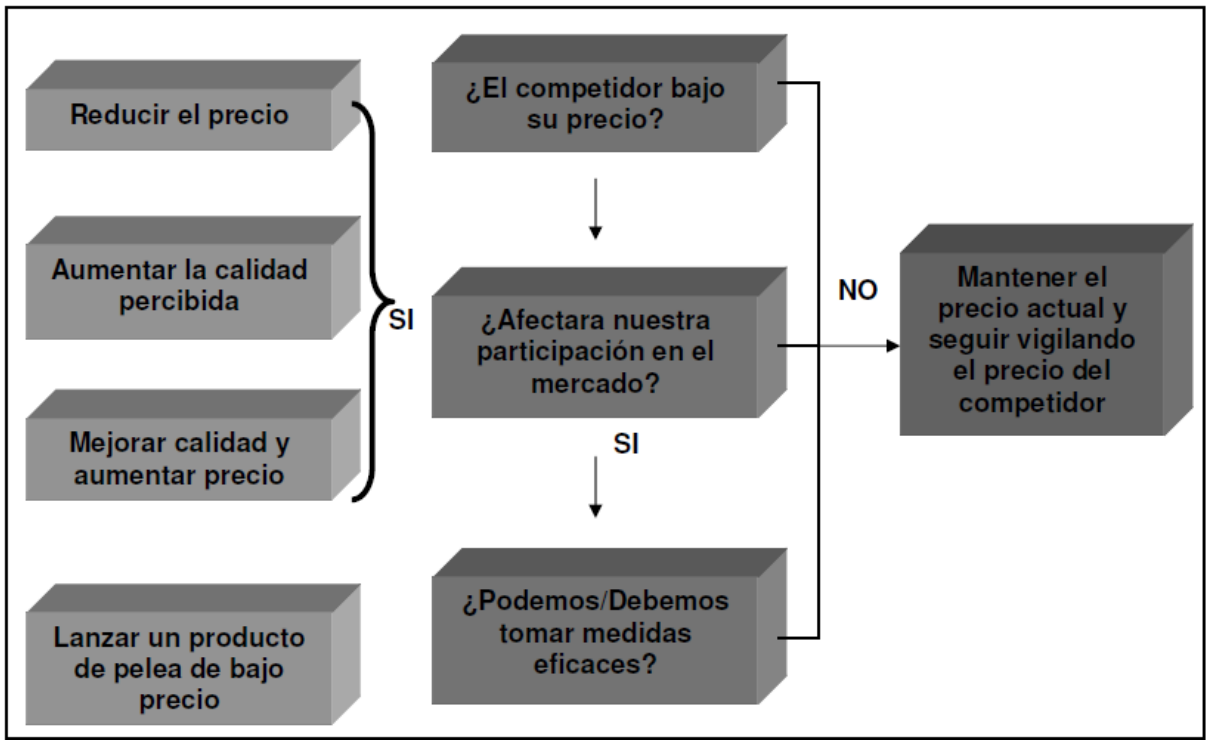


FIGURA 7. 2 Factores que afectan en el cambio de precio

Fuente Propia. (2010)

7.3 ANÁLISIS DE COSTOS

Tomando en cuenta el desarrollo del dispositivo, este puede ser integrado y

empaquetado en una diversidad de productos, los que se pueden comercializar. Como por ejemplo, productos como control de asistencia, control de acceso, sistemas de validación biométrica y autónoma que puede ser integrado en una diversidad de vehículos.

Con la finalidad de estructurar un plan de negocios viable para este desarrollo, se han desarrollado básicamente 1 producto que será comercialmente rentable. Se trata del control de acceso, esta solución será estandarizada y paquetizada para su comercialización, de acuerdo a esto, se estructuró las siguientes tablas de costo que permitirán establecer el margen de venta deseado para cada producto.

TABLA 7. 2 COSTOS CONTROL DE ACCESO

ÍTEM	ESPECIFICACIÓN	UNIDAD	CANTIDAD	COSTO	VALOR
1	Dispositivo biométrico FIM2030	UNIDAD	1	476	476
2	Dispositivo RFID ID-12	UNIDAD	1	105	105
3	Microcontrolador PIC16F877A	UNIDAD	2	11	22
4	DISPLAY LCD 16x2	UNIDAD	2	14	28
5	Teclado matricial 4x4	UNIDAD	2	9	18
6	Microcontrolador PIC16F628A	UNIDAD	1	4	4
7	Elementos electrónicos	VARIOS	1	35	35
8	Caja de proyectos (poliuretano)	UNIDAD	2	5	10
9	Costo de desarrollo y armado	UNIDAD	1	70	70
TOTAL COSTO					**$ 768,00**
MARGEN					% 40
TOTAL MARGEN					$ 307,20
PRECIO DE VENTA					**$ 1075,20**

El margen, para el proyecto, que se estableció luego de realizar el análisis de fijación de precios y el análisis de mercado, los que permiten fijar la estrategia de este negocio, como un producto que se regirá por sus bajos costos y la comparación

con los precios de la competencia relativa. De acuerdo a este sistema se pudo establecer este margen, apuntando a la venta de alto volumen.

Con la finalidad de establecer la rentabilidad de estos productos, es necesario aplicar ciertos criterios y herramienta que permitan validar el negocio en que se está incurriendo con el desarrollo de tecnología biométrica. Para el producto se ha aplicado dos indicadores, como son el VAN y el TIR, que permiten de alguna manera estimar y pronosticar la rentabilidad del negocio.

De acuerdo a la siguiente tabla de inversión inicial, se puede evaluar estos indicadores para el producto de control de acceso.

TABLA 7. 3 INVERSIÓN INICIAL PARA EL CONTROL DE ACCESO

RUBRO	VALOR USD.
EQUIPOS	768,00
CAPITAL DE TRABAJO	1.794,10
INVERSIÓN PUBLICITARIA	1.000,00
GASTOS DE CONSTITUCIÓN	800,00
EQUIPOS DE COMPUTACIÓN	700,00
OTROS COSTOS PREINV.	535,00
TOTAL	**5.597**

TABLA 7. 4 FINANCIAMIENTO DE INVERSIÓN

FUENTE	VALOR	%
CAPITAL PROPIO	5.597	100%
CREDITO		
TOTAL	**5.597**	**100%**

TABLA 7. 5 NOMINA DEL PERSONAL

CARGO	SUELDO NOMINAL	BÁSICO ANUAL	DECIMO TERCERO	DECIMO CUARTO	APORTE IESS	COST. TOTAL ANUAL	CANTIDAD PERSONAS	TOTAL
GERENTE	400	4.992	400	240	448,80	6.081	1	6.081
TÉCNICO	300	3.792	300	240	336,60	4.669	1	4.669
TOTAL		**8.784**	**700**	**480**	**785**	**10.749**	**2**	**10.749**

Estimando una producción a 10 años se obtiene:

TABLA 7. 6 PROYECCIÓN DE PRODUCCIÓN DEL CONTROL DE ACCESO

AÑO	CANTIDAD	PRECIO	AÑO	VALOR
0	25	1.070	**0**	
1	25	1.070,00	**1**	26.750
2	50	1.070,00	**2**	53.500
3	65	1.159,13	**3**	75.114
4	85	1.255,69	**4**	105.460
5	110	1.360,29	**5**	148.066
6	143	1.473,60	**6**	207.885
7	186	1.596,35	**7**	291.870
8	241	1.729,32	**8**	409.785
9	314	1.873,38	**9**	575.339
10	408	2.029,43	**10**	807.775,00

