ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"DISEÑO Y CONSTRUCCIÓN DE SISTEMAS DE SEGURIDAD Y CONTROL DE ACCESO MEDIANTE MICROCONTROLADORES PARA EL COLEGIO FERNANDO DAQUILEMA"

TÉSIS DE GRADO

Previa a la obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

PALACIOS SAMPEDRO LUIS GUSTAVO

TORRES LOZADA ANGÉLICA MARICELA

RIOBAMBA - ECUADOR

2011

A mi madre por guiarme positivamente durante mi formación personal y profesional, a mi familia por brindarme el calor de hogar, y a mi esposa por ser mi compañera en donde me refugio.

Luis.

A Dios, por todo lo que me ha dado.

A mis padres, por estar con migo en los momentos difíciles y por creer en mí.

A mis angelitos, que me dejaron las más grandes enseñanzas de vida y quienes desde el cielo me protegen.

A mi esposo, por acompañarme en este gran camino brindándome su cariño y fuerza para seguir adelante.

A mi hijo, que ha llegado a alegrar mi vida y por ser mi más grande motivación.

Angélica.

Dedico el presente trabajo a mi madre porque gracias a su esfuerzo culmino exitosamente mis estudios, a mi esposa y a nuestro hijo que con su presencia nos llena de felicidad, y a mis profesores que supieron compartir sus conocimientos durante la vida estudiantil

Luis.

A mi familia, amigos y maestros ya que siempre estuvieron a mi lado y contribuyeron en mi formación profesional y personal.

Angélica.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes DECANO FACULTAD INFORMATICA Y ELECTRÓNICA	_____	_____
Ing. Pedro Infante DIRECTOR DE LA ESCUELA DE TELECOMUNICACIONES Y REDES	_____	_____
Ing. Paul Romero DIRECTOR TESIS	_____	_____
Ing. Franklin Moreno MIEMBRO TRIBUNAL	_____	_____
Lcdo. Carlos Rodriguez DIRECTOR DEL DPTO DE DOCUMENTACIÓN	_____	_____
NOTA DE LA TESIS	_____	

“Nosotros Palacios Sampedro Luis Gustavo y Torres Lozada Angélica Maricela, somos responsables de las ideas, doctrinas y resultados expuestos en esta Tesis, y el patrimonio intelectual de la Tesis de Grado pertenecen a la Escuela Superior Politécnica de Chimborazo”.

_____ _____

Palacios Sampedro Luis Gustavo Torres Lozada Angélica Maricela

INDICE DE ABREVIATURAS

ADSL	Asymmetric Digital Subscriber Line
	(Línea de Abonado Digital Asimétrica)
AFAS	Automatic Fingerprint Authentication System
	(Sistema Automático de Verificación por huellas Digitales)
ARES	Advanced Routing and Editing Software
	(Software de Edición y Ruteo Avanzado)
CCD	Charge Coupled Device
	(Dispositivo de carga acoplada)
CPU	Unidad central de procesamiento
DMTF	Dual Tone Multifrecuency
	(Marcación de Tonos Multifrecuencia)
EEPROM	Electrically Erasable Programmable Read Only Memory
	(Memoria Solo de Lectura Programable Borrable Electricamente)
EPROM	Erasable Programmable Read Only Memory
	(Memorias Sólo de Lectura Programable Borrable)
GSM	Global System for Mobile communications
	(Sistema Global Para las Comunicaciones Móviles)
ISIS	Intelligent Schematic Input System
	(Sistema de Enrutado de Esquemas Inteligente)
LCD	Liquid Crystal Display
	(Pantalla de Cristal Liquido)
LED	Ligh Emitting Diode
	(Diodo Emisor de Luz)
N.A	Normalmente Abierto
N.C	Normalmente Cerrado
NIP	Número de Identificación Personal

OTP	One Time Programable
	(Programable una sola vez)
PCB	Pinted Circuit Board
	(Tarjeta de Circuito Impreso)
PIR	Passive Infra Red
	(Infrarrojo Pasivo)
RAM	Random Access Memory
	(Memoria de Acceso Aleatorio)
ROM	Read Only Memory
	(Memoria de solo lectura)
RTB	Red Telefónica Básica
TCI	Tarjeta con Circuito Integrado
VCC	Voltaje de Corriente Continua
VCD	Voltaje de Corriente directa
VSM	Virtual System Modelling
	(Sistema Virtual de Modelado)
µC	Microcontrolador

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

MARCO REFERENCIAL

1.1 INTRODUCCIÓN

En el presente documento se detallará el diseño y construcción de los sistemas de seguridad y control de acceso, para esto se desarrollará programas que serán grabados en los microcontroladores, conjuntamente se analizarán las señales provenientes de los diferentes sensores, generando una respuesta eficiente a cada evento que se controle.

Las partes principales que se analizarán son: Elementos que intervienen en el sistema de seguridad con monitoreo, esto se lo realizará a través de la red telefónica, programación de microntroladores. Control de acceso, basado en sistemas biométricos exclusivamente en detectores de huelas dactilares. Así como las diferentes aplicaciones y circuitos imprentados en las diferentes etapas de los mencionados sistemas.

1.2 ANTECEDENTES

Los sistemas de seguridad han ido evolucionando conforme se van desarrollando nuevas tecnologías y los usuarios exigen mejores soluciones a sus problemas, con menor tiempo de respuesta, con mayor eficiencia y un mínimo de fallas. Hay una gran variedad, pueden encontrarse desde sencillos dispositivos, para una seguridad poco compleja, hasta edificios inteligentes en donde dispositivos son capaces de tomar decisiones.

La exigencia de seguridad depende de las necesidades existentes en el área a proteger, es por esto que las empresas que se dedican a brindar estos servicios, han desarrollado seguridad, tanto en forma tradicional como con tecnología de punta.

En los últimos años se ha venido desarrollando sistemas de seguridad con monitoreo, es decir que su inspección se lo puede realizar estando a grandes distancias del área protegida, para este control se puede utilizar la red telefónica publica, mediante internet utilizando el protocolo TCP/IP, ondas electromagnéticas entre otras. Con esta tecnología se eleva el nivel de confianza de los usuarios, es por esta razón que hoy en día 8 de cada 10 personas en el mundo, poseen estos sistemas, ya sea para sus autos, negocios, viviendas, etc.

De la misma manera, se ha buscado procedimientos sofisticados para permitir el ingreso de una persona a una zona determinada de manera automática, encontrando en los sistemas biométricos el método más seguro para permitir el acceso. Estos métodos eran exclusivamente utilizados por instituciones forenses y/o gubernamentales como consecuencias de los enormes costos que involucraba esta tecnología, totalmente cerrada a personas e instituciones civiles, pero el énfasis en el crecimiento de la identificación automática de personas basadas en sus huellas dactilares hace que este sistema sea cada vez más accesibles, esta es la alternativa más consolidada y fiable contemporáneamente, siendo utilizados ampliamente en los sistemas de control de acceso elevando el nivel de seguridad al permitir el ingreso a una persona.

1.3 JUSTIFICACIÓN

El colegio Fernando Daquilema de la ciudad de Riobamba, ha realizado la adquisición de equipos tecnológicos, invirtiendo un alto presupuesto, por lo cual necesita elevar el nivel de seguridad en las áreas donde se encuentran dichos equipos, ya que estas están protegidos por candados en las puertas, y al ser manipulados o violentados dichos objetos se puede romper la poca confiabilidad que brindan. Para elevar el nivel de protección se va a realizar el diseño e implementación del sistema de seguridad con microcontrolador, constando de sensores ubicados en lugares estratégicos y monitoreo a través de la red telefónica. Con este sistema el colegio obtendrá beneficios como son: elevar el nivel de seguridad en el área vulnerable, monitoreo atreves de RTB, incrementar la confianza de protección en las autoridades de la institución.

Adicionalmente el colegio tiene documentación importante, que se encuentra dentro del área administrativa exclusivamente en el rectorado, a la cual accede fácilmente personal autorizado o no. Para tener una inspección se va a desarrollar el Sistema de Control de Acceso con microcontroladores. El control se lo realizara mediante el ingreso de un NIP (número de identificación personal), y la verificación de autenticidad por sistema biométrico basado en detección de huellas dactilares. Los benéficos que se obtendrá con este sistema son: control de acceso solo a personas autorizadas, mayor seguridad en la documentación que se encuentra al interior.

Los sistemas están desarrollados con tecnología que ofrecerá confiabilidad, durabilidad y rapidez de respuesta, presentando una interfaz amigable para el usuario, sin descuidar la protección contra personas que manipulen los sistemas, para fines ajenos de los cuales fueron diseñados.

La seguridad electrónica ya no es un lujo sino una necesidad.

1.4 OBJETIVOS

Objetivo General

- Diseñar y construir sistemas de seguridad y control de acceso mediante microcontroladores para el colegio Fernando Daquilema.

Objetivos Específicos

- Estudiar el funcionamiento de los componentes electrónicos que forman parte del sistema de seguridad y control de acceso
- Diseñar el sistema de seguridad y control de acceso
- Implementar la interfaz electrónica de cada sistema
- Realizar la programación del software para los sistemas
- Verificar del funcionamiento del sistema de seguridad y control de acceso

1.5 HIPÓTESIS

Mediante la implementación del proyecto se contribuirá a tener las áreas relevantes protegidas contra personas no autorizadas, además permitirá que el personal debidamente autentificado pueda ingresar a las áreas donde se encuentra la documentación importante del colegio Fernando Daquilema de la ciudad de Riobamba.

CAPÍTULO II

FUNDAMENTO TEÓRICO

INTRODUCCIÓN

En este capítulo se detallará el funcionamiento de los sistemas y los componentes que intervienen en cada uno de ellos, se analizará en detalle las características de los dispositivos electrónicos principales para poder implementar cada sistema.

De la misma manera se especificará las generalidades de los microcontroladores y los programas utilizados para la manipulación de los mismos.

2.1SISTEMA DE SEGURIDAD

Sistema de seguridad son varios dispositivos ubicados estratégicamente en el área protegida para detectar, intrusión, presencia, o invasión de un extraño que no disponga de acceso permitido a dicho lugar.

2.1.1 DESCRIPCIÓN DE SISTEMAS SEGURIDAD

El sistema de seguridad electrónico se divide en tres partes:

1. Detección (Sensores)
2. Procesamiento (Central)
3. Respuesta (Luces, sirena, monitoreo, actuadores, etc)

1. Detección

a) Interior. Se logra básicamente con detectores de movimiento.

b) Perimetral. Con sensores magnéticos de apertura. También pero en menos medida se utilizan detectores de rotura de vidrios y barreras infrarrojas.

Una protección ideal es la que utiliza a+b

Si se realiza la protección sólo con sensores interiores, la respuesta se producirá cuando el intruso ya está adentro de la propiedad y si el lugar es una casa habitada, estas áreas de detección no podrán funcionar cuando haya gente en el lugar, con lo que sólo se protege el lugar cuando no hay nadie.

Si se protege sólo con sensores perimetrales, si algún intruso intenta ingresar la respuesta será instantánea, pero si no hay nadie en el lugar y la apertura o vidrio quedó abierto o roto, en el supuesto de un segundo intento el perímetro no detectará porque ya fue violado.

Con la utilización apropiada de los dos sistemas se eliminan los riesgos cruzados de ambos por separado porque un sistema cubre las deficiencias del otro.

2. Procesamiento

Para esto se dispone de una central de alarma, la cual procesa las señales recibidas activando los actuadores, preferentemente debe instalarse en un lugar oculto, y por lo menos un teclado para su comando de donde se activa, desactiva y maneja el sistema.

La central de alarma deberá tener una batería de gel libre de mantenimiento con autonomía suficiente por si hay corte de luz.

El tipo de central debe ser microprocesada y tener un discado telefónico automático

Si se trata de un pequeño comercio o una casa pequeña con una entrada, bastará con un solo teclado instalado en la entrada, cerca de la puerta. Por el contrario, si la propiedad es de varias plantas y tiene entrada de servicio independiente, deberá contarse con un teclado en el área segura cercana al dormitorio donde, en caso de asalto, las personas puedan encerrarse para esperar la respuesta y ayuda.

3. Respuesta

Es lo que le da sentido a todo lo anterior, en caso de que el sistema ha sido alterado en respuesta se procederá a encender actuadores que informaran mediante sonidos, iluminación, llamadas etc, la activación del sistema.

Finalmente, **el monitoreo es lo que transforma una instalación de alarma en un sistema de seguridad**, ya que en caso de alarma no sólo sonará la sirena en el lugar protegido, sino que

además, en forma instantánea y automática, la central de monitoreo recibirá la señal, dando aviso a la policía y a las personas que el propietario haya designado para cada caso.

El monitoreo no sólo es el apoyo fundamental para una alarma de robo, sino que es la única solución para contrarrestar los efectos de intentos de asalto, incendio, emergencia médica, inundación, etc.

Monitoreo es el proceso que permitirá dar notificación que el sistema se ha activado por la presencia de personal no autorizado

2.1.2 FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD

El sistema tiene conexiones de entrada para recibir las señales providentes de los diferentes sensores, conexiones de salida que son los que se ocupan de realizar acciones disuasorias, advertencia, automatización etc.

Cuando el sistema empieza a funcionar, este inicia varias acciones en forma automática. Por ejemplo si se detecta la intrusión de una persona en un área determinada, se activara una sirena y se procederá a realizar una llamada de emergencia a uno o varios números de teléfono. Si se detecta la presencia de humo, calor o ambos, envía mensaje telefónico o acciona la apertura de rociadores ubicados en lugares estratégicos, para que apaguen el fuego. Si se detecta la presencia de agentes tóxicos en un área, se procederá a cerrar las puertas para que no se expanda el problema, estos ejemplos nos ayuda a comprender el funcionamiento del sistema.

Uno de los usos más difundidos de un sistema de seguridad es advertir el allanamiento en una vivienda o inmueble, locales comerciales. Los equipos de alarma pueden estar conectados con una Central Receptora, también llamada Central de Monitoreo, con el propietario mismo (a través de teléfono o TCP/IP) o bien simplemente cumplir la función disuasoria, activando una sirena. Para la comunicación con una Central Receptora de Alarmas, se necesita de un medio de comunicación, como pueden serlo: una línea telefónica RTB o una línea GSM (celular), mediante transmisión

TCP/IP que utiliza una conexión de banda ancha ADSL y últimamente servicios de Internet por cable Modem.

2.2 SISTEMA DE ALARMA

Un sistema de alarma es un elemento de alerta pasiva. Esto significa que no evitan una intrusión, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles intrusos. Son capaces además de reducir el tiempo de ejecución de la invasión, reduciendo así las pérdidas.

La necesidad de controlar el ingreso de personas no autorizadas en algún lugar determinado es la base de la existencia de estos equipos, los cuales mantienen la seguridad en comercios, oficinas, industrias, almacenes, laboratorios, etcétera. La instalación de los sistemas de alarmas contra intrusos ha contribuido a reducir la cantidad de robos y hurtos producidos en los hogares, almacenes, etc, de todo el mundo, presentando la ventaja directa de la seguridad que brinda a las personas y sus bienes.

2.2.1 TIPOS DE ALARMAS

En el mercado nacional y a nivel mundial existen diversos tipos de alarmas las cuales se podrían clasificar de la siguiente manera:

POR SU RESPUESTA

- ✓ Alarmas sin conexión a una central de monitoreo
- ✓ Alarmas conectadas a una central de monitoreo

POR SU INSTALACION ELECTRICA

- ✓ Alarmas cableadas
- ✓ Alarmas Inalámbricas

POR TIPO DE MONITOREO

- ✓ Telefónico
- ✓ Por radio
- ✓ Internet
- ✓ Por celular

2.2.2COMPONENTES DE SISTEMA DE ALARMA

Un sistema de alarma se compone de varios dispositivos que están conectados a una central procesadora. Existen diversos dispositivos para el sistema, estos serán instalados según el nivel de seguridad requerido en un área determinada, La conexión de los componentes puede ser inalámbricamente (RF), o por cableado.

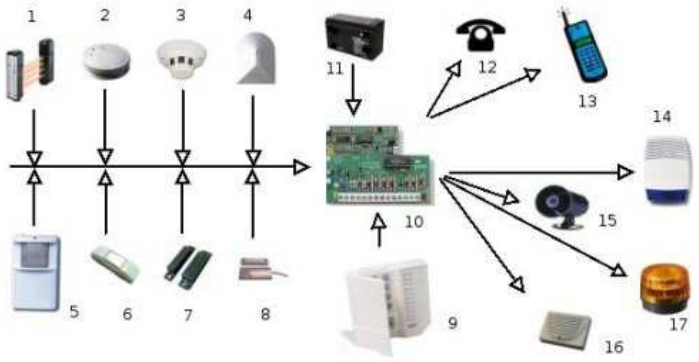


Figura II.1. Componentes de Sistema de Alarma

- **Central de Alarma**

Es el elemento central es decir es el CPU del sistema, es el que recibe las señales de los sensores, y actúa en consecuencia disparando los actuadores correspondientes, también almacena claves de activación o desactivación.

Entre los principales componentes que se almacena en la central es la memoria, la placa base, fuente de alimentación. Por lo general se encuentra ubicado en un lugar oculto, para que se difícil la ubicación si un intruso desea manipularlo.