Precio calculado según la inflación anual (abril 2009/abril 2010) dada por el banco central en su página virtual:
http://www.bce.fin.ec/resumen_ticker.php?ticker_value=inflacion

Fuente: Propia. (2010)

TABLA 7. 7 CALCULO DE LA TASA INTERNA DE RETORNO PARA EL CONTROL DE ACCESO

	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5	AÑO 6	AÑO 7	AÑO 8	AÑO 9	AÑO 10
FUENTES											
CAP.PROPIO	5.597										
ING. POR VTAS	-	26.750	53.500	75.344	106.106	149.427	210.437	296.356	417.356	587.758	827.734
VALOR RESCATE	-	-	-	-	-	-	-	-	-	-	1.868
SALDO ANTERIOR		1.794	12.174	38.951	78.966	137.823	223.434	346.789	523.792	776.624	1.136.544
TOTAL FUENTES	5.597	28.544	65.674	114.295	185.071	287.250	433.871	643.145	941.148	1.364.382	1.966.145
USOS											
GASTOS DE NOMINA		10.749	11.645	12.615	13.665	14.804	16.037	17.373	18.820	20.388	22.086
GASTOS DE ADM. Y SERVICIOS		15	15	15	15	15	15	15	15	15	15
PROVISIÓN IMPREVISTOS	-	134	268	377	531	747	1.052	1.482	2.087	2.939	4.139
TOTAL USOS		10.898	11.928	13.007	14.211	15.566	17.104	18.870	20.922	23.342	26.240
SALDO FUENTES - USOS	**1.794,10**	**17.646**	**53.747**	**101.288**	**170.860**	**271.684**	**416.767**	**624.275**	**920.226**	**1.341.040**	**1.939.905**
SALDO ANTERIOR		1.794	12.174	38.951	78.966	137.823	223.434	346.789	523.792	776.624	1.136.544
Depreciación Activos Fijos		291	291	291	291	291	291	291	291	291	291
Amortizaciones		467	467	467	467	467					
UTILIDAD		**15.094**	**40.815**	**61.579**	**91.136**	**133.103**	**193.042**	**277.196**	**396.143**	**564.125**	**801.203**
Participación Trabajador (15%)		2.264	6.122	9.237	13.670	19.965	28.956	41.579	59.421	84.619	120.180
UTLIDAD DESPUES DE PART	**-**	**12.830**	**34.693**	**52.342**	**77.466**	**113.138**	**164.086**	**235.616**	**336.721**	**479.506**	**681.022**
Impuesto a la Renta (25%)		3.207	8.673	13.086	19.366	28.284	41.021	58.904	84.180	119.877	170.256
UTILIDAD DESPUES DE IMPUESTO	**1.794**	**9.622**	**26.019**	**39.257**	**58.099**	**84.853**	**123.064**	**176.712**	**252.541**	**359.630**	**510.767**
SALDO DE CAJA	**1.794**	**12.174**	**38.951**	**78.966**	**137.823**	**223.434**	**346.789**	**523.792**	**776.624**	**1.136.544**	**1.647.602**
Inversion Inicial	5.597										
Flujo de efectivo	(5.597)	10.380	26.777	40.014	58.857	85.611	123.355	177.003	252.832	359.921	512.925
TASA INTERNA DE RETORNO	286,33%										

Fuente: Propia. (2010)

TABLA 7. 8 CALCULO DEL VAN PARA EL CONTROL DE ACCESO

FLUJO DE EFECTIVO						
AÑO	**INVERSIÓN**	**COSTOS OPERATIVOS**	**PART. TRABAJADORES**	**IMPUESTO RENTA**	**INGRESOS**	**FLUJO**
0	5.597					(5.597)
1		10.898	2.264	3.207	26.750	10.380
2		11.928	6.122	8.673	53.500	26.777
3		13.007	9.237	13.086	75.344	40.014
4		14.211	13.670	19.366	106.106	58.857
5		15.566	19.965	28.284	149.427	85.611
6		17.104	28.956	41.021	210.437	123.355
7		18.870	41.579	58.904	296.356	177.003
8		20.922	59.421	84.180	417.356	252.832
9		23.342	84.619	119.877	587.758	359.921
10		26.240	120.180	170.256	829.601	512.925
TASA INTERNA DE RETORNO						**286,33%**
VALOR ACTUAL NETO AL 10,00%						**778.196**
RELACIÓN BENEFICIO COSTO						**16,72**

CAPITULO VIII.

CONCLUSIONES

- La realización de un proyecto de desarrollo de esta naturaleza, donde se establecen parámetros y recursos de la industria nacional para desarrollarse y crear bases para la investigación y el desarrollo nacional, genera una gran importancia a la hora de crear conciencia respecto del potencial de desarrollo tecnológico que se pueda generar dentro del ambiente universitario de la ESPE-L.
- El desarrollo de este equipo ha permitido cumplir con todos los objetivos planteados y ha creado una ventaja competitiva que nos permitirá incorporarnos fácilmente al mercado, es decir, que debido a que el desarrollo se realizó en forma local, la posibilidad de crear soluciones a la medida de cada requerimiento es considerablemente alta.
- En cuanto al funcionamiento del equipo, se ha demostrado su alta eficiencia y eficacia a la hora de realizar la identificación de identidad con la huella dactilar. Sus características de funcionamiento y adaptabilidad han creado en este equipo un amplio perfil de negocio, permitiendo crear una variada gama de productos con tecnología biométrica.
- Respecto de las modificaciones mecánicas en el vehículo sobre el cual se instaló el prototipo biométrico debe aclararse que no se hizo imprescindible suspender elementos como el Switch de contacto u otro elemento eléctrico propio del vehículo. Así, el vehículo posee ahora tres modos para la puesta en marcha del motor.
- Desde el punto de vista de la disminución de costos, el potencial de este producto no irá en desmedro de su calidad, es decir, que es comparable a los productos encontrados en el mercado mundial. La ventaja, es que el desarrollo del producto no se verá reflejado en los mismos niveles de margen en el precio de venta final.
- A través de la implementación del sistema de identificación biométrica y automatización del control de puesta en marcha del motor, se ha logrado incrementar el nivel de seguridad en el área automotriz, cumpliendo con el

objetivo de contribuir a la reducción del índice de robo de vehículos.

- El uso del dispositivo de identificación por radiofrecuencia nos ha permitido entender de mejor manera el funcionamiento de los sistemas inmovilizadores. Además de que nos ha permitido crear un sistema muy curioso y único para el control de bloqueo/desbloqueo de las puertas del vehículo, donde no se hace necesario el contacto físico con el vehículo ni tampoco el uso de botones externos. Una de las ventajas de este sistema es que el transponder es de tamaño reducido y cerrado herméticamente, eliminando así el riesgo de daño por condiciones de humedad.
- En cuanto a lo personal, este desarrollo ha permitido que como estudiantes de ingeniería podamos insertarnos en el mundo laboral, creando uno de los departamentos en la empresa más esquivos de la industria nacional, que es el de la investigación y el desarrollo.
- Como resultado de este proyecto y destacando la importancia de los conocimientos entregados durante el proceso de la carrera impartida por la Universidad, como estudiantes hemos podido conocer e involucrarnos en el mundo empresarial y tomando el lema de la Universidad hemos emprendido el desafío de convertirnos en los lideres en innovación tecnológica.