- **Teclado**

Por lo general trata de un teclado numérico de 4X4 del tipo telefónico. La función principal es de proporcionar a los usuarios identificados (generalmente por códigos) activar o desactivar el sistema. Además de esta función básica, puede tener funciones especiales como llamada de emergencia, activación de actuadores, etc.

- **Actuadores**

Son aquellos elementos que provocan un suceso sobre un proceso automatizado. Existen varias formas de dar aviso cuando el sistema se ha activado, estas pueden ser acústicas (sirenas), iluminación, video etc.

- **Sensores y Detectores**

Son dispositivos que detectan cambios como, temperatura, movimiento, atmosféricos, etc.

Los tipos más comunes de detectores, son los **magnéticos** se trata de un sensor que forma un circuito cerrado por un imán y un contacto muy sensible que al separarse, cambia el estado (se puede programar como NC o NA) provocando un salto de alarma, se utiliza en puertas y ventanas.

Otro tipo son los sensores **inerciales**: están preparados para detectar golpes sobre una base, se colocan especialmente en cajas fuertes, también en puertas, paredes y ventanas, detectan el intento de forzar su apertura.

Por último se comenta sobre el sensor de **movimiento**, que es un dispositivo que detecta el movimiento físico y emite una señal que se la puede llevar al módulo de control domótico y mediante la programación adecuada lanzar las salidas correspondientes.

2.3 SENSORES

Se denomina sensor a todo elemento capaz de transformar señales físicas como temperatura, intensidad luminosa, fuerza, humedad, etc, en señales eléctricas

2.3.1 CLASIFICACIÓN DE LOS SENSORES

A los sensores se pueden clasificar según el parámetro físico que miden; temperatura, fuerza, etc. También atendiendo el tipo de salida como son analógicas o digitales.
En la siguiente tabla se detalla algunos tipos y ejemplos de sensores electrónicos:

Tabla II.I. Tipo de Sensores

MAGNITUD	TRANSDUCTOR	CARACTERÍSTICA
Posición lineal o angular	Potenciómetro	Analógica
=	Encoders	Digital
Desplazamientos y deformación	Transformador diferencial	Analógica
=	Galga extensiométrica	Analógica
Velocidades lineales y angulares	Dinamo tacométrica	Analógica
=	Encoder	Digital
=	Detector inductivo	Digital
Aceleración	Acelerómetro	Analógico
=	Sensor de velocidad	Digital
Fuerza y par	Galgas	Analógico
Presión	Membranas	Analógica
=	Piezoeléctricos	Analógica
Caudal	Turbina	Analógica
=	Magnético	Analógica

Temperatura	Termopar	Analógica
=	PT100	Analógica
=	NTC	Analógica
=	PTC	I/O
=	Bimetal	I/O
Sensores de presencia	Inductivos	I/O
=	Capacitivos	I/O
=	Ópticos	I/O Analógica
Sensores táctiles	Matriz de contactos	I/O
=	Piel artificial	Analógica
Visión artificial	Cámaras de video	Procesamiento digital
=	Cámaras CCD	Procesamiento digital

2.3.2 SELECCIÓN DE LOS SENSORES UTILIZADOS

Para la selección de los sensores se ha tomado en consideración varios aspectos como, la disponibilidad en el mercado, precisión y durabilidad

- **Disponibilidad en el mercado**

Dentro del Ecuador se puede encontrar fácilmente sensor de movimiento PIR, magnéticos, de humo.

- **Precisión**

La precisión es el máximo error esperado en la medida, esto no debe superar el 5%, para obtener una medida aproximada a la real.

- **Durabilidad**

Es necesario que los sensores posean un tiempo de vida superior a un año para tener resultados óptimos, cuando lean señales.3

2.3.3 SENSOR PIR

El sensor PIR “Passive Infra Red” es un dispositivo piro-eléctrico (detector de calor) que mide cambios en los niveles de radiación infrarroja emitida por los objetos a su alrededor. En otras palabras se puede decir que mide el cambio de calor, no la intensidad de calor. Estos sensores detecta movimiento mediante un promedio de calor irradiado en el tiempo, como respuesta cambio cambia el nivel lógico.

2.3.3.1 FUNCIONAMIENTO DEL SENSOR PIR

Lo primero que debemos saber cuáles son los componentes principales del sensor PIR y qué función desempeñan:

- ✓ Lente
- ✓ Sensor Piro-eléctrico
- ✓ Amplificador
- ✓ Circuitería de Detección
- ✓ Microprocesador

El Lente se compone de muchos lentes pequeños que se llaman lenslets, cada uno de estos enfoca energía infrarroja hacia el sensor piro-eléctrico. Cada foco de energía que existe en un lenslet se conoce como “zona”

Sensor Piro-eléctrico de dos elementos, un positivo y un negativo, crean dos aéreas dentro de una zona. Si entra en la zona positiva se produce un cargo positivo, y si al contrario entra en la zona negativa se produce un cargo negativo. Los dos cargos se combinan para producir una salida.

El **Amplificador** está conectado a los elementos y aumenta el cargo.

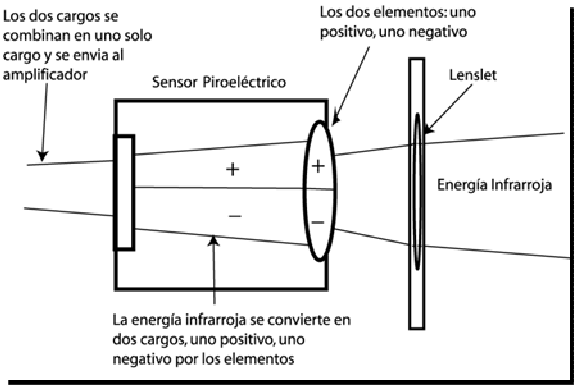


Figura II.2. Descripción del sensor-piro-eléctrico

La **circuitería de detección y el microcontrolado**r analizan las señales amplificada para determinar la alteración de estas; el software de análisis está dentro del micro controlador.

2.3.3.2 PARÁMETRO PARA LA DETECCIÓN

Para una detección más exacta se utiliza varios métodos, pero se mencionaran los más utilizados:

1. **Umbrales**

Tiene dos umbrales un positivo y un negativo, se ha establecido para tener una representación de condiciones normales, cuando los voltajes sale de uno o de los dos umbrales se detecta movimiento.

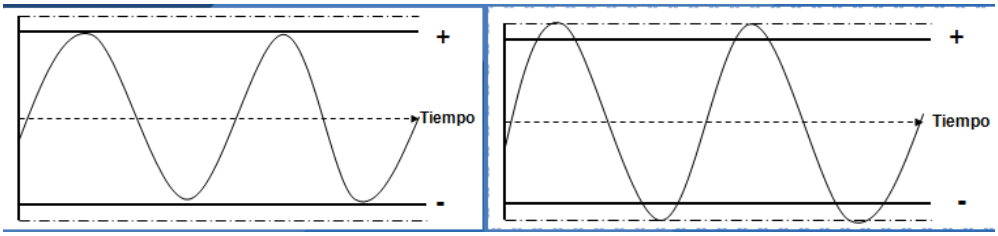


Figura II.3. Detección por umbral

2. **Filtración de Señales**

Lo que se realiza es una eliminación de señales que están fuera del rango normal de movimiento, cuando sube o baja la señal de su posición normal. Esto depende directamente de la velocidad con

la que camina la persona y cuan cerca esta del sensor, el microprocesador ignora frecuencias que están fuera del rango normal.

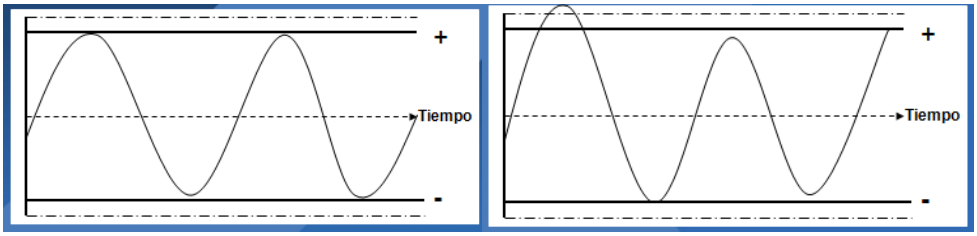


Figura II.4. Detección por filtración de Señales

3. **Análisis de Amplitud**

Se compara los niveles de señales a los umbrales, es decir la amplitud de la señal.

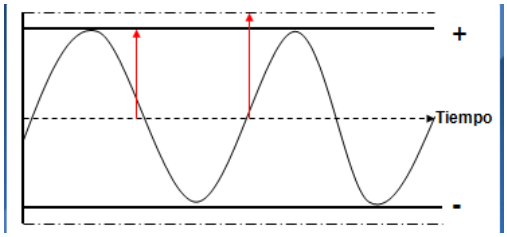


Figura II.5. Detección por filtración de Señales

4. **Análisis de Tiempo**

Se calcula el tiempo entre las variaciones de los umbrales y por cuánto tiempo duró la variación

5. **Compensación de Temperatura**

Cuando la diferencia entre la energía infrarroja de una persona y la del ambiente disminuye o aumenta, la señal hace referencia a este cambio. El microcontrolador determina la temperatura correcta y ajusta los umbrales de acuerdo a ello

2.3.3.3 SENSOR PIR INMUNE A MASCOTAS

Este sensor por lo general utiliza sensor piro-eléctrico de dos elementos cortados y separados verticalmente

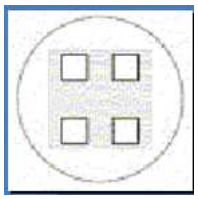


Figura II.6. Sensor piro-eléctrico de dos elementos cortados

Cuando se utiliza este tipo de sensor emite la señal infrarroja, y podemos observar en la figura II.7 que el hombre atraviesa por lo menos dos zona, a diferencia de la mascota que atraviesa una sola, en caso del piro-eléctrico de dos elementos que el hombre o la mascota pueden estar dentro de una sola zona. Este es el funcionamiento básico de este tipo de sensor inmune a mascotas.

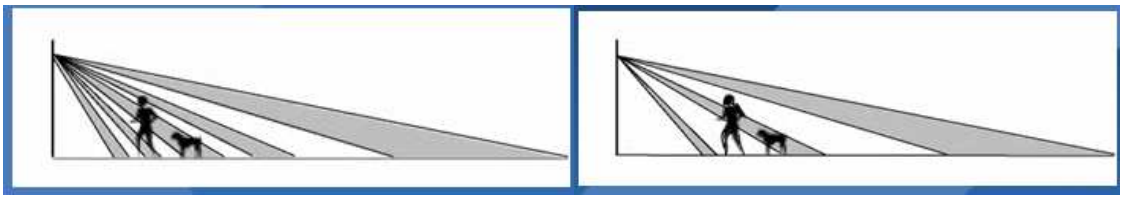


Figura II.7. Funcionamiento de sensor PIR inmune a mascotas

2.3.3.4 SENSOR COMET PIR

Es una solución de bajo costo para aplicaciones residenciales, inmune a mascotas hasta de 42 libras, incluso a varios roedores

Comet Pir es un angular de 12 x12 con alto desempeño de captura, inmunidad a falsas alarmas, con compensación de temperatura.

Conexión de bornes.

12VCD: entrada de la fuente de alimentación
Alarma: Conmutador de forma (N.C)
Tamper: Conmutador de la forma (N.C)

Figura II.8. Sensor Comet PIR

2.3.4 SENSOR MAGNÉTICO DE APERTURA

Los sensores magnéticos funcionan basándose en el capo magnético creado por un imán. Este sensor consiste en 2 simples piezas que se ubican en los vértices de las puertas y ventanas, estas piezas están en contacto junto con la otra, en el momento en que se abre la puerta el contacto se abre (circuito se abre) y se dispara el sensor. Es simple y efectivo por que si se intenta cortar los cables igualmente se abrirá el circuito.

Figura II.9. Sensor magnético de apertura

2.4 CONTROL DE ACCESO

2.4.1INTRODUCCIÓN

En la actualidad podemos observar que el acceso a determinadas áreas dentro de empresas, fábricas, hospitales instituciones educativas, almacenes, entre otros, están restringidas a personal no autorizado, sin la necesidad de que una persona este verificando la autenticidad del personal que desea acceder, esto gracias a sistemas control de acceso electrónico ya que estos nos brindan un rendimiento más óptimo.

El control de acceso electrónico administra eficientemente, el ingreso a las áreas restringidas, a usuarios debidamente identificados, incluso se puede llevar un registro confiable guardando la información a qué lugar, hora y quien accede a un sitio especifico, todo esto depende del nivel de seguridad que se desea.

Al controlar el ingreso electrónicamente se obtiene como beneficio el ahorro de tiempo, dinero, energía, confiabilidad, ya que nos permite verificar el acceso de una manera profesional y eficiente.

2.4.2 DEFINICIÓN DE SISTEMA DE CONTROL DE ACCESO

Es un sistema electrónico a través del cual se permite o niega el acceso a un recurso físico (área restringida), lógico (cuenta bancaria), o digital (archivo). Con una referencia estrictamente a un recurso físico, el término de control de acceso se refiere a restringir la entrada a un edificio, cuarto, o área específica, a personal no autorizado.

El control de acceso físico engloba tres hechos fundamentales: *quien, donde, y cuando*. **Quien** está permitido ingresar, **donde** está permitido el acceso y **cuando** esta admitido entrar

2.4.3 OPERACIÓN DE UN SISTEMA DE CONTROL DE ACCESO

Un sistema de control de acceso empieza a operar cuando una credencial es presentada a un lector, este envía la información de la credencial, usualmente un número, a un panel de control.

El panel de control compara el número de la credencial con la lista de control de acceso, permite o deniega la solicitud, y envía la información a la base de datos. Si el acceso es denegado basado en la lista de control de acceso, la puerta permanece cerrada, si hay concordancia entre la credencial y la lista de control de acceso, el panel opera un relé que abre la puerta.

Sin embargo esta descripción ilustra un factor muy importante, las credenciales pueden ser transferidas de una persona a otra, así una persona no autorizada a estar en cierto sitio puede ingresar con la credencial de otra. Para prevenir esto, dos métodos de autentificación pueden ser utilizados.

2.4.4 COMPONENTES DEL CONTROL DE ACCESO

Existen varios componentes para tener un control óptimo de acceso, entre los básicos para un funcionamiento se puede considerar:

- **Tarjeta controladora.-** Es la que realiza los procesos de control, haciendo referencia a los periféricos que se encuentran conectados en esta tarjeta, siendo esta el componente más importante.

- **Sensor.-**Es el o los dispositivos que informan sobre el estado objeto que impide el acceso, como puede ser el estado de la puerta cerrada o abierta.

- **Sistema de Detección.-** Son dispositivos que deben censar el tipo de información presentada por los usuarios, y estas pueden ser, credenciales, NIP o clave, y entradas biométricas.

- **Botón de Salida.-** Dispositivo mecánico que nos permite realizar la salida en caso que solo controlemos el ingreso.

- **Cerradura eléctrica.-** Es un dispositivo eléctrico el que al ser energizado produce un campo magnético que impide abrir la puerta, y al interrumpir la energía, la puerta se libera.

- **PC y Software.-** Es una herramienta que nos sirve para programar el acceso y monitorear el estado del sistema. No necesariamente tiene que ser una PC, puede ser un microcontrolador u otro dispositivo que sea capaz de procesar las señales.

2.4.5 MÉTODOS PARA CONTROL DE ACCESO

Para administrar los accesos de una forma profesional y eficiente, se debe elegir el nivel de seguridad que se requiere, entre los métodos de seguridad más utilizados están:

- **NIP (Número de Identificación Personal)**

Establece un código numérico a cada persona que tiene acceso a un área restringida, este código puede variar de cuatro a ocho dígitos, estos se enlaza con los derechos asignados a cada usuario. Este sistema es el más básico y económico, pero su nivel de seguridad es bajo, ya que si personal no autorizado obtiene el código, fácilmente puede acceder al sitio protegido.

- **PROXIMIDAD**

Se basan en transmisores (tarjetas o tags) y receptores que utilizan tecnología de radiofrecuencia, que actúan de forma inalámbrica intercambiando información, solo las tarjetas que estén autorizadas podrán permitir o negar el acceso a determinadas áreas.

La proximidad de la tarjeta es suficiente, al presentar el tag a una determinada distancia la información se envía al sistema de control y valida la autenticidad.

Figura II.10. Tarjeta de Proximidad

Su principal ventaja contra los demás sistemas, es que no necesita que la tarjeta sea pasada en un sentido específico, lo que le da mayor velocidad de lectura y poca resistencia de uso por parte de los usuarios, porque incluso la lectura de los datos se lo puede realizar mientras la tarjeta esta dentro de la billetera, cartera etc.

El sistema de proximidad es una de las tecnologías más utilizadas y se la utiliza tanto para personas como para automóviles.

- **TARJETAS INTELIGENTES**

Tarjeta inteligente o tarjeta con circuito integrado (TCI), es una tarjeta plástica que contiene un pequeño microprocesador que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad.

Existen dos tipos básicos de de interfaz de TCI; las de contacto y las de no contacto.

Las **TCI de Contacto** estas requieren ser insertadas en un lector, y la tarjeta inteligente con una conexión directa a un micromódulo conductivo en la superficie de la tarjeta

Figura II.11. Tarjeta inteligente de contacto

Las TCI de no contacto estas deben estar ubicadas cerca del lector (generalmente no superior a 10 centímetros) para que se realice el intercambio de información. El intercambio de información se realiza con ondas de radio frecuencia, esta comunicación se logra con una antena interna tanto en la tarjeta como en el lector.

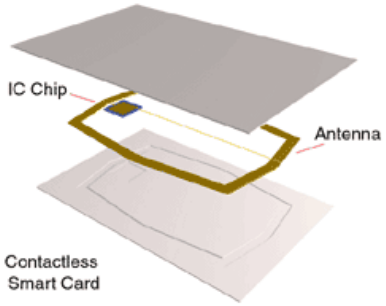


Figura II.12. Tarjeta inteligente de no contacto

Como mecanismo de control de acceso las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados.

- **SISTEMAS BIOMÉTRICOS**

Cada individuo posee características o identificadores únicos, los cuales nos hacen diferentes unos con otros, por ejemplo: huellas dactilares, la cara, el iris del ojo, la retina, la posición de las venas entre otras.

Por esta razón se han desarrollado Sistemas Biométricos que se basan en identificar o comprobar la identidad de una persona mediante sus características únicas, con esto dichos sistemas son los que brindan mayor seguridad en lo que se refiere a control de acceso.

Figura II.13. Identificadores personales para biometría

Su principal ventaja radica en el nivel de seguridad que brinda, ya que por su esencia es intransferible. Su principal desventaja está en el precio del lector, la velocidad de lectura (comúnmente son lentos o deben ir acompañados de un teclado para anteponer un código y acelerar el proceso de búsqueda) y muchas veces la resistencia de uso de parte del usuario.

2.4.6 COMPARACIÓN ENTRE LOS METDOS DE CONTROL DE ACCESO

Habiendo detallado las características de cada método de control de acceso, se puede resumir lo expuesto anteriormente en la Tabla II.II.

Tabla II.II. Cuadro comparativo entre los diferentes métodos de control de acceso

Tecnología de Lectura	**Seguridad/ Inviolabilidad**	**Desgaste de tarjeta**	**Desgaste del lector**	**Costo de mantenimiento**	**Precio tarjeta**	**Precio de lector**
Clave por Teclado	Muy Baja	No posee	Alto	Medio	No Posee	Bajo
Proximidad	Alta	No posee	No posee	Bajo	Medio-Bajo	Medio
Tarjeta Inteligente	Alta	Medio	Medio	Medio	Medio	Alto
Sistema Biométrico	Muy Alta	No posee	Bajo	Medio-Alto	No posee	Muy Alto

Una vez analizado los métodos para controlar el acceso y dependiendo del nivel de seguridad requerido, se puede optar por cualquiera de estos, o a su vez realizar una combinación, por ejemplo el usuario puede presentar su tarjeta de identificación y adicionalmente ingresar un NIP para que se le permita el acceso.

2.5 MICROCONTROLADORES

Es un circuito integrado programable, en cuyo interior posee toda la arquitectura de un computador, capaz de ejecutar las órdenes grabadas en su memoria. Está compuesto de varios bloques que desempeñan una función específica, sus componentes principales son:

- ✓ Procesador o CPU (Unidad Central de Procesamiento)
- ✓ Memoria RAM (Memoria de acceso aleatorio)
- ✓ Memoria para el programa tipo ROM/EPROM/EEPROM
- ✓ Líneas de Entrada Salida (I/O) también llamados puertos

El microcontrolador de fábrica no realiza tarea alguna, por lo que se le debe programar, y almacenarlo en memoria para que desempeñe una función. Este puede escribirse en distintos lenguajes de programación y pueden reprogramarse varias veces.

Por las características mencionadas y por su alta flexibilidad, los microcontroladores son utilizados como el cerebro de una gran variedad de sistemas electrónicos como: aplicaciones industriales de automatización y robótica, domótica, en automóviles, etc. Frecuentemente para referirse a este dispositivo se emplea la notación µC.

2.5.1 ARQUITECTURA DEL MICROCONTROLADOR

La arquitectura se define en el modo de operación del procesador en cuanto a conjunto de instrucciones y modo de ejecución de las mismas.

En cuanto al **conjunto de instrucciones se clasifican en tres grupos** CISC, RISC, SISC

- **CISC** (Computadores de Juego de instrucciones completo) disponen de más de 80 instrucciones máquina en su repertorio, algunas que son tan sofisticadas y potentes que requieren muchos ciclos para su ejecución.

- **RISC** (computadores de juego de instrucciones reducido) en estos las instrucciones maquina es muy reducido y las instrucciones son simples y generalmente se ejecutan en un ciclo. La sencillez de las instrucciones permiten optimizar el hardware y el software del procesador

- **SISC** (computadores de juego de instrucciones específico) en los uC destinados a aplicaciones muy concretas el juego de instrucciones, además de ser reducido, es muy específico, es decir, las instrucciones se adaptan a las necesidades de la aplicación específica.

En el **modo de ejecución de las instrucciones las arquitecturas se clasifican** en: Von Neuman y Harvard.

- En la **arquitectura Von Neuman** existe una sola memoria donde coexisten las instrucciones del programa y los datos, accedidos con un bus direccional, uno de datos y uno de control.

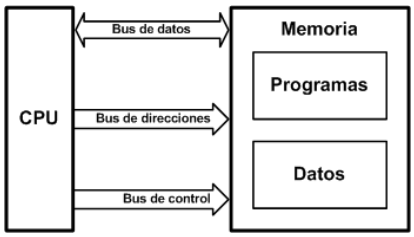


Figura II.14. Arquitectura Von Neuman

- En La **arquitectura Harvard** dispone de dos memorias independiente una de instrucciones y otra que contiene solo datos, el procesador tiene los buses segregados, de modo que cada tipo de memoria tiene un bus de datos, uno de direcciones y uno de control. El procesador puede acceder simultáneamente a cada memoria, por lo que la velocidad aumenta, típicamente pueden ser dos veces más rápidos que la arquitectura Von Neuman

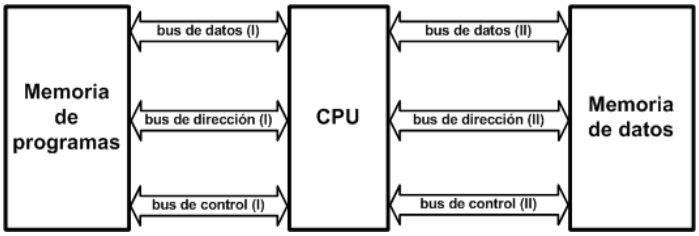


Figura II.15. Arquitectura Harvard

2.5.2 MEMORIA

En los microcontroladores la memoria de datos y la de instrucciones están incorporadas en el chip. Una parte debe ser no volátil, y debe contener el programa de instrucciones que gobierna la aplicaciones; otra parte de memoria será tipo RAM (Memoria de acceso aleatorio), volátil, y se destina a guardar la variables y los datos .

Como el µC solo se destina a una tarea en la memoria ROM (Memoria de solo lectura) solo hay que almacenar un único programa de trabajo. La RAM es de poca capacidad, pues solo debe contener las variables y los cambios de información que se produzca en el transcurso del programa.

Los fabricantes de microcontroladores trabajan con capacidades de ROM comprendidas entre 512 bytes y 8 Kbyte y de RAM comprendidas entre 20 y 512 bytes. En el mercado podemos encontrar microcontroladores con los siguientes tipos de memoria no volátil:

- **ROM con mascara**: memoria de solo lectura, se graba durante la fabricación del dispositivo.
- **OTP**: Programable una sola vez por el usuario
- **EPROM:** Puede grabarse y borrarse varias veces; el borrado se lo realiza mediante rayos ultravioleta
- **EEPROM:** Puede borrarse y grabarse eléctricamente.
- **FLASH:** memoria no volátil de bajo consumo que se puede escribir y borrar. Funciona como una ROM y una RAM pero es más pequeña.

La EEPROM y la FLASH pueden ser reprogramadas en el mismo circuito

2.5.3 RELOJ PRINCIPAL

Todos los microcontroladores disponen de un circuito oscilador el cual genera una onda cuadrada de alta frecuencia, que configura los impulsos de reloj usados en la sincronización de todas las operaciones del sistema.

Por lo general, el circuito de reloj está incorporado en el µC y sólo se necesitan unos pocos componentes exteriores para seleccionar y estabilizar la frecuencia de trabajo. Dichos componentes suelen consistir en un cristal de cuarzo junto a elementos pasivos o bien un resonador cerámico o una red R-C.

Aumentar la frecuencia de reloj supone disminuir el tiempo en que se ejecutan las instrucciones pero lleva a disponer de un incremento en el consumo de energía.

2.5.4 PUERTAS DE ENTRADA /SALIDA

Ponen al µC en contacto con su entorno. La principal utilidad de los pines que posee el µC, es soportar las líneas de E/S que comunican al computador interno con los periféricos exteriores; estas líneas se destinan a proporcionar el soporte a las señales de entrada, salida y control.

2.5.5 RECURSOS ESPECIALES

Cada fabricante ofrece varias versiones de la arquitectura básica del microcontrolador, ampliando las memorias, incorporando nuevos recursos, reduciendo las prestaciones, etc.

Los principales periféricos que contiene un microcontrolador son: temporizador, perro guardián, protección ante fallo de alimentación, estado de reposo o de bajo consumo, conversor A/D, conversor D/A, comparador analógico, modulador PWM, puertas de E/S digitales, puertas de comunicación.

Protección ante fallo de alimentación: Se trata de un circuito que resetea al microcontrolador cuando el voltaje de alimentación (VDD) es inferior a un voltaje mínimo ("brownout"). Mientras el voltaje de alimentación sea inferior al de brownout el dispositivo se mantiene reseteado, comenzando a funcionar normalmente cuando sobrepasa dicho valor.

Conversor A/D (CAD): Los microcontroladores que incorporan un Conversor A/D (Analógico/Digital) pueden procesar señales analógicas, tan abundantes en las aplicaciones.

Conversor D/A (CDA): Transforma los datos digitales obtenidos del procesamiento del computador en su correspondiente señal analógica.

Puertos de Entrada/Salida Digitales Todos los microcontroladores destinan algunas de sus pines a soportar líneas de E/S digitales. Por lo general, estas líneas se agrupan de ocho en ocho formando Puertos.

Comparador analógico: Algunos modelos de microcontroladores disponen internamente de un amplificador operacional que trabaja como comparador entre una señal fija de referencia y otra variable que se la suministra por un pin del dispositivo. La salida del comparador proporciona un nivel lógico 1 ó 0 según una señal sea mayor o menor que la otra.

Temporizador: Se utiliza para el control de tiempos y para llevar la cuenta de acontecimientos que suceden en el exterior

Perro Guardián: Consiste en un temporizador que, cuando se desborda y pasa por 0, provoca un reset automáticamente en el sistema

Módulo de anchura de impulsos PWM: Son circuitos que proporcionan en su salida impulsos de anchura variable, que se ofrecen al exterior a través de los pines del µC

Puertos de Comunicación: el objetivo es de dotar al microcontrolador la facultad de comunicarse con otros dispositivos externos, otros buses de microprocesadores, buses de redes y poder adaptarlos con otros elementos, bajo otras normas y protocolos; algunos modelos disponen directamente de esta tarea, entro los que se destacan:

- ✓ **UART,** adaptador de comunicación serie asincrónica
- ✓ **USART,** adaptador de comunicación serie sincrónica y asincrónica
- ✓ **USB, (**Universal Serial Bus**),** es un bus serial para los PC.
- ✓ **CAN** (Controller Area Network),permite adaptación con redes de conexión multiplexado.

2.5.6LENGUAJES DE PROGRAMACIÓN DE MICROCONTROLADORES

El único lenguaje que entienden los µC es el **código maquina** formado por ceros y unos del sistema binario.

- **Lenguaje Assambler**

Es un lenguaje de bajo nivel utilizado para escribir programas informáticos, expresa las instrucciones de una forma muy cercana al microcontrolador, ya que cada una de esas instrucciones se corresponde con otra de código máquina.

El programa escrito en este lenguaje se denomina **código fuente** se crea el fichero **(*asm).** El programa ensamblador proporciona a partir de este fichero el correspondiente código máquina, que suele tener la extensión ***hex.**

Entre las principales ventajas y desventajas tenemos:

- ✓ Programar en lenguaje ensamblador es difícil de aprender, entender, leer, escribir, depurar y mantener, por eso surgió la necesidad de los lenguajes compilados.

- ✓ Programar en lenguaje ensamblador lleva mucho tiempo.

- ✓ Son generalmente más rápidos, al programar cuidadosamente se pueden crear programas de 5 a 100 veces más rápidos que con lenguajes de alto nivel.

- ✓ Los programas ocupan menos espacio, puede ocupar la mitad de espacio que su contrapartida en lenguaje de alto nivel

- ✓ Con el lenguaje ensamblador se pueden crear segmentos de código imposibles de formar en un lenguaje de alto nivel.

- **LENGUAJE COMPILADOR**

La programación en un programa de alto nivel (como el Basic, C) permite disminuir el tiempo de desarrollo de un producto. No obstante, si no se programa con cuidado, el código resultante puede ser mucho más ineficiente que le programado en ensamblador. Las versiones más potentes suelen ser muy caras, aunque para los microcontroladores más populares pueden encontrarse versiones "demo" limitadas e incluso compiladores gratuitos

2.5.7 SELECCIÓN DEL MICROCONTROLADOR

Existen microcontroladores de 4, 8, 16,32 o 64 bits, de los cuales los de 8 bits son los más utilizados, ya que son apropiados para la mayoría de aplicaciones, lo que hace absurdo emplear µC más potentes y por ende más caros.

A la hora de escoger un microcontrolador para un diseño concreto se deben tomar en cuenta factores como la documentación, herramientas de desarrollo disponibles y su precio, la cantidad de fabricantes que lo producen y obviamente las características del microcontrolador (tipo de memoria, número de temporizadores, interrupciones, etc.)

En cuanto a la aplicación, antes de seleccionar un microcontrolador es imprescindible analizar los requisitos de la aplicación:

- ✓ Procesamiento de datos: se debe ver si es necesario manejar datos en forma rápida y con alta precisión, para lo que sería necesario un microcontrolador de 16, 32 o 64 bits si fuese necesario.

- ✓ Entrada-salida: es conveniente hacer un diagrama de bloque para ver cuántas señales se debe controlar.

- ✓ Memoria: dependerá de las necesidades de memoria RAM (volátil) y no volátil.

- ✓ Diseño de la placa: la selección del microcontrolador condicionará el diseño de la placa de circuitos. Puede que darse el caso que un µC barato, eleve el precio del resto de los componentes del circuito.

2.5.8 MICROCONTROLADOR PIC 16F877A

Este microcontrolador es fabricado por MicroChip familia a la cual se la denomina PIC es uno de los más utilizados para realizar proyectos que requieren mayor capacidad para almacenar datos, mayor número de puertos para trabajar como entrada o salida etc. La distribución de sus puertos así como los conversores que contiene el dispositivo se visualiza en la figura II.16.

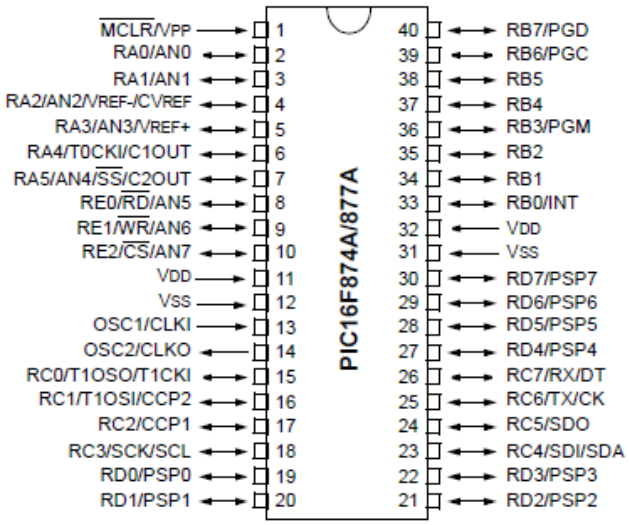


Figura II.16. Distribución de pines del PIC 16F877A

Entre las principales características del microcontrolador tenemos:

- Utiliza un procesador con una arquitectura en modo de operación **Harvard** y conjunto de instrucciones **RISC** de alto desempeño con un set de 35 instrucciones.
- Memoria de Datos EEPROM con capacidad de 256 posiciones de 8bits; con un 1.000.000 de ciclos de escritura y borrado, mayor de 40 años de retención
- Memoria RAM con capacidad de 368 posiciones de 8bits cada una.
- Memoria para el programa o FLASH de 8192 palabras
- Tiene 33 pines de E/S, con 5 puertos
- Convertidor A-D 8 entradas
- Las instrucciones se ejecutan en un ciclo de reloj excepto las de brinco que toman dos.
- Soporta hasta 20 MHZ de velocidad (200 ns por instrucción)
- Opciones de oscilador seleccionables
- Amplio voltaje de operación 2 a 5.5 V
- Corriente de pines de hasta 25 mA
- Bajo consumo de potencia
- Protección de código

El dispositivo necesita un oscilador externo que puede ser de cristal, RC entre otros, ya que no posee oscilador interno. Además una resistencia pull-up para conectarlo en el máster clear ya que no hay forma de deshabilitarlo.