RECOMENDACIONES

- Debe tenerse en cuenta en todo momento las características eléctricas de los dispositivos, puesto que al ser equipos de identificación de alta precisión manejan rangos de corriente y voltaje de solo hasta un % 5 del valor nominal.
- Debe cuidarse que la batería del vehículo se encuentre en buenas condiciones, y que el sistema de carga opere en condiciones óptimas para evitar desabastecimiento de energía hacia el identificador biométrico.
- Previo a la instalación de los dispositivos debe revisarse el sistema eléctrico en general, en busca de posibles cortocircuitos que podrían ocasionar daños graves al equipo biométrico.
- Para la ubicación del equipo biométrico debe analizarse previamente condiciones tales como: evitar zonas de excesiva vibración, evitar zonas de flujo de aire caliente, asegurar una fácil accesibilidad, ergonomía y estética, sin dañar las partes originales del vehículo. Aquí deberá considerarse las opciones de posibles tamaños y/o formas que deberá adoptar la carcasa del equipo, para una plena satisfacción del cliente.
- Para la instalación de este equipo en vehículos que poseen inmovilizador deberá presentarse una nueva cartera de opciones, modificando los menús a presentarse en el LCD, ya que en este tipo de vehículos no se puede lograr una automatización total o control de la puesta en marcha del motor prescindiendo del uso de llaves debido a que el sistema inmovilizador viene incorporado en el módulo de inyección y/o trabaja conjuntamente con él. Para este caso, el producto a crearse trabajará como un elemento de seguridad adicional, el cual elevará sustancialmente el nivel de seguridad en el control de acceso del vehículo.

APÉNDICE A

TABLA A. 1 LISTA DE COMANDOS

CONNECTION	CMD_REQUEST_CONNECTION (0x01) CMD_GET_FIRMWARE_VERSION2 (0x04) CMD_GET_DEVICE_INFO (0x05)
MATCHING	CMD_VERIFY_FP (0x11) CMD_IDENTIFY_FP (0x12) CMD_INSTANT_MATCHING (0x15) CMD_GET_TEMPLATE (0x16) CMD_CANCEL (0x17) CMD_INSTNAT_VERIFY (0x18) CMD_INSTNAT_IDENTIFY (0x19)
DATABASE MANAGEMENT	CMD_DELETE_FP (0x22) CMD_DELETE_ALL_FP (0x23) CMD_SET_MASTER (0x24) CMD_LEAVE_MASTER_MODE (0x26) CMD_SET_MASTER_PASSWORD (0x27) CMD_READ_USER_DATA (0x2B) CMD_WRITE_USER_DATA (0x2C) CMD_ERASE_USER_DATA_BLOCK (0x2D) CMD_DELETE_MASTER_PASSWORD (0x2E) CMD_ENTER_MASTER_MODE2 (0x2F) CMD_GET_FP_LIST2 (0x30) CMD_GET_MASTER_LIST2 (0x31) CMD_READ_LOG_DATA 2(0x32) CMD_REGISTER_FP (0x33) CMD_CHANGE_FP (0x34) CMD_ADD_FP (0x35) CMD_GET_FP (0x36) CMD_DELETE_ALL_LOG (0x37)
CONFIGURATION	CMD_SET_SYSINFO (0x4C) CMD_GET_SYSINFO (0x4D) CMD_SAVE_SYSINFO (0x4E) CMD_CHG_NUM_OF_TEMP (0x4F) CMD_SET_DEFAULT_SYSINFO (0x50)
SYSTEM MANAGEMENT	CMD_STATUS_CHECK (0x62) CMD_GET_FP_IMAGE2 (0x63) CMD_UPGRADE_FIRMWARE2 (0x64) CMD_SET_TIME (0x65) CMD_GET_TIME (0x66) CMD_CTL_IO (0x67) CMD_GET_IMAGE_QUALITY (0x68)

FUENTE: EN-FIM-ComProtocol-FIM20XX-v1.75

APÉNDICE B

TABLA B. 1 PAQUETES DE RESULTADOS

PACKET RESULT LIST	
RESULT_SUCCEEDED	0x01
RESULT_FAILED	0x02
RESULT_NOT_MASTER_MODE	0x03
RESULT_USED_ID	0x04
RESULT_INVALID_ID	0x05
RESULT_DB_IS_FULL	0x06
RESULT_NOT_IN_TIME	0x07
RESULT_INVALID_PARAM	0x09
RESULT_EXCEEDED_MASTER_CNT	0x0A
RESULT_OPP_INIT_FAILED	0x0C
RESULT_CANCELED	0x0D
RESULT_ANOTHER_FINGER	0x0E
RESULT_IDLE_STATUS	0x10
RESULT_TOO_LARGE_DATA[1)]	0x11
RESULT_IDENTIFY_TIMEOUT[2)]	0x12
RESULT_DB_ISNOT_EMPTY[3)]	0x13
RESULT_WRONG_TEMP_MODE[3)]	0x14
RESULT_INVALID_DATASIZE[3)]	0x15
RESULT_INVALID_DATA[3)]	0x16

1) Estos resultados sólo son soportados en FIM01-HV, FIM2030 y FIM2040.

2) En FIM01-HV, FIM2030 y FIM2040, este resultado es soportado en el firmware versión 1.13 o superior.

3) En FIM01-HV, FIM2030 y FIM2040, este resultado es soportado en el firmware versión 1.30 o superior.

FUENTE: EN-FIM-ComProtocol-FIM20XX-v1.75

APÉNDICE C

DESCRIPCIÓN DE COMANDOS

C.1 INICIALIZACIÓN

TABLA C. 1 CMD_REQUEST_CONNECTION

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x01	Command	0x01
Param1	X	Param1	RESULT_SUCCEEDED
Param2	X	Param2	Fingerprint Count
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 2 CMD_GET_FIRMWARE_VERSION2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x04	Command	0x04
Param1	X	Param1	RESULT_SUCCEEDED RESULT_CANCELED
Param2	X	Param2	Version Information
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 3 CMD_DEVICE_INFO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x05	Command	0x05
Param1	X	Param1	RESULT_SUCCEEDED RESULT_CANCELED
Param2	X	Param2	Device Name 0x00 – Reserved for old device 0x01 – Reserved for old device 0x02 – FIM10_HV 0x03 – FIM10_LV 0x04 – FIM01_HV 0x13 – FIM1030 0x33 – FIM2030 0x34 – FIM2040 0x3030 – FIM3030
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

C.2. COMPARACIÓN

TABLA C. 4 CMD_VERIFY_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x11	Command	0x11
Param1[1)]	0 – FP verification 1 – Password	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_INVALID_ID RESULT_INVALID_PARAM RESULT_NOT_IN_TIME RESULT_CANCELED
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	**IF** (Param1 == Succeeded) **IF** (Command Param1 = 0) Template Index Number **ELSE** 0 **ELSE** 0
Data Size	**IF** FP verification Size (a fraction of FPID) **ELSE IF** password Size (a fraction of FPID + password) **ELSE** 0	Data Size	0
Error Code	X	Error Code	Error Code
Data	**IF** (Param1 == 0) A fraction of FPID **ELSE IF** (Param1 == 1) A fraction of FPID + password **ELSE** -	Data	-

TABLA C. 5 CMD_IDENTIFY_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x12	Command	0x12
Param1	0 – User ID only request 1 – User ID and Template index request (FIM01 & FIM20 only)	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_IN_TIME RESULT_IDENTIFY_TIMEOUT (FIM01 & FIM20xx only) RESULT_CANCELED
Param2	X	Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)
Data Size	0	Data Size	**IF** (Param1 == Succeeded) **IF** (Command Param1 = 0) Size of FPID (various between devices) **ELSE IF** (Command Param1 = 1) Size of (FPID + Template Index) **ELSE** 0 **ELSE** 0
Error Code	X	Error Code	Error Code
Data	-	Data	**IF** (Param1 == Succeeded) **IF** (Command Param1 = 0) FPID **ELSE IF** (Command Param1 = 1) (FPID + Template Index) **ELSE** 0 **ELSE** 0

TABLA C. 6 CMD_INSTANT_MATCHING

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x15	Command	0x15
Param1	0 - Default 1 - FDA01 compatible style (FIM10 only)	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_INVALID_PARAM RESULT_TOO_LARGE_DATA RESULT_CANCELED
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	X
Data Size	Size (A fraction of Template)	Data Size	0
Error Code	X	Error Code	Error Code
Data	A fraction of Template	Data	-

The value '1' of param1 is supported in FIM10 firmware ver1.10 or later.