2.6 SOFTWARE DE PROGRAMACIÓN MICROCODE STUDIO

El software MicroCode Studio es un editor de texto que nos posibilita la programación de los microcontroladores PIC, este software necesita un compilador Pic Basic Pro el cual permite realizar la programación del µC en un lenguaje de alto nivel, lenguaje Basic. Por lo tanto MicoCode Studio y el compilador van juntos.

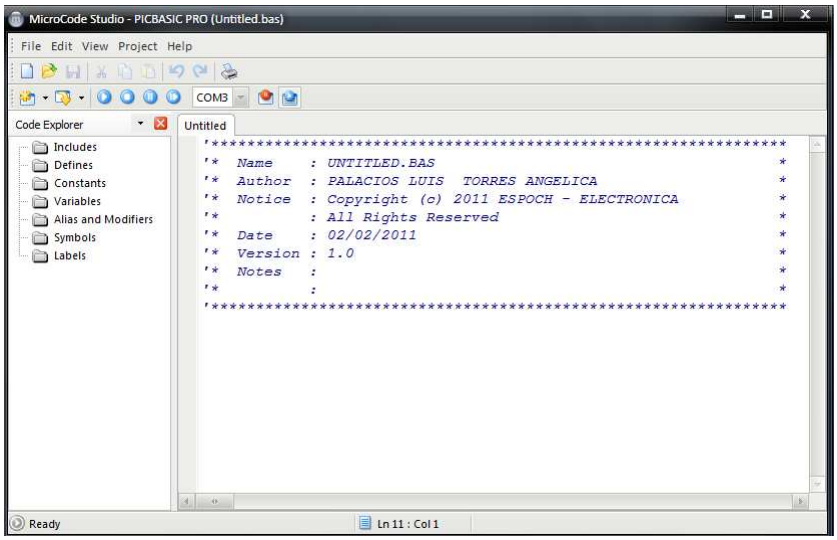


Figura II.17. Pantalla de Inicio del Microcode Studio

Se detallara las partes más importantes para del software, para poder entender la función que desempeñan las diferentes herramientas, con esto podemos entender los diferentes mensajes que visualiza el programa cuando se está editando y compilando la programación que tendrá el microcontrolador.

Lo primero será verificar que el compilador está instalado, esto lo comprobamos al dirigirnos a la pestaña *Help* y luego a la opción *About,* si no está instalado debemos descargarnos un compilador del internet, este es el que permitirá generar los diferentes archivos con las extensiones correspondientes en el momento de correr el programa.

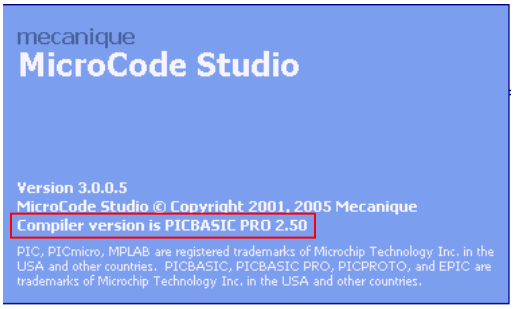
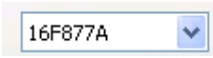
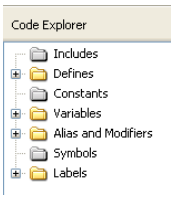


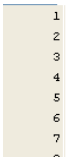
Figura II.18. Verificación del Compilador



En esta pestaña se podrá seleccionar el microcontrolador que se desea utilizar para la programación.



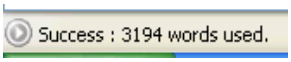
. – **Explorador de Código** Permite visualizar las variables subrutinas, constantes, alias y las etiquetas. Que se crean durante la programación se haya realizado, con la finalidad de encontrar rápidamente algún código que se necesite cambiar o editar o simplemente verificara cuales han sido creadas.



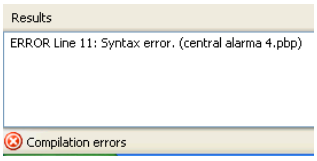
.- **Numeración de líneas del programa** esta herramienta es muy útil a la hora de compilar el programa, ya que si ocurre algún error, indiaca cual es la línea donde se produjo, y facilita el arreglo del mismo.


Estas herramientas son las de compilación y son las más importantes a la hora de montar el programa. El primer botón sirve solamente para compilar el programa, se lo puede activar al presionar F9, desde el teclado. Una vez compilado el programa genera 4 archivos **.ASM .MAC .PBP** y **.HEX** siendo el ultimo el más importante ya que es el que sirve para grabar el µC.

El segundo botón tiene dos funciones a la vez, la primera es de compilar el programa y generar los 4 archivos detallados anteriormente, y la segunda es de llamar al programador IC – PROG, el cual nos permitirá grabar el PIC



Una vez compilado el programa podemos obtener varios mensajes. Este mensaje visualiza el espacio que ocupó el programa en el PIC, en el ejemplo se ha ocupado 3194 palabras, y la compilación fue exitosa.



Indica que se produjo un error en la compilación del programa, el tipo de error y el número de línea donde está el error.

En la siguiente figura II.19 se muestra la ventana donde está el encabezado el programa y es donde se editara el programa.

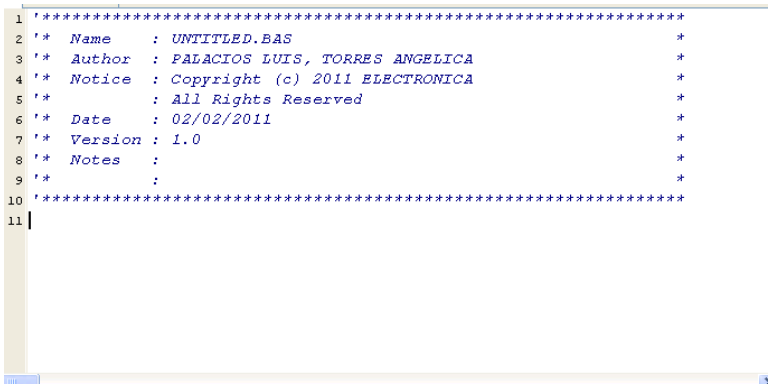


Figura II.19. Ventana de Edición del Programa

Una vez detalladas las herramientas más importantes del MicroCode Studio, se entenderá los errores y las posibles soluciones que podemos aplicar.

Este editor y compilador se ha utilizado para la programación de los microncontroladores, facilitando la edición en un lenguaje de alto nivel precisamente el Basic, adicionalmente genera el archivo .HEX, el cual servirá para poder grabar el PIC, utilizando un software y disponiendo del hardware necesario para realizar esta función.

2.7 SOFTWARE DE GRABACIÓN “PICKIT2”

El software de grabación es una herramienta fundamental ya que nos permite grabar el archivo .HEX en el microcontrolador, para realizar esta tarea se ha utilizado el grabador **PICKit2 programmer** que es un programador USB de PIC, el cual lo fabrica Microchip.

Este software para la instalación se lo puede descargar desde el internet o viene cuando se adquiere el grabador. Para entender el funcionamiento se detallará las partes principales del software el cual nos permitirá grabar el archivo .HEX en el microcontrolador.

2.7.1 PARTES PICKIT 2 PROGRAMMER

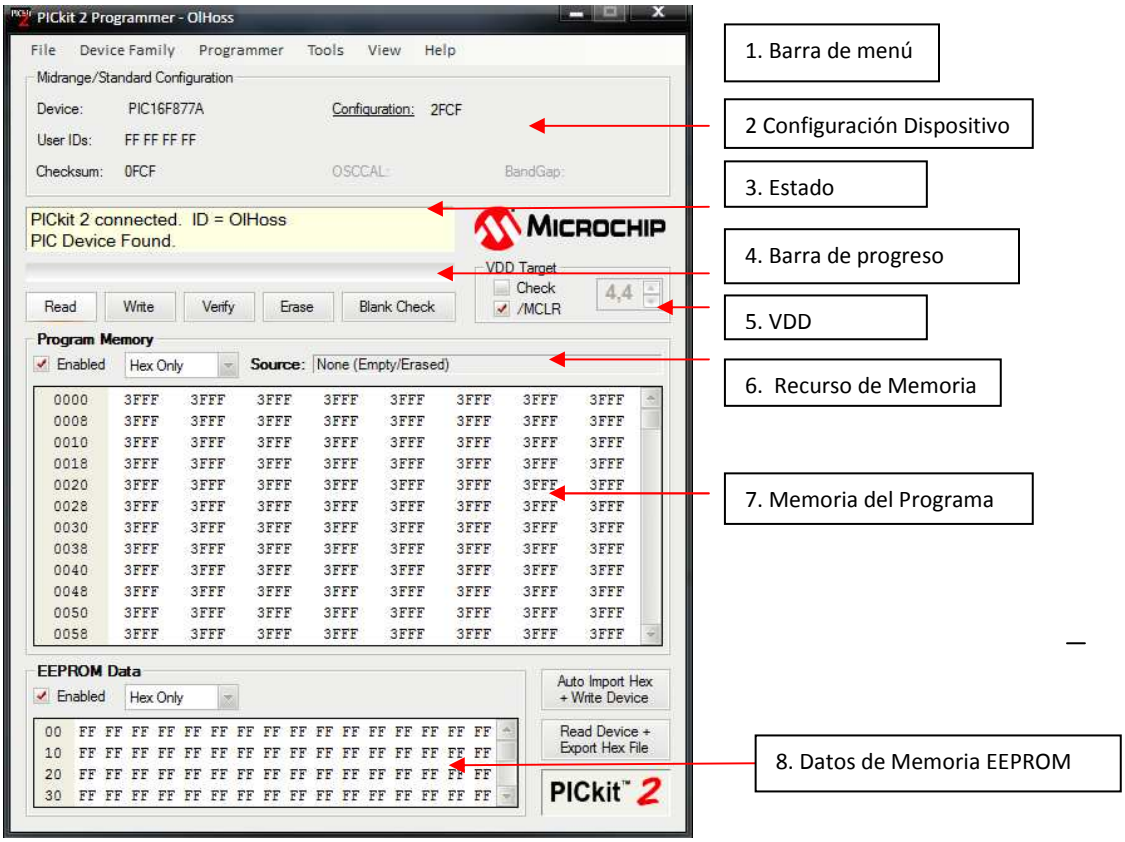


Figura II.20. Partes de PICkit2 Programmer

1. **Barra de Menú**

File.

Import Da la opción de seleccionar desde donde se va extraer el archivo HEX.

Export Exporta el archivo **Hex** leído desde el dispositivo

File History.- Visualiza un historial de los archivos HEX que han sido importados.

Exit.- Se utiliza para salir del programa

Device Family.- permite seleccionar el pic mediante tipo de familia. Ya sea configurado en auto detección de dispositivo o selección manual debe definir a que gama de familia pertenece el dispositivo según Tabla de dispositivos soportados.

Programmer.-Se utiliza para realizar varias funciones en el dispositivo entre las principales tenemos

Read Divece.- Lee programas de memoria, los datos de memoria EEPROM

Write Device.- Escribe, programas en memoria, los datos en memoria EEPROM

Verify.- verifica los programas de memoria

Erase.- Borra el contenido del dispositivo

Tools.- Entre las principales opciones que encontramos en esta pestaña tenemos

Enable Code Protect.- Habilita la protección del código en el microcontrolador para futuras operaciones de escritura. Para deshabilitar esta opción, toda la memoria del dispositivo de borrarse y ser escrita nuevamente

Enable Data Project.- Habilita la protección de datos en la memoria EEPROM para futuras operaciones de escritura. Para deshabilitar esta opción toda la memoria del dispositivo de borrarse y ser escrita nuevamente.

Check Communication.- Verifica la comunicación USB con el PICkit2 programmer.

Help En esta opción se encuentra toda la ayuda necesaria como es manual de usario, guía de herramientas lógicas, la versión del programa

2. Configuración del Dispositivo

En la configuración del dispositivo, se visualiza el microcontrolador que se utiliza, ID User, y una pequeña información del dispositivo que se está utilizando

3. Estado

Esta ventana muestra las operaciones que se realizan en curso. Si la operación es exitosa el estado de la ventana estará en color verde, si la operación falla, la condición de la ventana se mostrara de color rojo, y si la operación muestra color amarillo significa un tipo de alerta.

Figura II.21. Operación exitosa con PICkit2 Programmer

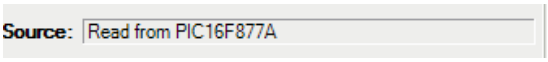
4. Barra de Progreso


Visualiza el progreso de una operación

5. VDD

Se puede activar o desactivar marcando la casilla, adicionalmente la tensión puede ser modificada dependiendo del dispositivo de destino

6. Recurso de Memoria



Muestra la fuente de los datos cargados en el dispositivo. Si se lee desde un archivo hexadecimal, se mostrara el nombre del archivo, y si se lee desde un dispositivo, se mostrara el nombre del mismo.

7. Memoria del Programa

La ventana de memoria de programa muestra el código del programa en formato hexadecimal. El código puede ser editado en la ventana. La casilla de verificación junto a la ventana de memoria de

programa sólo está disponible en dispositivos con memoria EEPROM de datos. Si la casilla está marcada, la memoria de programa, y configuración de las palabras se escriben, leen, y verifican en el dispositivo, si la casilla de verificación no está marcada la configuración no será alterada durante una operación de venta de dispositivos.

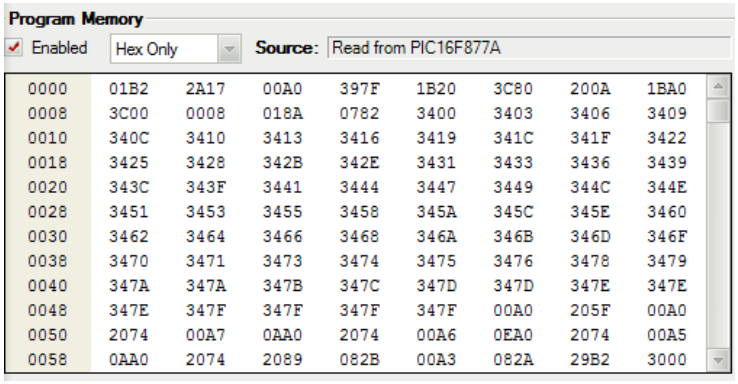


Figura II.22. Ventana de la memoria del programa

8. Datos de Memoria EEPROM

La ventana de memoria EEPROM de datos muestra el código del programa en formato hexadecimal. El código puede ser editado en la ventana. Si la casilla está marcada, entonces el dispositivo EEPROM se sobrescribirán con los datos de la ventana. Si la casilla no está activada, el dispositivo EEPROM no serán borrados o alterados durante una operación de venta de dispositivos. La casilla de verificación no afecta a las operaciones de dispositivos Borrar o cheque en blanco. Ambas casillas ventana de la memoria no se puede borrar al mismo tiempo.

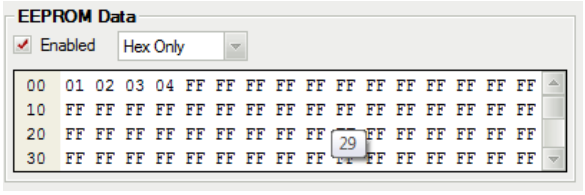


Figura II.23. Ventana de la memoria EEPROM

2.8 SOFTWARE DE SIMULACIÓN PROTEUS

El software de simulación Proteus es una herramienta útil para estudiantes y profesionales, permite el diseño de circuitos empleando un entorno gráfico, en el cual es posible colocar los símbolos representativos de los componentes y realizar la simulación de su funcionamiento sin riesgo de ocasionar daños a los circuitos. Lo que más interés ha despertado es la capacidad de simular adecuadamente el funcionamiento de los microcontroladores más populares (PICS, ATMEL-AVR, MOTOROLA, 8051, etc.)

Proteus suministra tres potentes subentornos como son el ***ISIS*** para el diseño gráfico, ***VSM*** (Virtual System Modelling) para la simulación y el ***ARES*** *(Advance Routing Modelling)* para el diseño de placas. La versión que se ha utilizado para el desarrollo de la tesis es 7.1 sp2

2.8.1 ISIS DE PROTEUS

EL modulo ISIS (Intelligent Schematic Input System), es un programa que nos permite dibujar sobre una área de trabajo, un circuito que posteriormente podemos simular. Entre las principales utilidades que posee están, librerías de componentes, conexión automático entre 2 puntos del esquema, enumeración automática de componentes etc.

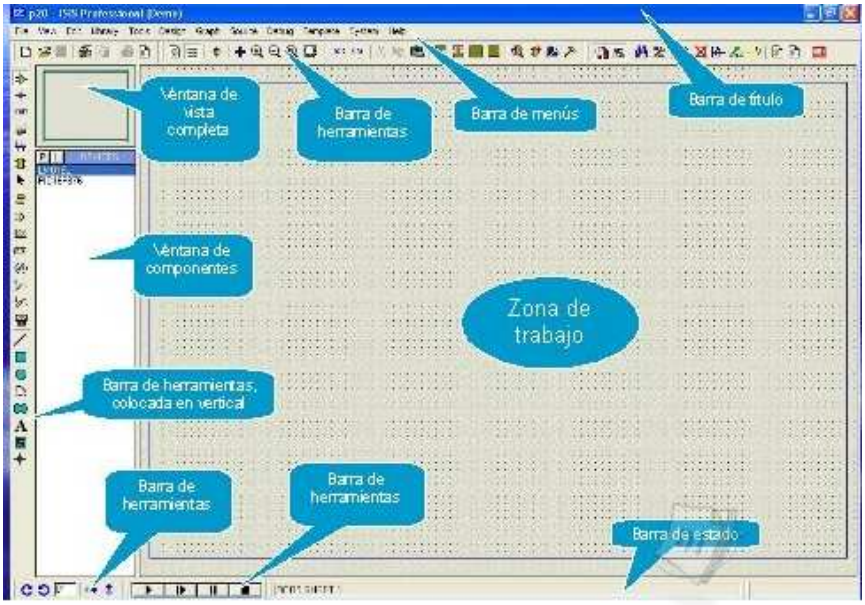
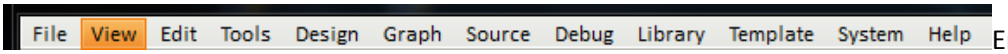


Figura II.24. Entorno de Trabajo ISIS

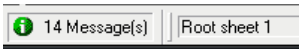
En la **barra de títulos** se muestra el icono del programa, el nombre del archivo y la leyenda de ISIS Profesional



En la **barra de menus** permite al acceso a las opciones del programa, varias de estas están disponibles en el icono de las barras de herramientas.

Barra de Herramientas Son numerosas, el usuario puede colocar en distintas posiciones de los bordes, son de suma importancia, ya que con estas podemos seleccionar la opción indicada para realizar el diseño.

Figura II.25. Barra de Herramientas de Trazado



En la **barra de estado** se visualiza mensajes informativos de los componentes que intervienen en la simulación, así también se muestra las coordenadas cuando se ubican los mismos.

La **zona de trabajo** es donde se monta los elementos que forman parte del circuito.

2.8.2 CONEXIÓN DEL CIRCUITO

Para empezar a dibujar, tenemos que seleccionar los elementos que van a utilizarse para el circuito, para esto se escoge modo componentes y luego presionamos el botón P de la ventana dispositivos y librerías.

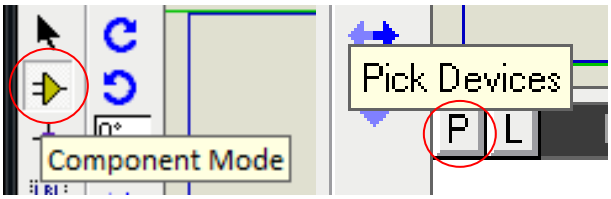


Figura II.26. Selección de componentes

Al presionar P nos presentara la ventana de *Pick Device* en donde tenemos: la categoría, subcategoría, el fabricante, el símbolo del dispositivo así como la forma que se representa en la placa, es aquí donde seleccionamos los elementos necesarios para montar el circuito.

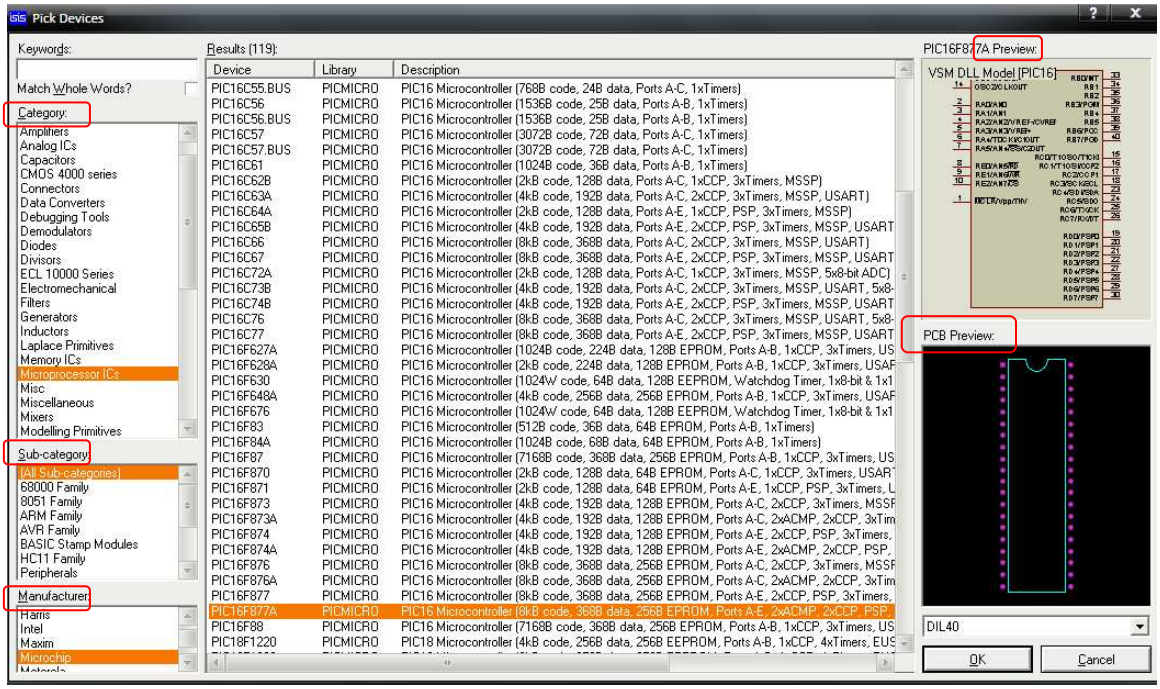
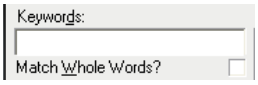


Figura II.27. Ventana selección y características del componente



La búsqueda se puede facilitar al ingresar el nombre del dispositivo, en el campo Keywords.

La principal utilidad que se le da al ISIS de proteus en el desarrollo de la tesis es para la simulación de circuitos con microcontroladores. Aquí seleccionamos el µC que se necesita, y se introduce el

archivo .hex el cual contiene el programa que necesita el dispositivo para empezar a funcionar. Para realizar esta operación ubicamos el elemento en el área de trabajo damos doble click, nos aparecerá la ventana de *Edición de Componentes* y en el campo *Program File* ubicamos el archivo .hex, adicionalmente nos da opciones de ingresar la frecuencia de reloj.

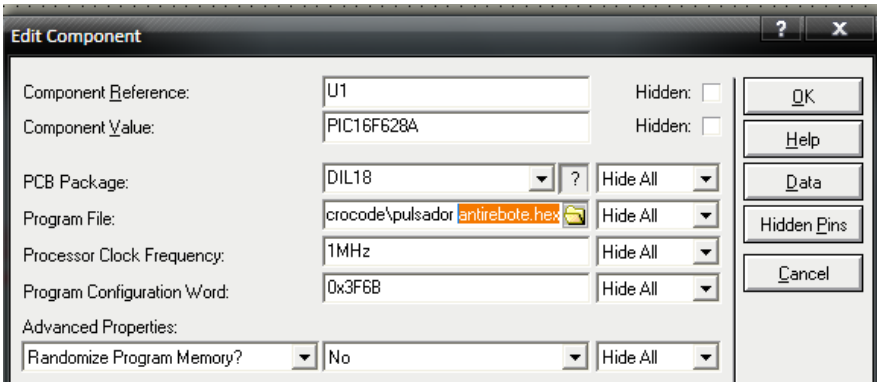


Figura II.28. Ingreso archivo .hex en el microcontrolador

Cuando se termine de seleccionar los componentes, los ubicamos en la ventana de trabajo y procedemos a unirlos para armar el circuito, una vez terminado el proceso presionamos PLAY para empezar con la simulación.

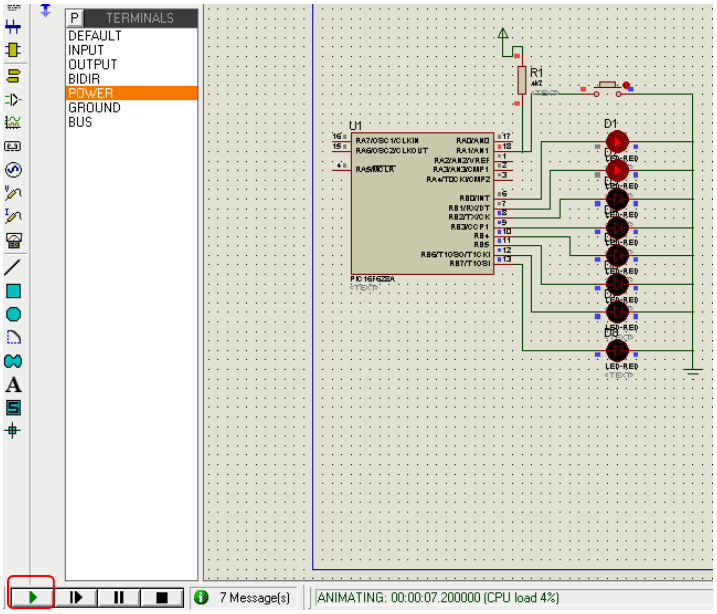


Figura II.29. Simulación de circuito en ISIS

2.8.3 SOFTWARE DE RUTEADO ARES DE PROTEUS

Uno de los subentornos de proteus es***ARES*** *(Advance Routing Modelling)*, se utiliza para el diseño de circuitos impresos PBC (Printed Circuit Board).

Para el desarrollo del PBC se lo puede realizar a partir del circuito creado en ISIS, es decir disponemos del esquema realizado previamente, esta manera se crea el ruteado automáticamente, también se los puede realizar manualmente es decir buscando los elementos y unirlos mediante un esquema que el usuario disponga.

Varios dispositivos que se encuentran en ISIS, no tienen vista para PBC, o simplemente en las librerías de ares no se encuentran, por lo que el programa da la capacidad de crear nuestros componentes, para esto hay que tener en consideración las dimensiones de los mismos, un ejemplo es potenciómetro, simula su funcionamiento, pero cuando se busca en ares no tenemos este dispositivo.

Para el desarrollo de la tesis se utilizó el ruteado manual, asi mismo se creó varios elementos como son, resistencias de ½ watio, diodos led, borneras, conectores entre otros

- **Entorno de Trabajo**

Figura II.30. Entorno de Trabajo Ares

Menús: Encontramos los menús para guardar el diseño, crear los ficheros GERBER, distintas opciones de visualización, herramientas de ruteado, etc

Barra Herramientas: aquí tenemos varias opciones como elección de las herramientas para la creación de las pistas, comprobación de conexión,etc.

Barra Selección: nos permitirá seleccionar la capa de trabajo, dentro de la pantalla de edición, también podremos seleccionar los elementos que deseamos etc

Barra de Estado: nos muestra la posición en la que se encuentra el cursor, esta se puede dar en Th (mils) o milímetros (mm). La relación que hay entre estas medidas es la siguiente: 40mils = 1mm, de forma que con esta relación ya podemos hacernos una idea de las medidas.

Pantalla de Edición: Aquí realizaremos el diseño de nuestro ruteado.

- **Creación de Encapsulados**

- En primer lugar observamos las características de distancias y grosor de nuestro dispositivo, por ejemplo una resistencia de ½ watio, dispone de un cuerpo de 5mm y una distancia entre patillas de 1,5cm, grosor de las patillas es de 0.8mm. Ponemos la medida en mm ya que facilita la interpretacion

- Introducimos una nueva herramienta que permite "añadir un falso origen de coordenadas" denominada "***False Origin***"  y que facilitará el dimensionado de las partes de nuestro encapsulado.

- Añadimos los taladros de nuestro componente, seleccionando los PADs correspondientes y colocaremos de forma que cumplan la distancia que deseamos entre patillas, en nuestro caso esta distancia será de 150mm, a continuación dibujamos el cuerpo de nuestra resistencia, como se dijo será de unos 5mm por lo que se utilizara un recuadro con la herramienta "***2D GRAPHICS BOX MODE***"  . Podemos dibujar también las patillas de la resistencia, sin más que llevar lineas desde cada uno de los PADs al cuerpo de nuestro elemento, mediante la herramienta "***2D GRAPHICS LINE MODE***" como se muestra en la siguiente figura:

Figura II.31. Creación del encapsulado de una resistencia

- Con el componente ya diseñado el siguiente paso consistirá en poder unir todas las partes del mismo en un solo encapsulado, es decir juntar los PADs con las líneas que dibujan el contorno de nuestra resistencia, para ello disponemos de la herramienta "**Make Package"**  situada en el menú Library. Al pulsar sobre esta herramienta nos aparece la siguiente

ventana (figura II.32.), donde se debe ingresar: *nombre del encapsulado, categoría, tipo de encapsulado, alguna descripción*

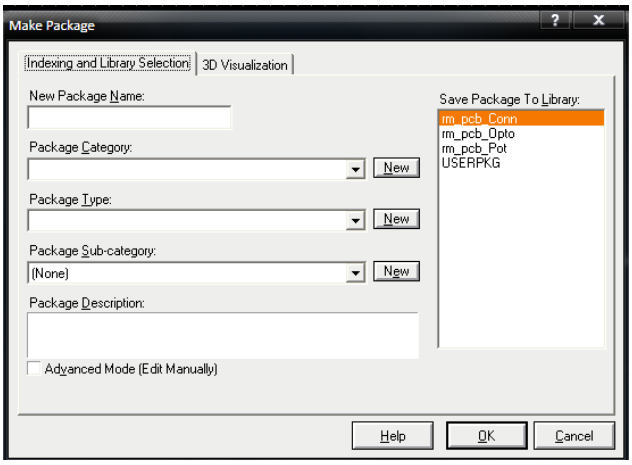


Figura II.32. Ventana de Make Packgace

Una vez realizado esto podemos disponer de nuestro encapsulado, es recomendable guardar todos los encapsulados creados en una solo librería

- **Diseño de PCB (Circuito Impreso)**

Para esta operación se partirá de un circuito realizado en ISIS, es decir disponemos del esquemático realizado previamente

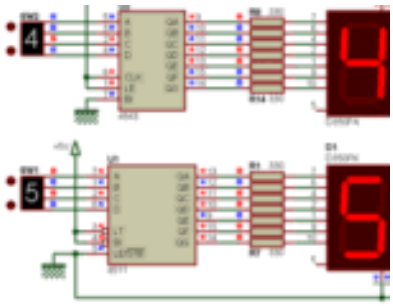


Figura II.33. Circuito esquemático realizado en ISIS

Con el diseño ya completo nos cerciooraremos de que la lista de uniones es la correcta, para esto iremos a la opción "***Design Explorer***" que se encuentra en el menú ***Design.***

Una vez realizada esta acción se nos abrirá una ventana en la que encontraremos todos los componentes de nuestro circuito con sus correspondientes conexiones. Aquí deberemos tener en cuenta que todos nuestros componentes que tengan algún contacto con masa (GND) o con VCC estén en todos denominados de igual modo.

Figura II.34. Listado de elementos

Para generar el listado de conexiones, escogeremos la herramienta "***Netlist to Ares***" del menú TOOLS

Realización PBC en Ares

- Primeramente se debe limitar la placa PCB, para esto se debe escoger la herramienta "***2D Graphics Box***" , y seleccionar la capa Board Edge, con esto ya podemos realizar el borde de nuestra PCB.

  Una vez delimitada la placa, el siguiente paso es el posicionamiento de los elementos, para eso se debe tener el encapsulado de todos los componentes.

Posicionamiento Automático.- Realizado por ARES, para lo cual bastará con seleccionar dentro del menú *Tools* la herramienta **"Auto Placer"**. Para poder utilizar esta herramienta, es necesario haber definido previamente los límites de nuestra placa.

Ruteado de las Pistas.- Con los componentes ya dispuestos en su posición, pasamos a realizar el ruteado de las pistas. Se debe tener en cuenta que las líneas "verdes" son las líneas correspondientes a las uniones (netlist) entre los componentes, es decir las líneas que indican qué está conectado con qué.

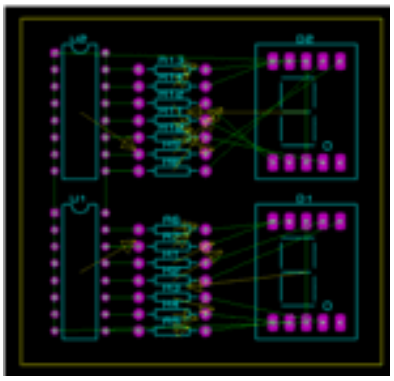


Figura II.35. Ruteado de Pistas

Mediante la herramienta **"Auto Router"**  del menú *Tool*, se visualizará una pantalla en la que indicaremos el grid, las pistas a ruta, etc.

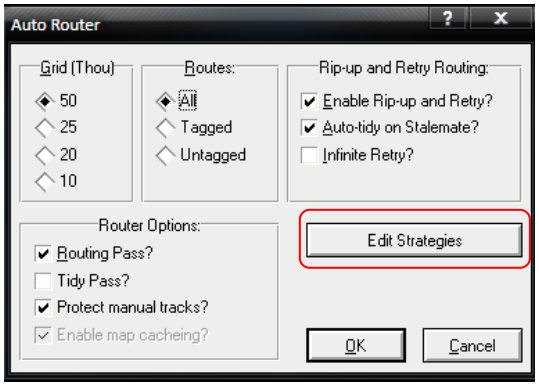


Figura II.36. Pantalla de Auto Router

Lo más sobresaliente de la ventana *Auto Router* será el botón de **Edit Strategies,** donde Podremos elegir si deseamos realizar el rutado a una sola capa o si por el contrario vamos a utilizar más de una, para ello debemos realizar lo siguiente:

Si vamos a trabajar con una sola capa, dentro del primer PAR de capas (Horz-Vert) seleccionaremos como horizontal la Bot Copper y en Vertical seleccionaremos NONE. Si deseásemos 2 o más capas en vez de seleccionar NONE proseguiríamos con la capa que nos interesase.