TABLA C. 7 CMD_GET_TEMPLATE

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x16	Command	0x16
Param1	0 - Default 1 - FDA01 compatible style (FIM10 only)	Param1	RESULT_SUCCEEDED RESULT_FAILELD RESULT_NOT_IN_TIME RESULT_CANCELED
Param2	X	Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)
Data Size	0	Data Size	**IF** (Param1 == Succeeded) Size (A fraction of Template) **ELSE** 0
Error Code	X	Error Code	Error Code
Data	-	Data	**IF** (Param1 == Succeeded) A fraction of Template **ELSE** -

The value '1' of param1 is supported in FIM10 firmware ver1.10 or later.

TABLA C. 8 CMD_CANCEL

COMMAND PACKET		ACKNOWLEDGEMENT PACKET[1)]	
Command	0x17	Command	0x17
Param1	X	Param1	RESULT_IDLE_STATUS
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error Code

TABLA C. 9 CMD_INSTANT_VERIFY

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x18	Command	0x18
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_INVALID_PARAM RESULT_INVALID_ID RESULT_TOO_LARGE_DATA RESULT_CANCELED

Param2	(Packet Index (0~N) << 8)
	+ (Max Packet Index N)
		Param2	IF (Param1 == Succeeded)
			Template Index Number
			ELSE
			0

Data Size	Size (A fraction of FPID + Template)	Data Size	0
Error Code	X	Error Code	Error Code
Data	A fraction of FPID + Template	Data	-

TABLA C. 10 CMD_INSTANT_IDENTIFY

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x19	Command	0x19
Param1	0 – User ID only request 1 – User ID and Template index request (FIM01 & FIM20 only)	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_IDENTIFY_TIMEOUT RESULT_INVALID_PARAM RESULT_TOO_LARGE_DATA RESULT_CANCELED
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	X

Data Size	Size (A fraction of Template)	Data Size	IF (Param1 == Succeeded)
			IF (Command Param1 = 0)
			Size of FPID (various between devices)
			ELSE IF (Command Param1 = 1)
			Size of (FPID + Template Index)
			ELSE
			0
			ELSE
			0

Error Code	X	Error Code	Error Code

Data	A fraction of Template	Data	IF (Param1 == Succeeded)
			IF (Command Param1 = 0)
			FPID
			ELSE IF (Command Param1 = 1)
			(FPID + Template Index)
			ELSE
			0
			ELSE
			0

C.3 MANEJO DE LA BASE DE DATOS

TABLA C. 11 CMD_DELETE_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x22	Command	0x22
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA REAULT_INVALID_ID RESULT_NOT_MASTER_MODE
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	**IF** (Param1 == Succeeded) Registered FP Count **ELSE** 0
Data Size	Size (A fraction of FPID)	Data Size	0
Error Code	X	Error Code	Error Code
Data	A fraction of FPID	Data	-

TABLA C. 12 CMD_DELETE_ALL_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x23	Command	0x23
Param1	0 – Delete all FP 1 – Delete all user (except Master) 2 – Delete all Master	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_MASTER_MODE RESULT_CANCELED
Param2	X	Param2	Registered FP count
Data Size	0	Data Size	0
Error Code	X	Error Code	Error Code

TABLA C. 13 CMD_SET_MASTER

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x24	Command	0x24
Param1	0 – Clear Master Flag 1 – Set Master Flag	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_INVALID_PARAM REAULT_INVALID_ID RESULT_NOT_MASTER_MODE RESULT_EXCEEDED_MASTER_CNT
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	Master Count
Data Size	Size (A fraction of FPID)	Data Size	0
Error Code	X	Error Code	Error Code
Data	A fraction of FPID	Data	-

TABLA C. 14 CMD_LEAVE_MASTER_MODE

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x26	Command	0x26
Param1	X	Param1	RESULT_SUCCEEDED RESULT_NOT_MASTER_MODE
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 15 CMD_SET_MASTER_PASSWORD

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x27	Command	0x27
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_MASTER_MODE
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	X
Data Size	Size (A fraction of Password)	Data Size	0
Error Code	X	Error Code	Error code
Data	A fraction of Password	Data	-

TABLA C. 16 CMD_READ_USER_DATA

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x2B	Command	0x2B
Param1	Address	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_MASTER_MODE
Param2	User data length (byte)	Param2	**IF** (Param1 == RESULT_SUCCEEDED) User data length (byte) **ELSE** 0
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) User data length (byte) **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	**IF** (Param1 == RESULT_SUCCEEDED) User data **ELSE** -

TABLA C. 17 CMD_WRITE_USER_DATA

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x2C	Command	0x2C
Param1	Address	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_MASTER_MODE
Param2	User data length (byte)	Param2	X
Data Size	User data length	Data Size	0
Error Code	X	Error Code	Error code
Data	User Data	Data	-

TABLA C. 18 CMD_ERASE_DATA_BLOCK

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x2D	Command	0x2D
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 19 CMD_DELETE_MASTER_PASSWORD

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x2E	Command	0x2E
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 20 CMD_ENTER_MASTER_MODE2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x2F	Command	0x2F
Param1	Master authentication type Master FP = 0 Master password = 1 FDA board password = 2 Null = 3 Master FP from host = 4 Master FP from host (FDA01 style) = 5 (FIM10 only)	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_INVALID_PARAM RESULT_INVALID_ID RESULT_CANCELED
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N)	Param2	Master authentication type Master FP = 0 Master password = 1 FDA board password = 2 Null = 3 Master FP from host = 4 Master FP from host (FDA01 style) = 5 (FIM10 only)
Data Size	**IF** Master FP Size (A fraction of FPID) **ELSE IF** master password Size (A fraction of FPID + Password) **ELSE IF** device board password Size (A fraction of password) **ELSE IF** Master FP from host Size (A fraction of FPID + Template) **ELSE IF** null 0	Data Size	0
Error Code	X	Error Code	Error code
Data	**IF** Master FP A fraction of FPID **ELSE IF** master password A fraction of FPID + Password **ELSE IF** device board password A fraction of Password **ELSE IF** Master FP from host FPID + Template **ELSE IF** null -	Data	-