Es recomendable al terminar el ruteado realizar un chequeo completo del circuitos para detectar posibles errores, para ello podemos usar las herramientas "***Design RulesChecker"*** que nos indicará si hemos cometido algún error, tales como distancias entre pistas, de pista a pad, etc, y mediante la opción ***"Conectivity Rules Checker"*** que permite verificar si todas y cada una de las conexiones que estaban establecidas han sido ruteadas de forma correcta.

Con esto quedaría finalizado el diseño de la placa, de forma que ya estaríamos listos para obtener los ficheros de taladrado, GERBER.

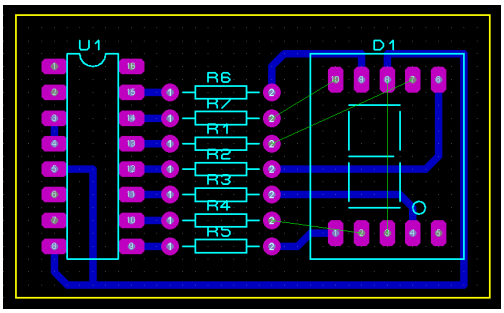


Figura II.37. Ruteado completo

Ruteado Manual.- Al igual que el ruteado automático, los componentes deben estar ubicados dentro de los límites de la placa, la diferencia que para unir los elementos, se utiliza la herramienta ***TRAC MODE*** 

Las versiones de proteus superiores a la 7.0 presenta la opción de visualización en 3D, la que nos da una prospectiva casi real como quedaran los elementos montados en la placa, para generar esta vista en la barra de menú seleccionamos ***Output*** y escogemos ***3D Visualization***

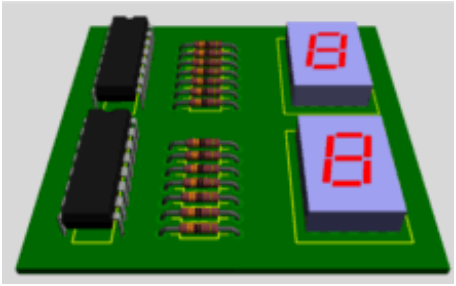


Figura II.38. Visualización 3D de PCB

CAPÍTULO III

SISTEMA BIOMÉTRICO Y LECTOR DE HUELLAS DACTILARES

3.1 SISTEMA BIOMÉTRICO

La palabra biometría deriva de dos palabras: bio (vida) y metría (medida). La ciencia biométrica se define como el análisis estadístico de observaciones biológicas.

La biometría, es la aplicación de estos métodos estadísticos y del cálculo al estudio de los seres Vivos. La identificación biométrica es entonces, la verificación de la identidad una persona midiendo digitalmente determinados rasgos de alguna característica física o psicológica.

Los seres humanos poseemos características que nos hacen diferenciar unos de otros, las cuales pueden ser: las huellas dactilares, la posición de las venas, la cara, la voz, la retina del ojo, entre otros.

Se entenderá por sistema biométrico a un sistema automatizado que realiza funciones de biometría. Es decir, un sistema que basa sus decisiones en reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automática.

Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores

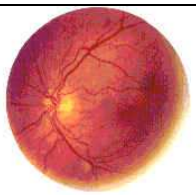
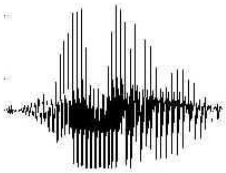
 a) Rostro	 b) Termograma facial	 c) Huella Dactilar
 d) Geometría de la mano	 e) Venas de la mano	 f) Iris
 g) Patrones de la retina	 h) Voz	 i) Firma.

Figura III.39.Técnicas Biométricas

Estas técnicas biométricas toman en consideración lo atómico y lo del comportamiento de una persona, por esta razón se debe tomar en consideración cual técnica utilizar, por ejemplo la huella dactilar es la misma día a día, con excepción si ha tenido algún daño físico, a diferencia de la firma que puede ser influido por factores psicológicos no intencionales.

Con las técnicas detalladas anteriormente se podrá dividir en dos grupos a los sistemas biométricos:

- **Sistemas Físicos:** Permiten el análisis y la verificación en diferentes partes del cuerpo humano como son: Huella Digital, palmar, geometría de la mano o la cara.

- **Sistemas Psicológicos:** Con estos sistemas se evalúan de forma psicológica de dos características del cuerpo humano, mediante la voz y la firma textual

3.1.2CARACTERÍSTICAS DEL SISTEMA BIOMÉTRICO PARA IDENTIFICACIÓN PERSONAL

Las características básicas que un sistema biométrico para identificación personal debe cumplir se puede resumir en:

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato".

La fiabilidad, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc

3.1.3 ARQUITECTURA DEL SISTEMA BIOMÉTRICO PARA IDENTIFICACIÓN PERSONAL

La arquitectura típica de un sistema biométrico se presenta en la Figura III.39. Esta puede entenderse conceptualmente como dos módulos:

- ✓ Módulo de inscripción
- ✓ Módulo de identificación

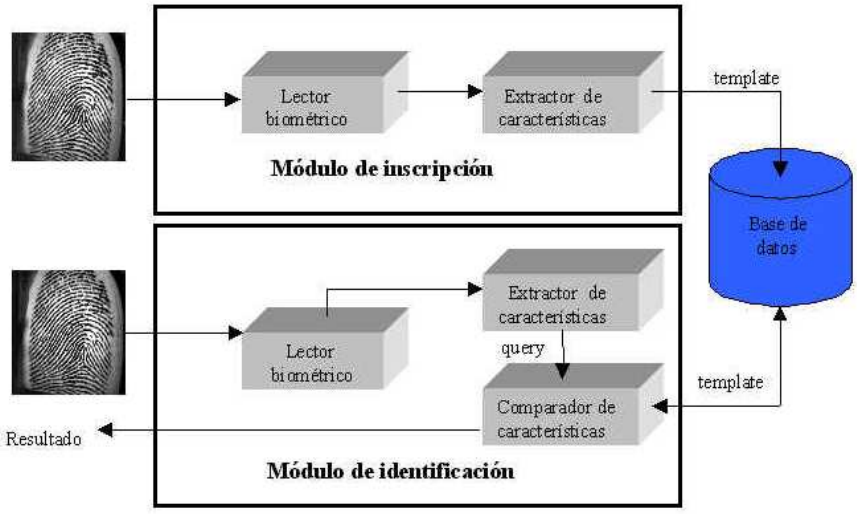


Figura III.40. Arquitectura de un sistema biométrico para identificación personal

Módulo de inscripción

Se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder comparar a ésta, con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El ***lector biométrico*** se encarga de adquirir datos referentes al indicador biométrico elegido y entregar una representación en formato digital de éste. El ***extractor de características*** saca, a partir de la salida del lector, características representativas del indicador biométrico, que será almacenado en una base de datos central u otro medio como una tarjeta, recibirá el nombre de *template*. En otras palabras un *template* es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso

Módulo de identificación

Es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza 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 los *templates*. La representación resultante se denomina *query* y es enviada al comparador de *características* que confronta a éste con uno o varios *templates* para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de *fase de inscripción*, mientras que los procesos realizados por el módulo de identificación reciben la denominación de *fase operacional*. A continuación se entregan detalles de esta última.

3.1.4 EXACTITUD EN LA IDENTIFICACIÓN

Una decisión tomada por un sistema biométrico diferencia entre "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1. Una persona autorizada es aceptada,
2. Una persona autorizada es rechazada,
3. Un impostor es rechazado,
4. Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. Por lo tanto, las estadísticas anteriores se utilizan para establecer dos tasas de errores:

1. **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,
2. **Tasa de falso rechazo** (***FRR***: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.

La FAR y la FRR son funciones del grado de seguridad deseado. 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. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la figura 2. El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

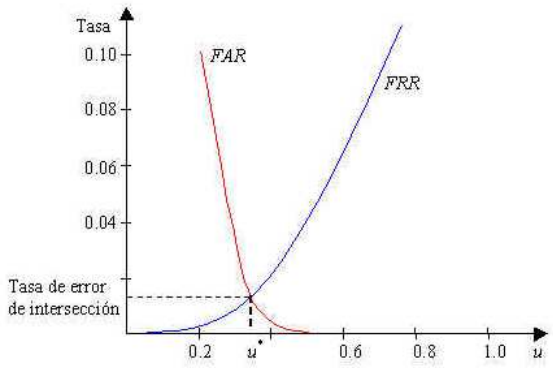


Figura III.41. Grafica típica de la tasa de falso rechazo (FRR) y de falsa aceptación (FAR) para un sistema biométrico

3.1.5 SISTEMA BIOMÉTRICO BASADO EN HUELLA DACTILAR

Son sistemas que basan sus decisiones de reconocimiento tomando como característica personal la huella dactilar. De acuerdo con el modo de operación en que trabajen estos son conocidos como:

- **AFIS**

Automatic Fingerprint Identification System (Sistema Automático de Identificación por Dactilares), Consiste en conocer solo la imagen de la huella dactilar y compararla con las existentes en la base de datos para hallar la identidad de la persona a la que pertenece dicha huella (1:n). Estos sistemas tienen una gran demanda pero su tecnología sigue aun en estudio por que presenta aun fallas

- **AFAS**

Automatic Fingerprint Authentication System (Sistema Automático de Verificación por Huellas Dactilares), consiste en obtener una imagen de la huella dactilar de una persona, de la cual conoce su identidad, para compararla con la que esta almacenada en la base de datos y verificar si la huella dactilar pertenece a esa persona (1:1)

3.1.5.1 APLICACIONES DE SISTEMA BASADO EN HUELLAS DACTILARES

Las aplicaciones pueden ser divididas principalmente en los siguientes grupos:

Comerciales: Tales como el acceso a las redes de computadoras, seguridad de datos electrónicos, comercio electrónico, tarjetas de crédito, control de acceso físico, teléfonos celulares, etc.

Gubernamentales: Tales como en documentos de identificación personal, licencias de conducir, seguridad social, pasaportes etc.

Forenses: Identificación de cadáveres, investigaciones criminales, identificación de personas extraviadas etc.

3.2 HUELLAS DACTILARES

Las huellas dactilares son patrones constituidos por rugosidades en forma de salientes llamadas crestas papilares y depresiones llamadas surcos interpapilares o valles. Se forman a partir del sexto mes, manteniéndose invariables a través de la vida del individuo, a menos que sufra alteraciones debido accidentes tales como cortes o quemaduras, estas tienen la característica de

ser única e irrepetible, tanto en los mismos dedos de la persona como en gemelos, trillizos. Se estima que la probabilidad de que dos personas tengan la misma huella dactilar es aproximadamente de 1 en 64.000 millones

Las impresiones dactilares son las reproducciones resultantes de la huella dactilar sobre una superficie plana, permaneciendo almacenada en formato analógico (papel) o formato digital (archivo), en estas las crestas papilares se aprecian como líneas más oscuras y los surcos como líneas más claras.

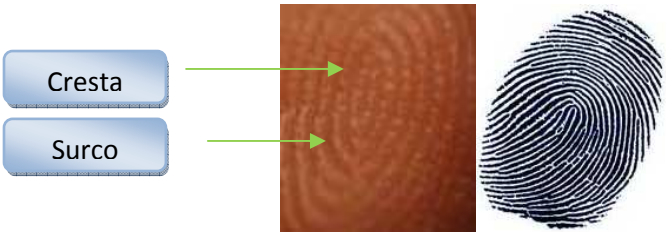


Figura III.42.a) Huella Dactilar b) Impresión Dactilar

3.2.1 CARACTERÍSTICAS GLOBALES

Son patrones geométricos de las crestas que son reconocibles a simple vista, usualmente la determinación del patrón al que pertenece la huella dactilar se obtiene mediante el conocimiento de sus puntos singulares.

Área Patrón.- Es la parte principal de la huella dactilar y está constituida por las crestas y todas sus características

Líneas Tipo.- Son definidas como dos crestas que se inician paralelamente y divergen sobre el área patrón, estas crestas pueden ser continuas o no. (Ver figura Figura III.43.)

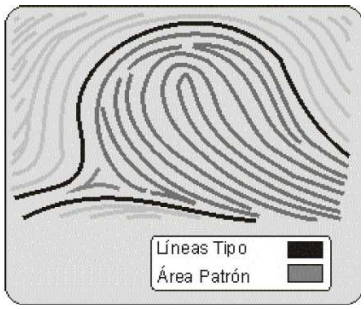


Figura III.43. Área Patrón y Línea Tipo

- **Puntos Singulares**

Punto Core.- Esta localizado dentro del área patrón, en donde las crestas presentan una mayor curvatura, normalmente suele tomar el punto más alto de la cresta central. Las técnicas para su determinación son muy complejas

Punto Delta.- Es el punto de divergencia de la líneas tipo, más internas que tienden a envolver el área patrón. Un *Delta* es un triángulo constituido por las crestas que pueden formarse de dos maneras: por la bifurcación de una línea simple o por la brusca diferencia de dos líneas paralelas.

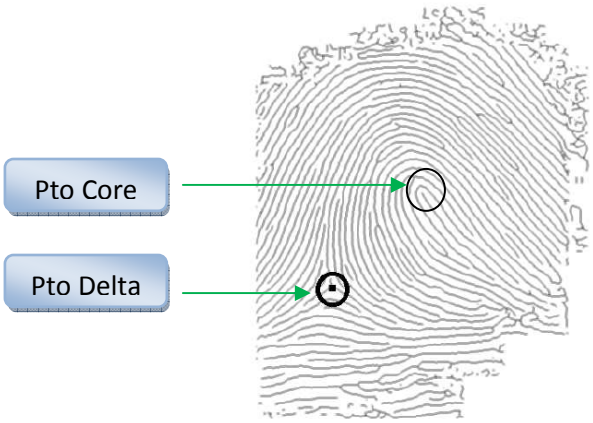


Figura III.44. Representación de los puntos singulares

3.2.2 CARACTERÍSTICAS LOCALES

Las características locales implantan la individualidad de la huella dactilar, están representados por puntos conocidos como minucias. Las crestas en una huella dactilar no son continuas, ni

rectas, sino más bien cambian de dirección, cortándose y bifurcándose. Los puntos en donde los cambios ocurren son denominados ***minucia.***

En una imagen de alta calidad es posible encontrar entre setenta y cien minucias, siendo suficiente información para determinar la individualidad de una persona. Los tipos de minucias más comunes son (Figura III.45.):

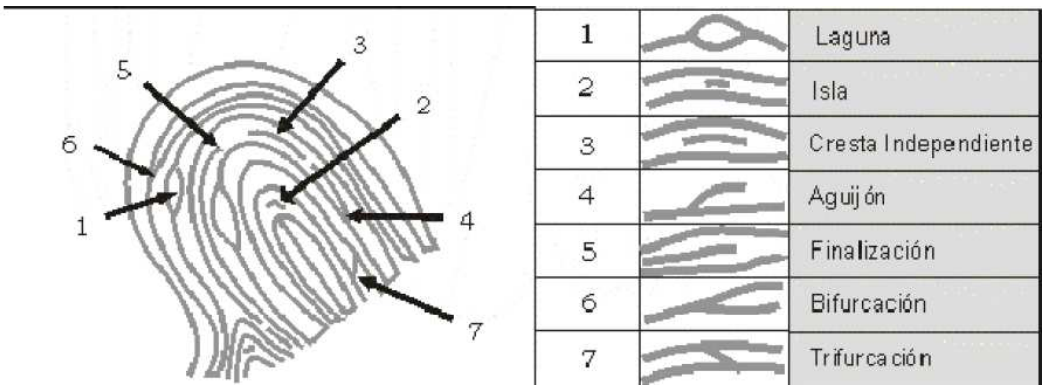


Figura III.45. Tipo de minucias

1. **Laguna.-** Es una cresta que se divide en dos ramas y se unifica nuevamente luego de recorrer una distancia corta creando un área determinada
2. **Isla.-** Es la cresta más pequeña que se puede encontrar en una huella, a tal grado que es semejante a un punto.
3. **Cresta Independiente.-** Es una cresta muy corta pero lo suficientemente grande para no ser una isla, no tiene bifurcación u otra división y está rodeada de valles.
4. **Aguijón.-** Es una cresta que se divide en dos ramas y una de estas recorre una distancia muycorta
5. **Finalización.-** Es el punto donde la cresta termina abruptamente
6. **Bifurcación.-** Es el punto donde se separan o encuentran las líneas la cresta y se divide en dosramas
7. **Trifurcación.-** Es producida por la unión de dos minucias de bifurcación.

3.2.3 ADQUISICIÓN DE HUELLAS DACTILARES

Para determinar si una huella es correcta el usuario debe colocar el dedo sobre el lector para adquirir una imagen, seguidamente se filtrara para obtener una imagen clara y extraer la minucias.