TABLA C. 21 CMD_GET_FP_LIST2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x30	Command	0x30
Param1	List data selection 0 = User count, ID list 1 = User count	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE RESULT_INVALID_PARAM RESULT_CANCELED
Param2	Packet Index (0~N)	Param2	**IF** (Param1 == RESULT_SUCCEEDED) (Packet Index (0~N) << 8) + (Max Packet Index N) **ELSE** -
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of (a piece of FP list block) **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	A piece of FP list block

TABLA C. 22 CMD_GET_MASTER_LIST2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x31	Command	0x31
Param1	List data selection 0 = Master count, ID list 1 = Master count	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE RESULT_INVALID_PARAM RESULT_CANCELED
Param2	Packet index (0~N)	Param2	**IF** (Param1 == RESULT_SUCCEEDED) (Packet Index (0~N) << 8) + (Max Packet Index N) **ELSE** -
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of (a piece of master list block) **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	A piece of master list block

TABLA C. 23 CMD_READ_LOG_DATA2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x32	Command	0x32
Param1	Log request mode 0 = **Param2** previous log read 1 = oldest unread log 2 = last written log 3 = All log 4 = from oldest unread to last	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE RESULT_INVALID_PARAM RESULT_CANCELED
Param2	**IF Param1** == 0 Nth log **ELSE IF Param1** == 3 Index(0~N) **ELSE IF Param1** == 4 Index (0~N) **ELSE** 0	Param2	**IF** (Param1 == RESULT_SUCCEEDED) (Packet Index (0~N) << 8) + (Max Packet Index N) **ELSE** -
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of a piece of Log data block **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	**IF** (Param1 == RESULT_SUCCEEDED) Size of a piece of Log data block **ELSE** 0

El registro del bloque de datos consiste en el número de registro devuelto, el tamaño de registro, y los datos del registro

Log data block = Log data count (2) + Log data size (2) + Log data size (28) x log data count.

TABLA C. 24 CMD_REGISTER_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x33	Command	0x33
Param1	0 – User 1 – Master Otherwise – Reserved	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_INVALID_PARAM RESULT_USED_ID RESULT_DB_IS FULL RESULT_NOT_MASTER_MODE RESULT_ANOTHER_FINGER RESULT_CANCELED
Param2	Packet index 0x00 – Extract 1st Template from sensor with ID and password 0x10 – Extract 1st Template from sensor with auto-generated ID 0x01 – Extract 2nd Template from sensor & Save 0x02 – Extract 2nd Template from sensor & Save with different finger 0x03 – Extract 3rd Template from sensor (FIM01 & FIM20xx only) 0x04 – Extract 4th Template form sensor & save (FIM01 & FIM20xx only) 0x05 – Extract 4th Template from sensor & save with different finger (FIM01 & FIM20xx only)	Param2	**IF** (Param1 == RESULT_SUCCEEDED) && (((Packet index == 0x01 or 0x02) && (2 templates mode)) || ((Packet index == 0x11 or 0x12) && (4 templates mode))) Registered FP Count (Only valid if succeed) **ELSE** 0
Data Size	**IF** (Packet index == 0) Size of (FPID + Password) **ELSE** 0	Data Size	0
Error Code	X	Error Code	Error Code
Data	**IF** (Packet index == 0) FPID + password **ELSE** 0	Data	-

TABLA C. 25 CMD_CHANGE_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x34	Command	0x34
Param1	0x01 – Change Master Privilege & Save 0x02 – Change Password & Save 0x10 – Change 1st template from host 0x11 – Change 2nd template from host Save 0x12 – Change 2nd template from host with different finger from 1st template Save 0x13 – Change 3rd template from host 0x14 – Change 4th template from host Save in 4 templates mode 0x15 – Change 4th template from host with different finger from 3rd template Save in 4 templates mode 0x20 – Change 1st template from sensor 0x21 – Change 2nd template form sensor Save in 2 templates mode 0x22 – Change 2nd template form sensor with different finger from 1st template Save in 2 templates mode 0x23 – Change 3rd template form sensor 0x24 – Change 4th template from sensor Save in 4 templates mode 0x25 – Change 4th template form sensor with different finger from 3rd template Save in 4 templates mode Others – reserved	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_NOT_IN_TIME RESULT_INVALID_PARAM RESULT_INVALID_ID RESULT_NOT_MASTER_MODE RESULT_CANCELED
Param2	**IF** (Param1 == 0x01) 0 – set to normal user	Param2	X

	1 – set to master **ELSE** Reserved		
Data Size	**IF** (Param2 == 0x02) Size of (FPID + Password) **ELSE IF** (Param2 == 0x10 or 0x11 or 0x12 or 0x13 or 0x14 or 0x15) Size of (FPID + Template) **ELSE IF** (Param2 == 0x01 or 0x20 or 0x21 or 0x22 or 0x23 or 0x24 or 0x25) Size of FPID **ELSE** 0	Data Size	0
Error Code	X	Error Code	Error Code
Data	**IF** (Param1 == 0x02) FPID + password **ELSE IF** (Param1 == 0x10 or 0x11 or 0x12 or 0x13 or 0x14 or 0x15) FPID + Template **ELSE IF** (Param2 == 0x01 or 0x20 or 0x21 or 0x22 or 0x23 or 0x24 or 0x25) FPID **ELSE** 0	Data	-

La función de cambio de identificación de una huella digital diferente es soportado en FIM01 y FIM20xx con firmware versión 1.20 o superior,

El modo de 4 templates es soportado en el firmware versión 1.30 o superior, y valores del 0x13 al 0x15 y del 0x23 a 0x25 en el **Param1** solamente son validos en modo de 4 templates.

TABLA C. 26 CMD_ADD_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x35	Command	0x35
Param1	DB structure version 1 – 2 templates data structure 2 – 4 templates data structure Others – reserved	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_INVALID_PARAM RESULT_USED_ID RESULT_DB_IS_FULL RESULT_NOT_MASTER_MODE RESULT_CANCELED RESULT_WRONG_TEMP_MODE
Param2	(Packet index (0~N) << 8) + (Max Packet Index N)	Param2	X
Data Size	Size (a piece of DB structure)	Data Size	0
Error Code	X	Error Code	Error Code
Data	A piece of DB structure	Data	-

TABLA C. 27 CMD_DELETE_ALL_LOG

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x37	Command	0x37
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE RESULT_CANCELED
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error Code

TABLA C. 28 CMD_GET_FP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x36	Command	0x36
Param1	Get operation 0 – FPID DB 1 – First DB 2 – Next DB Others – reserved	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_INVALID_PARAM RESULT_INVALID_ID RESULT_NOT_MASTER_MODE
			RESULT_CANCELED
Param2	The version of DB structure 1- 2 templates data structure 2- 4 templates data structure Others – reserved	Param2	0
Data Size	**IF** (Param1 == 0) Size of FPID **ELSE** 0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of DB structure **ELSE** 0
Error Code	X	Error Code	Error Code
Data	**IF** (Param1 == 0) FPID **ELSE** -	Data	**IF** (Param1 == RESULT_SUCCEEDED) DB structure **ELSE** 0

El valor 2 en **Param2** (modo de 4 templates) es soportado en el firmware versión 1.30 o superior.