Con este grupo de minucias, el software del sensor de huella digital genera un modelo en dos o tres dimensiones dependiendo de la tecnología utilizada. Las minucias se representan por una combinación de números (x,y) dentro de un plano y por un ángulo, los cuales vienen a servir como base para crear un conjunto de vectores que se obtienen al unir los puntos de las minucias entre sí mediante rectas que tienen un ángulo y dirección, generando una determinada figura única e irrepetible.

Para llevar a cabo el proceso inverso o verificación dactilar se utilizan estos mismos vectores y no imágenes

			
Captura la imagen de la huella dactilar	Identifica y Codifica la minucias	Genera una plantilla con la minucias	Vectorización

Figura III.46. Adquisición de Huella Dactilares

En la figura III.47. se muestra un diagrama de bloque de sistema AFAS que es un sistema biométrico basado en el modo de operación para la identificación de huella dactilar. En este pueden apreciarse diferentes fases necesarias para la verificación de la identidad de una persona, en base a la característica de la huella dactilar

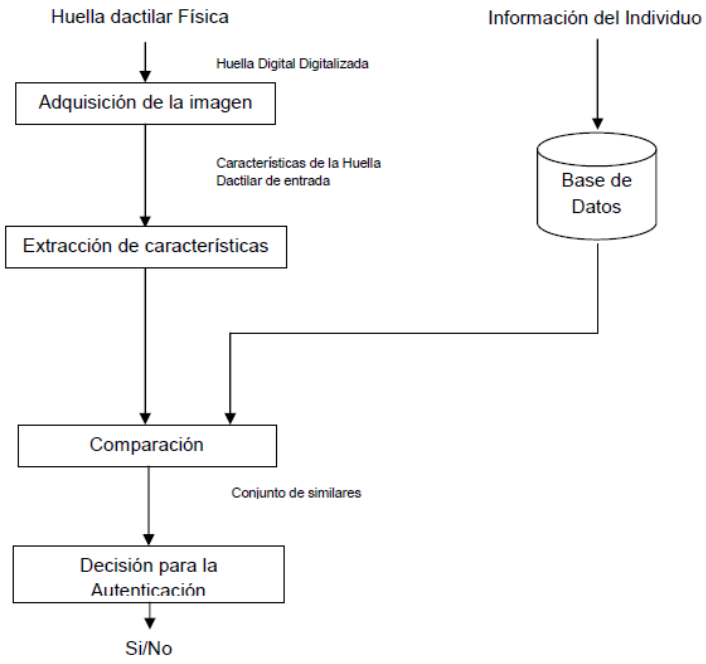


Figura III.47. Diagrama de Bloques sistema AFAS

Naturalmente, para poder identificar a una persona mediante sus minucias de su huella es necesario poder representar estas últimas para poder compararlas. La representación estándar consiste en asignar a cada minucia a su posición espacial (x,y) y una dirección, que es tomada respecto al eje x, en sentido anti horario.

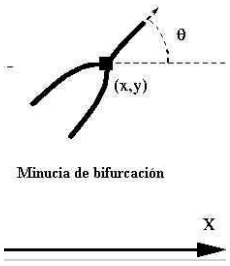


Figura III.48. Representación de una minucia

3.3 DETECTORES DACTILARES

Para la adquirir una imagen digital de una huella dactilar, existen diversos sensores que nos brindan una lectura utilizando diferentes tecnologías. Entre los sensores principales tenemos:

- **Sensores Ópticos**

El sensor óptico utiliza una cámara CCD (Dispositivo de carga acoplada) o CMOS, el cual tienen un arreglo de LEDs sensibles a la luz, que generan una señal eléctrica en respuesta a variaciones de luz.

El proceso de lectura inicia cuando el dedo es colocado sobre el prisma, el cual tiene una fuente de alumbrado (LEDs), que sirve para iluminar las crestas y surcos de la huella dactilar, y reflejar al CCD que genera la imagen invertida, con áreas más obscuras que representan más luz reflejada (crestas del dedo), y con áreas más claras que representan menos luz reflejada (los surcos del dedo).

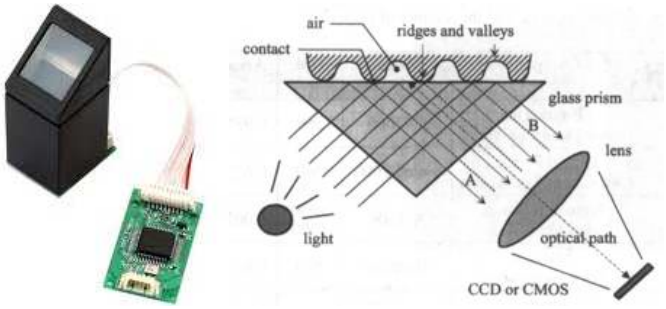


Figura III.49. a) Sensor Óptico b) Funcionamiento

La desventaja es que en ocasiones puede permanecer en la superficie del sensor algunos rasgos del dactilograma anterior

Las empresas líderes en la producción de este escáner son: Delay, Dermalog, Smiths, Heiman Biometrics

- **Sensores Capacitivos**

Al igual que el sensor anterior este genera una imagen de las crestas y surcos, pero en vez de hacerlo con luz, los capacitores utilizan la corriente eléctrica. En la superficie del circuito integrado de silicona se dispone de un arreglo de celdas, sensores capacitivos; la capacitancia (habilidad parar almacenar carga) de cada celda (pixel) es medida individualmente, gracias a esta cualidad, el capacitor en una celda bajo una cresta tendrá una mayor capacitancia que la almacenada en un surco o valle.

El procesador del lector lee esta salida de voltaje y determina si es característico de una cresta o valle, y podrá construir una imagen de la huella.

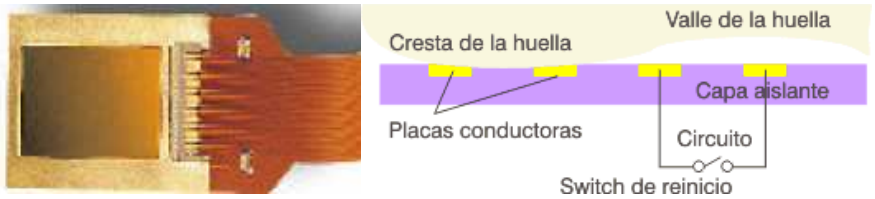


Figura III.50. a) Sensor Óptico b) Funcionamiento

La desventaja es que puede presentar problemas si la yema del dedo esta húmeda o muy seca, en este caso se obtendrán imágenes negras o pálidas

Entre las empresas líderes en este sector se encuentran: Infineon, Verdicom, Sony, y ST Microelectronics

- **Sensor Termoeléctrico**

Utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos.

El método termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip.

- **Sensores de Campo eléctrico (E-Field)**

Este sensor funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). Esta tecnología origina un campo entre el dedo y el semiconductor adyacente que simula la forma de surcos y crestas epidérmicas, reproduciendo una imagen clara que corresponde con mucha exactitud a la huella dactilar.

- **Sensores sin contacto**

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico produciendo una distorsión de la imagen, adicionalmente necesita de un algoritmo más complejo

3.3.1 MODULO DE HUELLA DACTILAR NITGEN FIM3040 LV

Figura III.51.Módulo de Huella Dactilar Nitgen FIM3040-LV

Es un módulo de reconocimiento de huella digital autónomo está 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 FIM3040-LV ofrece una alta capacidad de reconocimiento y una gran velocidad para operaciones de identificación 1:N y verificación 1:1.

La carga de datos en memoria se hace localmente desde el mismo sensor óptico. El FIM30 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 ofrece un entorno de desarrollo cómodo y seguro para aplicaciones off-line.

En aplicaciones off-line habitualmente se guardan los usuarios en la memoria del equipo (para hasta 100 dedos, cada dedo registra 2 veces la huella dactilar) y se identifica usando el motor de búsqueda del algoritmo interno.

El módulo de reconocimiento biométrico de huella dactilar FIM30 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.

Las características técnicas se detallan en el datasheet del dispositivo (**ver anexo 1**)

- **Principales Características**

- ✓ Funcionalidad de identificación de huella dactilar on-line y off-line incorporada.
- ✓ Tasa de identificación 1:1 y 1:N muy elevada: FAR : 1/100.000 y FRR : 1/1.000
- ✓ Algoritmo y sensor óptico de elevada dureza
- ✓ Alto grado de precisión en la identificación, incluso con huellas de pequeño tamaño, húmedas o secas
- ✓ Rápida adquisición de todo tipo de huellas prácticamente bajo cualquier condición.
- ✓ Memoria para 100 huellas dedos (cada dedo registra 2 veces la huella dactilar).
- ✓ El acceso al dispositivo desde el host puede protegerse por huella o password.
- ✓ Ofrece un entorno de desarrollo cómodo sin necesidad de conexión a PC (aplicaciones off-line)
- ✓ 2 puertos de comunicaciones RS-232 para conexión a PC o host (aplicaciones on-line)
- ✓ Protocolo de comunicaciones ASCII
- ✓ Tensión de alimentación de 3,5 V
- ✓ Tamaño reducido, robustez y larga vida sin mantenimiento

- **Aplicaciones**

- ✓ Sistemas de control de acceso
- ✓ Sistemas de control de presencia
- ✓ Sistemas de gestión de asistencia laboral
- ✓ Cajas fuertes
- ✓ Control de vehículos, maquinaria y equipos electrónicos

- ✓ Otras aplicaciones en las que se requiera identificación cómoda y segura para el usuario (sin posibilidad de suplantación de identidad)

CAPÍTULO IV

DISEÑO DE HADWARE Y SOFTWARE DE LOS SISTEMAS

Introducción.

En este capítulo se detallara los circuitos de conexión así como los diagramas de flujo que servirán de base para desarrollar el programa en cada sistema. De la misma manera se especificara el funcionamiento de los circuitos en base a los requerimientos de la institución.

4.1 UBICACIÓN DE LOS SISTEMAS

El sistema de seguridad y control de acceso será implementado en el Colegio Fernando Daquilema, para brindar seguridad a las oficinas del rectorado y secretaria, que se encuentra en el segundo piso del primer bloque. Se escogió estos lugares previo acuerdo con las autoridades de la institución y por ser lugares donde se requiere un elevado nivel de seguridad, ya que en estas aéreas es donde se encuentran la documentación de vital importancia y equipos informáticos.

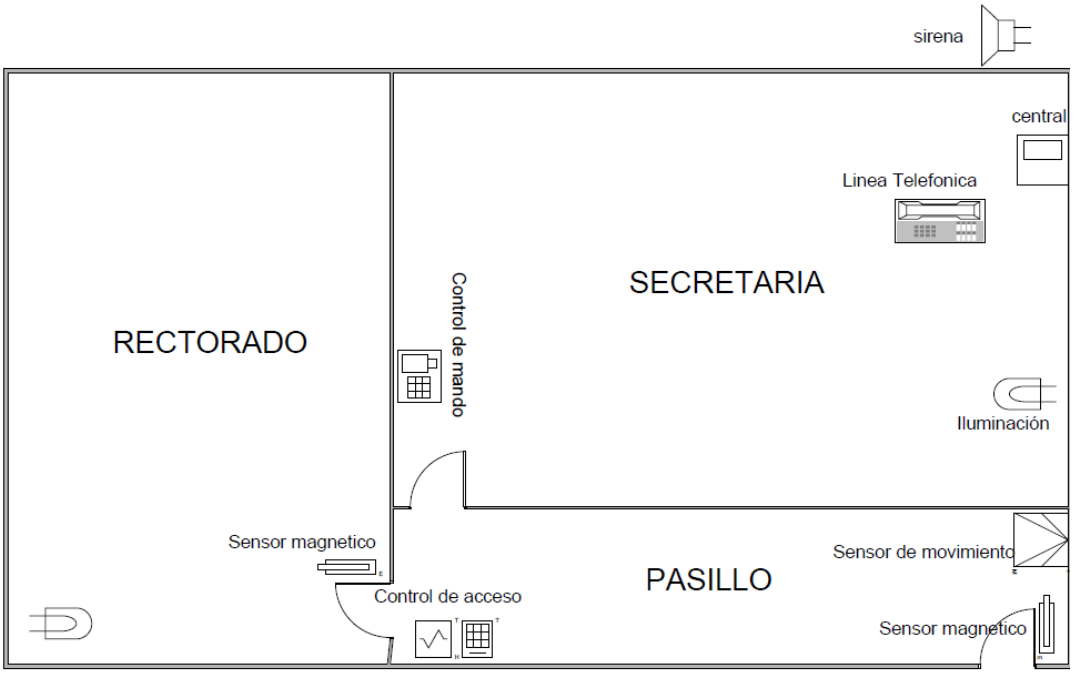


Figura IV.52. Ubicación de sistema de seguridad

4.2 REQUERIMIENTOS DEL SISTEMA DE SEGURIDAD

En base al nivel de seguridad requerido en la institución se establecieron los siguientes requerimientos:

El sistema de seguridad visualizara en el LCD varias opciones como son:

- Un menú el cual nos guiara para activar o cambiar de clave para la alarma.
- Ingreso correcto o erróneo de la clave
- Tiempo de salida

- Llamada de emergencia
- Si un sensor ha sido activado

La alarma se activara al ingresar una clave, si esta es mal ingresada se bloqueara el teclado y no se encenderá la alarma.

- Para desbloquear el teclado se presionara la letra “A”, y nos permitirá ingresar nuevamente la clave de activación.
- Una vez activada la alarma, entra a un temporizador de salida de 60 segundos antes que empiece a funcionar los sensores.
    - antes de que este tiempo termine se puede apagar la alarma

Después de ingresar la clave de activación de alarma exitosamente y finalizado el temporizador de salida los sensores se activaran, empezaran a detectar que no existan alteraciones dentro del área.

- Si se detecta alguna anomalía pasa a un temporizador de ingreso para apagar la alarma este es de 25 segundos, se ha considerado esto por el motivo que el horario de entrada del personal administrativo es a las 8 am, y los estudiantes de la institución se encuentran en clases, y al activar la sirena inmediatamente, interrumpiría las actividades que se realizan en el colegio
- ✓ Una vez culminado el temporizador de ingreso, se encenderá la sirena y la iluminación, seguidamente pasara a un temporizador de pánico, que nos dará un tiempo de 90 segundos, para apagar el sistema ingresando la clave. Si en este temporizador no es desactivada la alarma, realizara una llamada de emergencia.

Si se desea cambiar la clave de activación, se lo debe realizar cuando la alarma está apagada, y visualizamos el menú de opciones, se seleccionara la opción 2

- Se solicitara que ingrese la clave actual y luego la nueva clave.

Adicionalmente para que el usuario interprete fácilmente las señales se ha colocado diodos led para ver las zonas alteradas. Las claves serán ingresadas mediante un teclado de 4x4.

4.3 DISEÑO DE HARDAWARE DEL SISTEMA DE SEGURIDAD

4.3.1 ETAPAS DE SISTEMA DE SEGURIDAD

El sistema de seguridad está compuesto básicamente de tres etapas: la etapa Detección (sensores), procesamiento (central), y la respuesta (actuadores y monitoreo). Estos tienen diferentes funciones, pero están relacionados entre sí para cumplir con una sola tarea, que es advertir de cualquier allanamiento al área protegida.

Como se menciono anteriormente el sistema de seguridad está compuesto de 3 etapas principales como se puede observar en la figura IV.53, así como del monitoreo del sistema mediante RTB (Red Telefónica Básica)

Figura IV.53. Etapas del sistema de seguridad

Una vez establecidos el nivel de seguridad se utilizará los siguientes circuitos para activar los diferentes sensores y actuadores

4.3.2 CIRCUITOS DE LA ETAPA DE DETECCIÓN

Para esta etapa se utilizará sensor de movimiento PIR, el cual nos dará una protección interior, y para reforzar la seguridad se utilizará sensor magnético, este dará una protección perimetral, estará ubicado en la puerta del área protegida, aquí también se analizará la conexión del teclado el cual nos permitirá activar o desactivar nuestro sistema

- **Circuito del Sensor Comet PIR**

El sensor detecta el movimiento mediante el promedio de calor irradiado en el tiempo, como respuesta a la variación de calor vamos a interpretar como un cambio lógico 0L o 1L. Mediante el

siguiente circuito (ver Figura IV.55). Es inmune a mascotas y a falsas alarmas por lo que cumple con las necesidades de la institución requiere

Los bornes de conexión del dispositivo se muestra en la figura IV.54, las especificaciones son:

- Voltaje de Operación : 9 a 16 VDC
- Corriente max 12mA
- Contacto de Alarma N.C
- Contacto de Temper N.C
- Compensación Automática de Temperatura

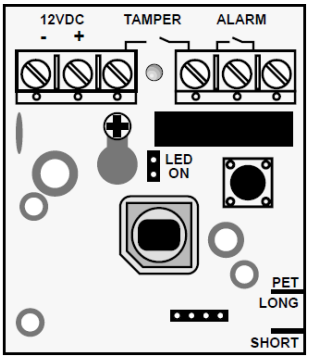


Figura IV.54 Bornes de conexión del sensor Comet PIR

El diseño se está realizando con microcontroladores y necesitamos que nos dé niveles lógicos para que puedan ser interpretados, tomando en consideración que cuando detecta movimiento el led del dispositivo se enciende, y la el circuito de la alarma, cambia de N.C pasa a N.A, por lo que la interpretación quedaría:

- Cuando detecta movimiento es igual a 0 lógico
- Cuando no detecta movimiento es 1 lógico.