C.4 CONFIGURACIÓN

TABLA C. 29 CMD_SET_SYSINFO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x4C	Command	0x4C
Param1	**SI_Type**	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_MASTER_MODE
Param2	SI_Value	Param2	0
Data Size	0	Data Size	**IF** (Param1 == Succeeded) Size (SI_INFO) **ELSE** 0
Error Code	X	Error Code	Error code
	-		**IF** (Param1 == Succeeded) SI_INFO **ELSE** -

TABLA C. 30 CMD_GET_SYSINFO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x4D	Command	0x4D
Param1	**SI_Type**	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_NOT_MASTER_MODE
Param2	X	Param2	SI_Value
Data Size	0	Data Size	**IF** (Param1 == Succeeded) Size (SI_INFO) **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	**IF** (Param1 == Succeeded) SI_INFO **ELSE** -

TABLA C. 31 CMD_SAVE_SYSINFO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x4E	Command	0x4E
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 32 CMD_CHG_NUM_OF_TEMP

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x4F	Command	0x4F
Param1	Number of Template (2 or 4)	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE RESULT_INVALID_PARAM RESULT_DB_ISNOT_EMPTY
Param2	X	Param2	X
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code

TABLA C. 33 CMD_DEFAULT_SYSINFO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x50	Command	0x50
Param1	0	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_MASTER_MODE
Param2	0	Param2	0
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code
	-		-

C.5 MANEJO DEL SISTEMA

TABLA C. 34 CMD_STATUS_CHECK

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x62	Command	0x62
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED
Param2	X	Param2	STATUS = IDLE (0x00) BUSY (0x01) : Current executed command DB_UPLOADING (0x03) : During power-up operation, a device isn't ready to communicate
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code
Data	-	Data	-

TABLA C. 35 CMD_GET_FP_IMAGE2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x63	Command	0x63
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_NOT_IN_TIME RESULT_CANCELED
Param2	Packet index (0~N)	Param2	**IF** (Param1 == RESULT_SUCCEEDED) (Packet Index (0~N) << 8) + (Max Packet Index N) **ELSE** 0
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of (a piece of image data block) **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	**IF** (Param1 == RESULT_SUCCEEDED) A piece of image data block **ELSE** -

TABLA C. 36 CMD_UPGRADE_FIRMWARE2

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x64	Command	0x64
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_CANCELED
Param2	(Packet Index (0~N) << 8) + (Max Packet Index N-1)	Param2	Command packet param2 value
Data Size	Size of (a fragment of Firmware data block)	Data Size	0
Error Code	X	Error Code	Error code
Data	Firmware data block	Data	-

TABLA C. 37 CMD_SET_TIME

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x65	Command	0x65
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_DATASIZE RESULT_INVALID_DATA RESULT_CANCELED
Param2	X	Param2	0
Data Size	Size of TIME_INFO	Data Size	0
Error Code	X	Error Code	Error code
Data	TIME_INFO	Data	-

TABLA C. 38 CMD_GET_TIME

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x66	Command	0x66
Param1	X	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_CANCELED
Param2	X	Param2	0
Data Size	0	Data Size	**IF** (Param1 == RESULT_SUCCEEDED) Size of TIME_INFO **ELSE** 0
Error Code	X	Error Code	Error code
Data	-	Data	**IF** (Param1 == RESULT_SUCCEEDED) TIME_INFO **ELSE** -

TABLA C. 39 CMD_CTL_IO

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x67	Command	0x67
Param1	Selection of GPIO 0x01 – Sensor LED 0x40 – Relay Channel 0 (FIM01 & FIM20 Only) 0x41 – Relay Channel 1 (FIM01 & FIM20 Only) Others – Reserved	Param1	RESULT_SUCCEEDED RESULT_FAILED RESULT_INVALID_PARAM RESULT_CANCELED
Param2	Value 0 – Low/Off 1 – High/On	Param2	0
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code
Data	-	Data	-

TABLA C. 40 CMD_GET_IMAGE_QUALITY

COMMAND PACKET		ACKNOWLEDGEMENT PACKET	
Command	0x68	Command	0x68
Param1	0	Param1	RESULT_SUCCEEDED RESULT_FAILED
Param2	0	Param2	Quality Value
Data Size	0	Data Size	0
Error Code	X	Error Code	Error code
	-		-

Este comando devuelve la calidad de la imagen después de usar los comandos siguientes.

CMD_VERIFY_FP

CMD_IDENTIFY_FP

CMD_INSTANT_MATCHING

CMD_GET_TEMPLATE

CMD_GET_FP_IMAGE2

CMD_ENTER_MASTER_MODE2

CMD_REGISTER_FP

CMD_CHANGE_FP

Para otros comandos, el valor de calidad de la imagen no es válido.

El rango de calidad es de 0 (calidad baja) a 100 (calidad alta).

AVISO

La ‘X' significa “no hay cuidado”, para que usted pueda enviar algún valor. Pero para la compatibilidad futura, nosotros recomendamos que usted envíe “0”.

BIBLIOGRAFÍA

Angulo Usategui, José María; Angulo Martínez, Ignacio (1998). “Microcontroladores PIC. Diseño práctico de aplicaciones”. McGraw-Hill. Madrid. España. 221 pp.

Carlos A. Reyes “Microcontroladores PIC”. Programación en Basic. 3ra Edición. Volumen 1

Tapiador Mateos, Marino; Sigüenza Pizarro, Juan A. (2005). “Tecnologías Biométricas”. Ra-Ma. Madrid. España. 440 pp.

Wayman, James L. (2000). “Nacional Biometric Test Center Collected Works 1997-2000”. Versión 1.2, San José. California. 277 pp.

Disponible online: http://www.engr.sjsu.edu/biometrics/nbtccw.pdf

SITIOS WEB

Directorio Electrónico de Guatemala (2006).

http://www.deguate.com/infocentros/gerencia/admon/porter.htm

Electronic Frotier Fundation (1990).

http://www.eff.org/Privacy/Surveillance/biometrics/

Jean-Francois Mainguet (2006).

http://perso.orange.fr/fingerchip/biometrics/biometrics.htm

Robotker tecnalia (2005).

http://www.robotiker.com/castellano/index.jsp

Secugen Co. (2006).

http://www.secugen.com

The Biometric Consortium (2005).

http://www.biom etrics.org

UNAM, Estándares de seguridad en la información (2005).

http://enterate.unam.mx/Artculos/2005/febrero/seguridad.htm

Vault Information Service LLC (1997).

http://www.8052.com/tutorial.phtml

Wayman, James L. Biometric Technology Testing (2000).

http://www.engr.sjsu.edu/biometrics/publications.html

ANEXOS

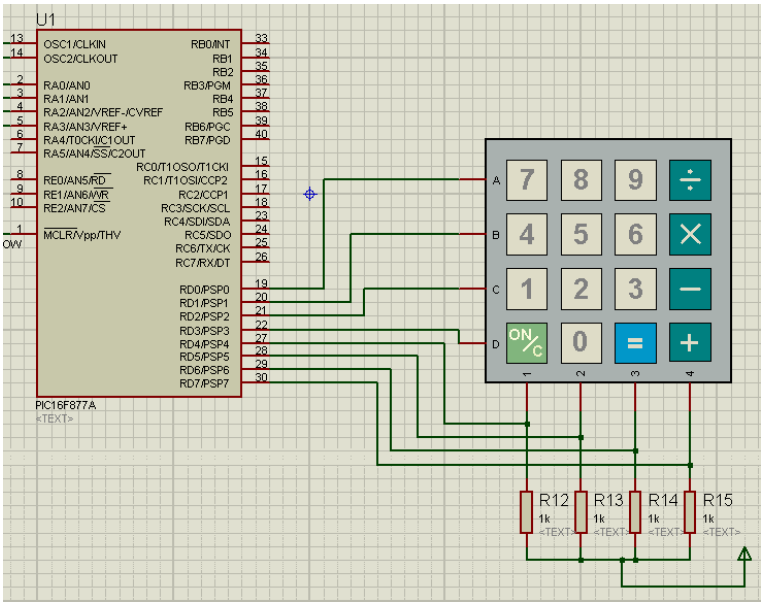


Diagrama de conexión de teclado

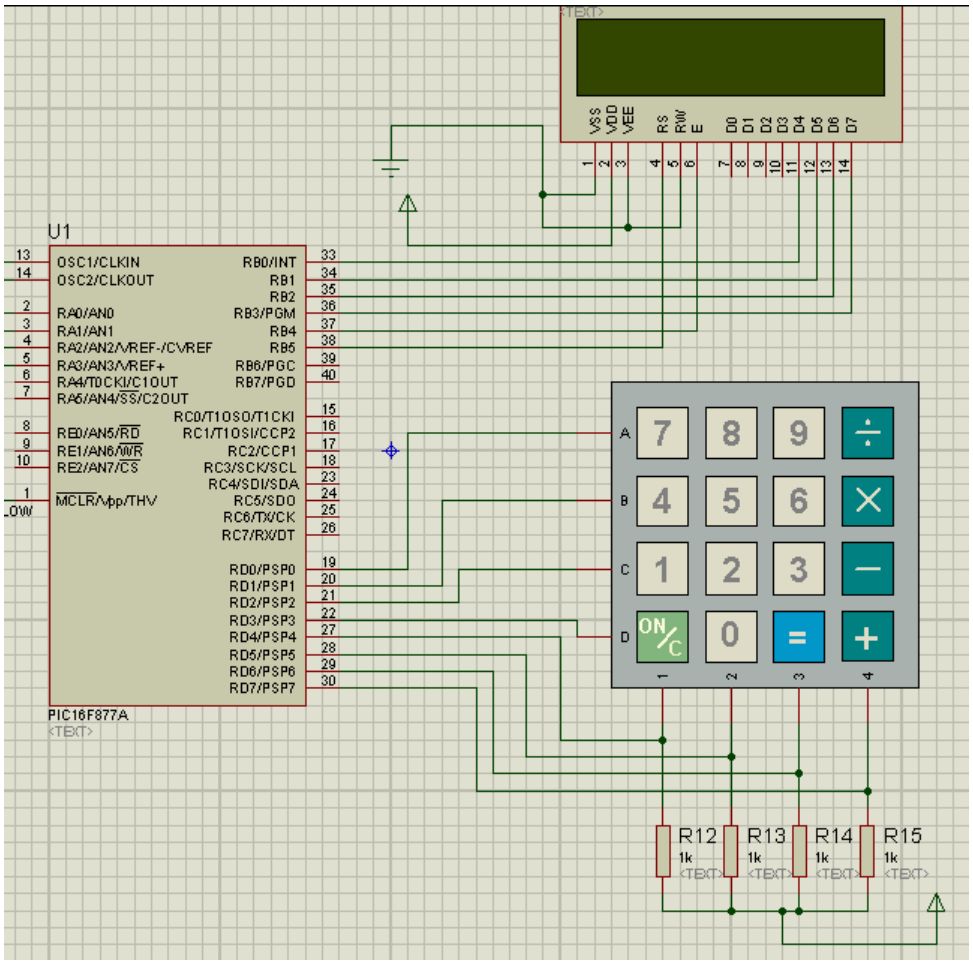


Diagrama de conexión del visor

Fuente: Propia (2010)

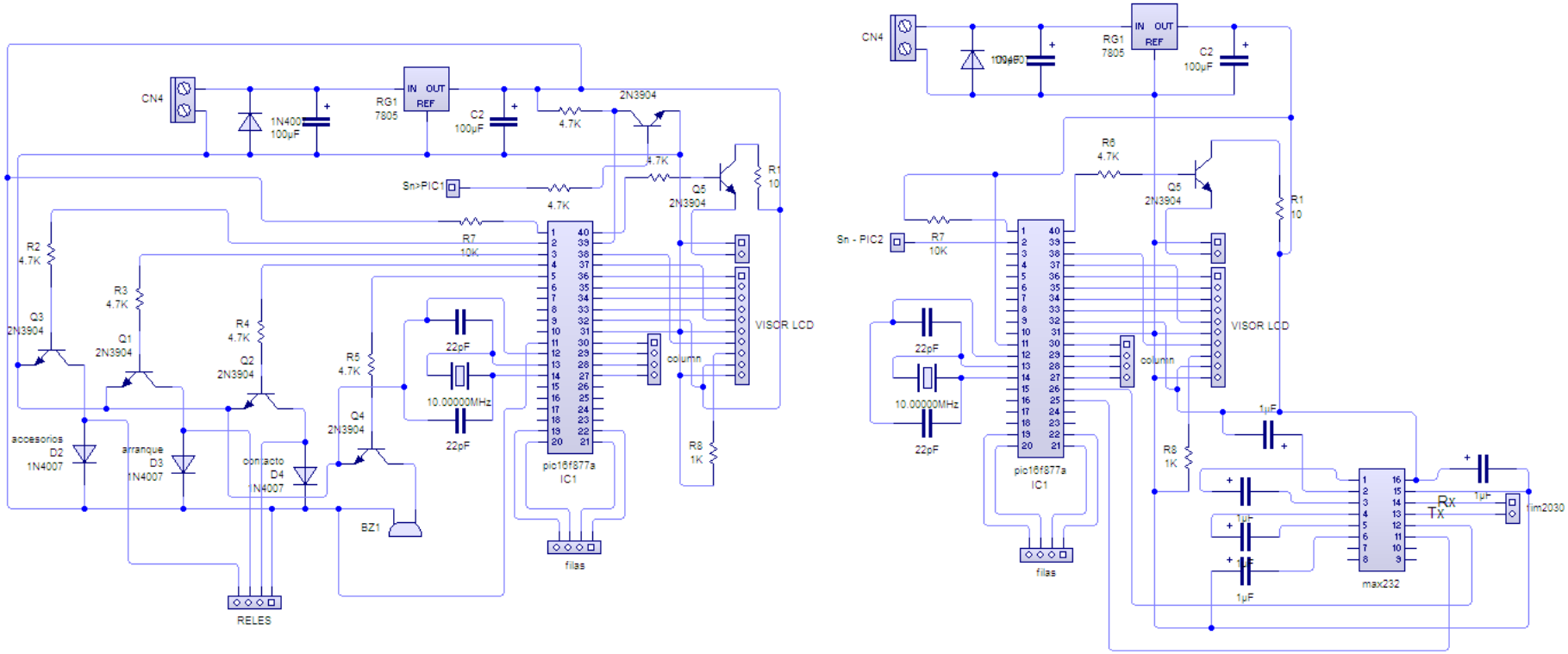
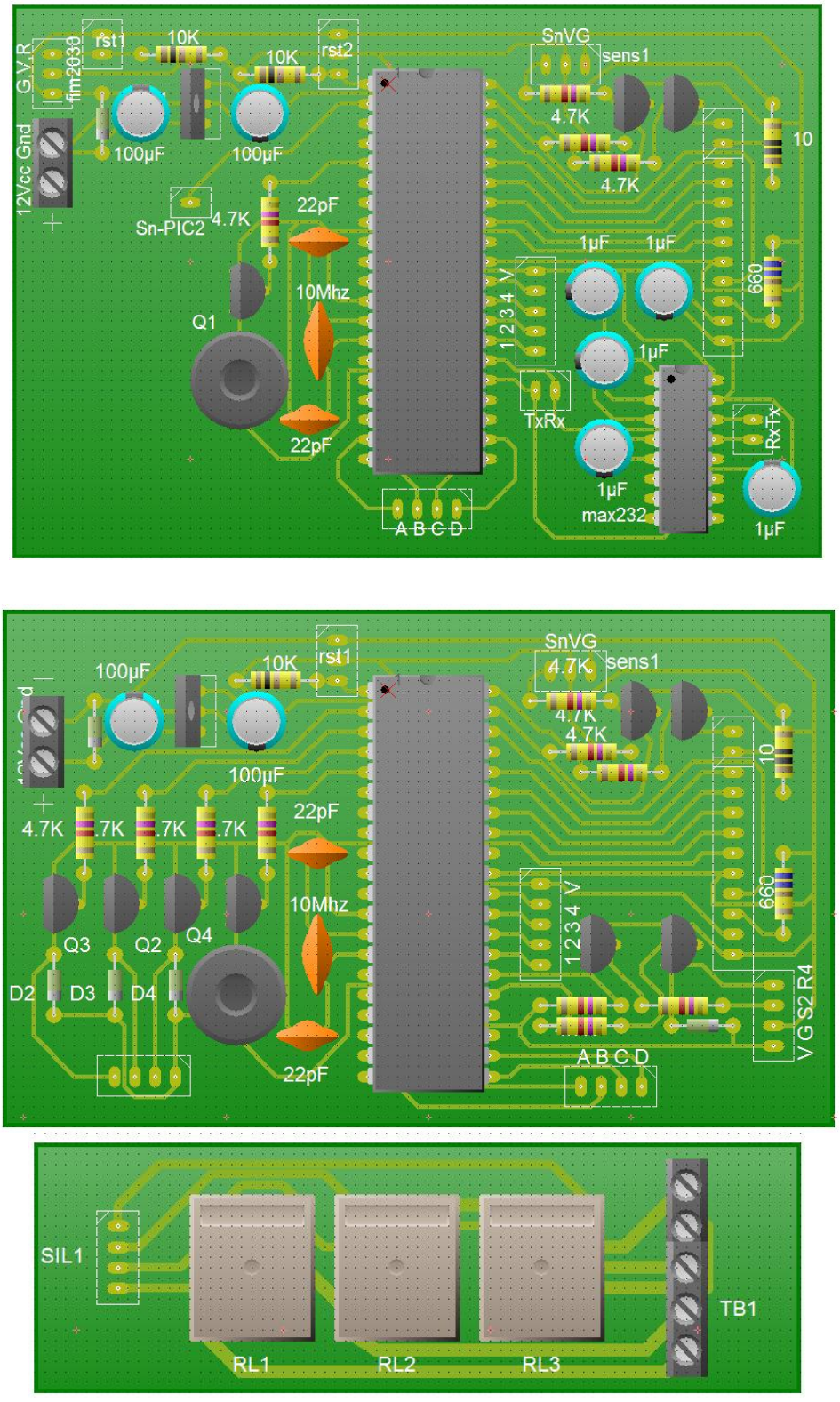


Diagrama completo de conexión

Fuente: Propia LIVEWIRE (2010).



Circuitos de control de dispositivos

Fuente propia PCB WIZARD (2010)

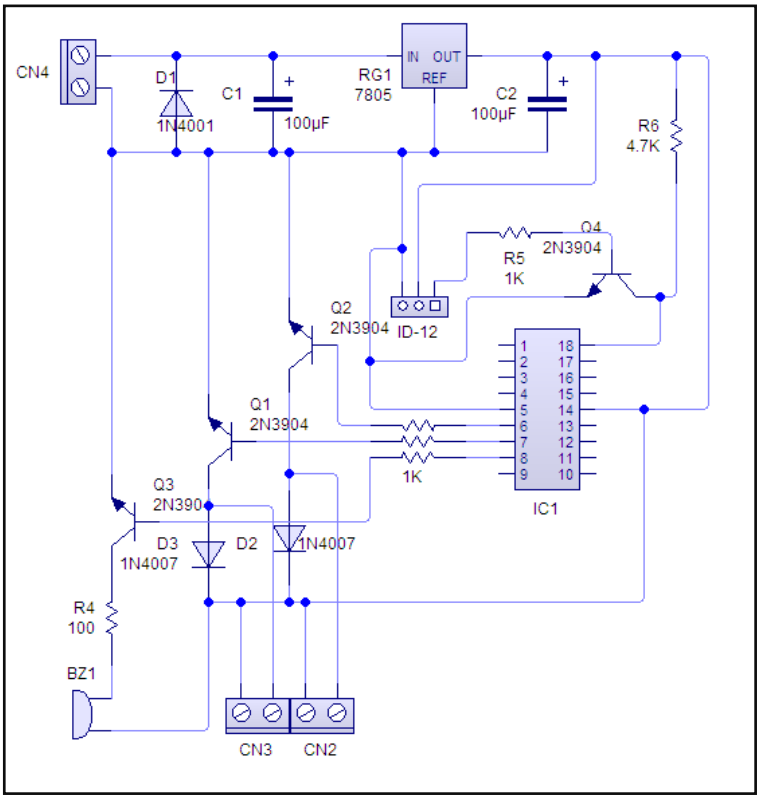
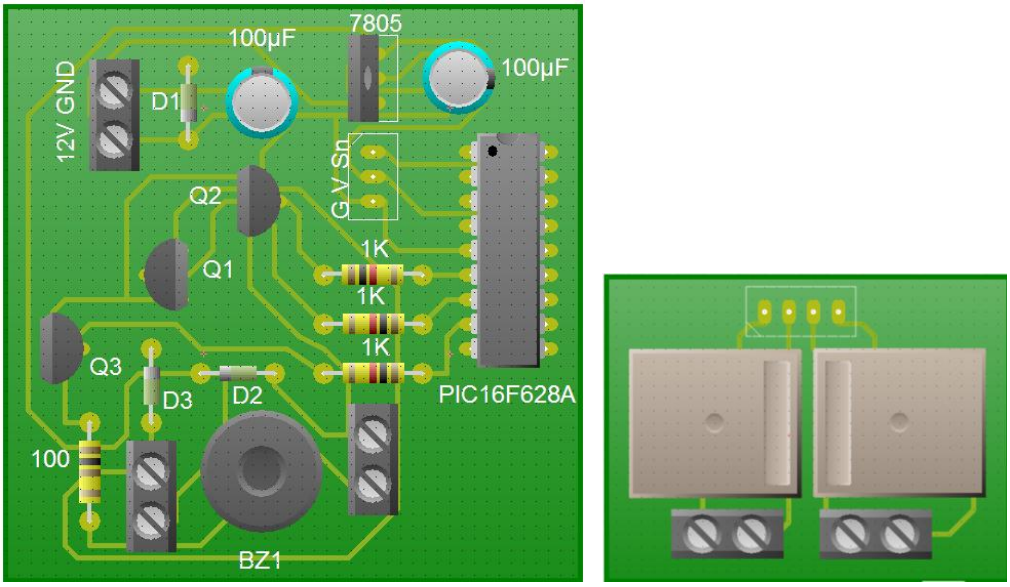


Diagrama de conexión del control de apertura de puertas



Circuito de control de acceso con ID-12 y Pic16F628A

Fuente: Propia (2010)