Se puede decir que la alarma del dispositivo está actuando como un interruptor para cambiar de un nivel a otro, por lo que el borne de la alarma del sensor PIR le conectamos a 5VCD.

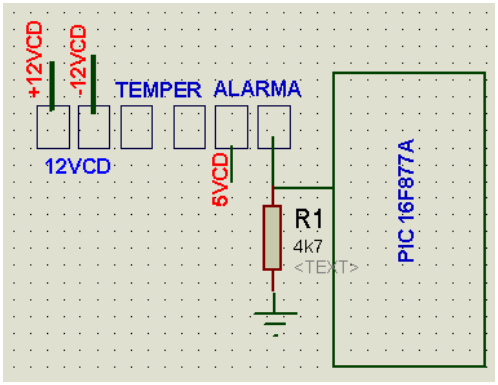


Figura IV.55 Circuito de conexión del sensor PIR al microcontrolador

Estado 1

No detecta movimiento, interruptor cerrado

Vin = 5 VCD

R = 4,7 KΩ

$$I = \frac{Vin}{R1} = \frac{5}{4700} I = 1{,}06mA$$

$$V1 = R1 * I$$

$$V1 = 4{,}98\,VCD = 1L$$

Estado 2

Detecta movimiento, interruptor Abierto

Vin = 0VCD por lo tanto V1 = 0L

Con esta conexión él µC puede interpretar fácilmente el cambio de nivel y ser programado para que cuando el sensor entregue un valor de 1L, no encienda los actuadores, y si el dispositivo da un valor de 0L encienda los actuadores. Adicionalmente si el cable de conexión que va desde el sensor al PIC, es cortado, automáticamente cambia de nivel por lo que garantiza una detección óptima.

- **Circuito del Sensor Magnético de apertura**

El funcionamiento de este sensor es muy sencillo, al estar las dos piezas unidas el circuito esta N.C, pero cundo se separan (se abre la puerta) el circuito se abre, este dispositivo se lo ubica en puertas y ventanas. Ahora se necesita niveles lógicos para la interpretación del microcontrolador, por lo que se realizo el siguiente circuito:

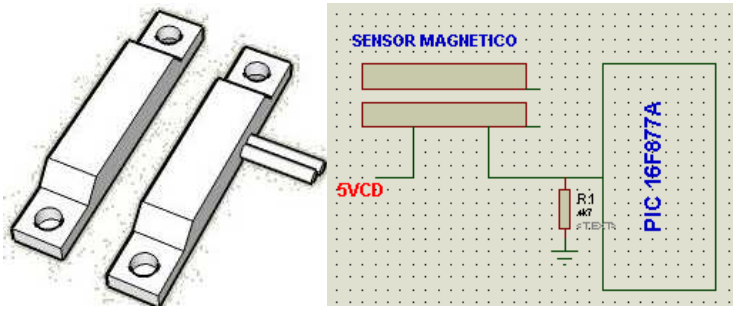


Figura IV.56. Circuito de conexión del sensor magnético al microcontrolador

Con este circuito, se obtiene los niveles lógicos necesarios, cuando se separa el sensor nos dará 0 lógico y cuando esta unido (cerrada la puerta) nos dará un valor de 1 lógico. Estos niveles son los óptimos para procesar las señales en el microcontrolador el cual va cumplir la función de procesamiento. Como se puede notar realiza la misma función que el circuito de conexión del sensor PIR.

- **Circuito de Conexión del Teclado**

Los teclados son útiles para ingresar los datos, para luego ser procesados y tener respuestas, por lo que este dispositivo es de gran utilidad en sistema de seguridad para que el usuario pueda activar o desactivar la alarma. El teclado que se utilizará es un matricial de 4x4 que dispone de un conector simple de 8 pines que corresponden con las 4 filas y 4 columnas

Figura IV.57. Teclado matricial 4x4

Para entender su funcionamiento, podemos observar su estructura interna en la siguiente figura:

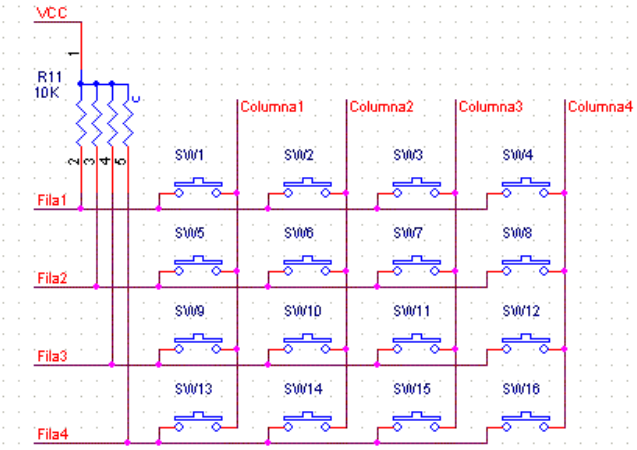


Figura IV.58. Estructura interna teclado 4x4

El teclado está compuesto de una serie de pulsadores conectados entre sí, formando una matriz, con sus respectivas filas y columnas, por lo que se puede conectar a 1L o 0L.

Para que nuestro circuito funcione óptimamente al conectarse al micrcontrolador, necesitamos conectar 5VCD a las filas del teclado y en serie una resistencia de 4,7KΩ para proteger nuestro circuito con esto obtenemos que la corriente sea de 1mA, suficiente porque el PIC soporta hasta 25 mA:

$$I = \frac{E}{R} = \frac{5}{4,7} = 1mA$$

Finalmente la conexión del teclado quedaría como se muestra en la figura IV.59, tómese en cuenta que para realizar la simulación la conexión se ha utilizado programa PROTEUS, y el teclado que aquí se visualiza, no coincide con el orden de los números del teclado real.

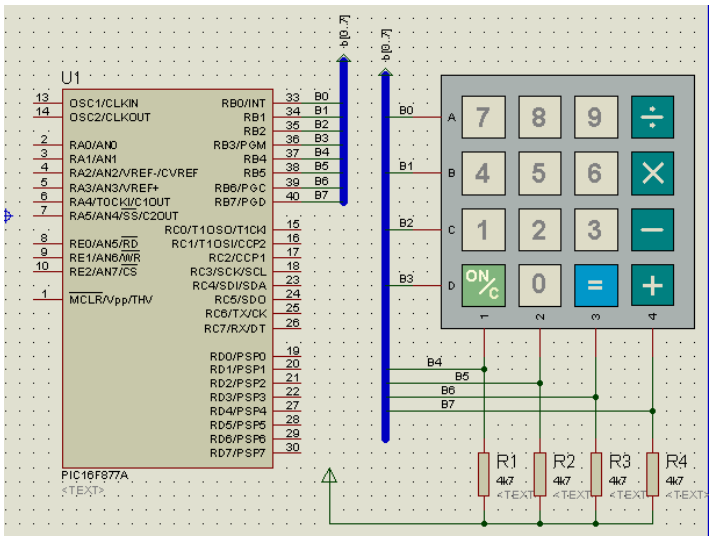


Figura IV.59. Circuito de conexión del teclado 4x4 al microcontrolador

Para una lectura del teclado se realiza un barrido, es decir se apaga o se envía un 0L atreves del microcontrolador a una columna y se compara que fila ha cambiado de estado, esto ocurre cuando una tecla es presionada; en el siguiente ejemplo se detalla este funcionamiento:

LOW B

IF UNO = 0 THEN

NUM = 4 : RETURN

ENDIF

IF DOS = 0 THEN

NUM = 5 : RETURN

ENDIF

IF TRES = 0 THEN

NUM = 6 : RETURN

ENDIF

IF CUATRO = 0 THEN

NUM = 0 : RETURN

ENDIF

HIGH B

Se puede observar que se apaga la columna B, y se procede a comparar si la fila uno es igual a 0 entonces en la variable **num** almacena el valor 4, caso contrario compara si la fila dos es igual a 0 si estos sucede almacene en la variable **num** el valor 5, este procedimiento se repite para el resto de filas de la columna B, así mismo se lo realiza para las columnas restantes.

Se toma en consideración que el µC para que lea una línea de comando es de un milisegundo, y para que una persona presione una tecla y libere rápidamente la misma, requiere como mínimo 100 milisegundos, en ese tiempo el PIC realiza como mínimo 10 barridos, por lo que seguro detectara inmediatamente una tecla pulsada, por lo que también se recomienda realizar un control anti-rebote es decir un procedimiento que detecte cuando la tecla se ha liberado para que no sea leída varias veces.

4.3.3. ETAPA DE RESPUESTA

Cuando el sistema ha sido alterado, en respuesta se producirá una acción que advierta de esta anomalía, para esto se utilizará emisión de sonido mediante sirena, iluminación, y una llamada telefónica a un centro de control. Esta acción es disuasoria ante la presencia de algún intruso dentro del área protegida, adicionalmente se analizará la conexión del LCD.

- **Circuito de sirena**

La sirena nos advertirá que el sistema ha sido alterado, mediante la emisión de un sonido de dos tonos. Este dispositivo tiene las siguientes características:

- Alimentación 12VCD
- Potencia de 30 W
- Sirena de dos tonos

Por lo general los actuadores necesitan voltajes superiores a los 5VCD, por que manejan potencias elevadas. El microcontrolador nos envía niveles lógicos para activar o desactivar los actuadores, por lo que se ha utilizado un circuito de conmutación para facilitar la operación de la sirena. Para esto se ha empleado:

Un relé de 12VCD

Transistor 2N3904

Diodo Rectificador

Resistencia de 4,7KΩ

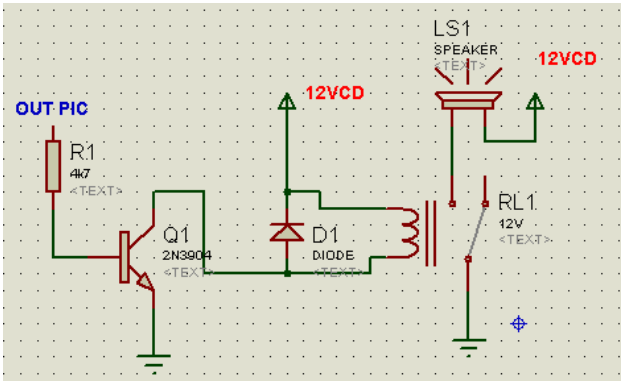


Figura IV.60. Circuito de conexión de la sirena

En este circuito el transistor está trabajando en la zona de saturación, esta zona como se sabe sirve para aplicaciones de conmutación, y se puede considerar las corrientes que lo atraviesan casi nulas, así como se estima un corto circuito entre colector y emisor es decir VCE ≈ 0V. En este circuito tenemos dos estados los cuales serán analizados:

- Estado 1 cuando la salida del microcontrolador es de 0VCD, el relé no se activa
  - IB = 0v
  - Ic = 0V (TRANSISTOR NO CONDUCE)

Esto sería lo ideal lo exacto es:

IB = 0

En la segunda malla

– 12 VCD +VCE = 0

VCE = 12 VCD

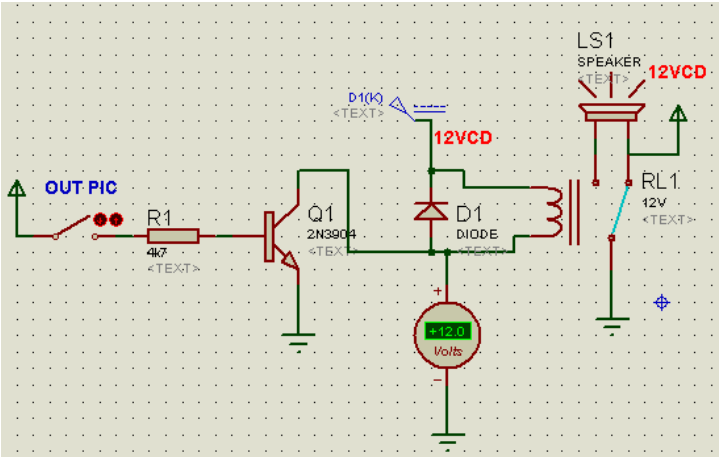


Figura IV.61. Circuito de conmutación cuando la Vi = 0 VCD

Por lo que el relé no se activa

- Estado 2, cuando la salida del microcontrolador es 1 lógico o 5 VCD, aquí el VC ≈ 0VCD por lo que el diodo empieza a funcionar y relé se activa.

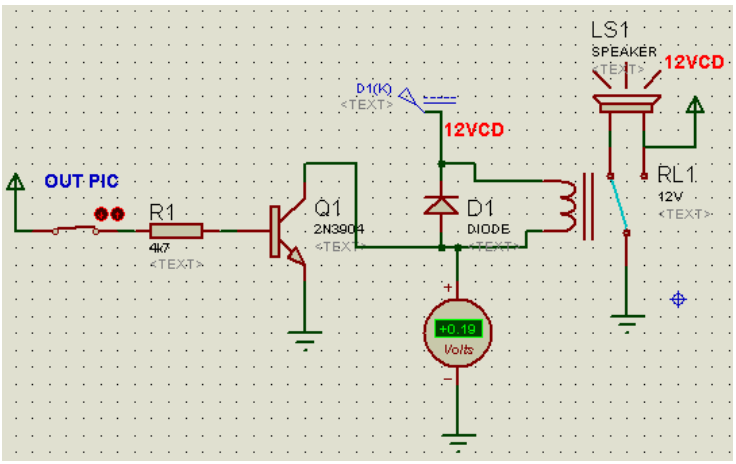


Figura IV.62. Circuito de conmutación cuando la Vi = 5 VCD

- **Circuito de llamada Telefónica**

Otro tipo de respuesta del sistema, es la advertencia del allanamiento mediante la llamada de emergencia a una central que estará monitoreando la alarma.

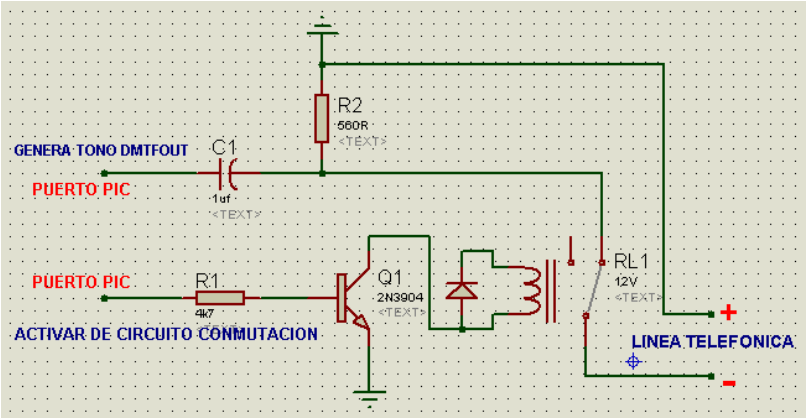


Figura IV.63. Circuito para generar llamada telefónica

Para este procedimiento se ha utilizado un puerto del PIC, el cual va activar un circuito de conmutación como el que se explico anteriormente, donde el transistor va a trabajar como un interruptor, este se encuentra en la zona de saturación, el cual activara el relé y cerrara el circuito del teléfono.

El otro puerto del PIC se utilizara para enviar los tonos DMTF pertenecientes a la combinación de frecuencias de cada número, se ha colocado una resistencia de 470Ω de 1 watio, paralela a la red telefónica, sirve para simular la carga del teléfono, con esto se tendrá el tono de marcado. El capacitor electrolítico de 1µf a 100V, sirve para mejorar la onda que sale del PIC, y para protección del mismo. Se debe considerar que el lado positivo de la red telefónica debe ir a tierra del circuito.

Una vez activado el relé esperamos dos segundos, luego se procederá a la marcación y enviar los tonos DMTF correspondientes a los números de la central de control, se espera 5 segundos y luego se envía el tono de emergencia.

- **Circuito de Conexión del LCD 20x4**

El modulo LCD (Display de Cristal Liquido), es utilizado para mostrar mensajes en el estado que se encuentra el sistema, el LCD utilizado es el de 20x4 con Backligh el cual tiene 16 pines.

Tabla IV.III. Función de cada Pin del LCD

Pin	Simb	Descripción
1	VSS	Tierra de Alimentación GND
2	VDD	Alimentación de +5VCD
3	Vo	Ajuste del contraste del cristal Liquido (0 a +5V)
4	RS	Selección de registro control/datos RS=0 reg control RS=1 reg datos
5	R/W	Lectura/Escritura en LCD RW=0 escritura (W) RW=1 lectura (R)
6	E	Habilitación E=0 modulo desconectado E=1 modulo conectado
7	D0	Bit menos significativo (Bus de datos bidireccional)
8	D1	
9	D2	
10	D3	
11	D4	
12	D5	
13	D6	
14	D7	Bit más significativo (Bus de datos bidireccional)
15	A	Alimentación de Backligh +3,5 0 +5VCD
16	K	Tierra GND del Backligh

Los LCD se puede conectar con el PIC con un bus de 4 o 8 bits, la diferencia está en el tiempo en que se demora, pues la comunicación a 4 bits, primero envía los 4 bits más altos y luego los 4 bits más bajo, mientras que los de 8 bits envían todo al mismo tiempo, esto no es un inconveniente ya que el μC trabaja en microsegundos. Pero la gran ventaja de realizar la conexión a 4 bits, es la disminución de cables que se deben conectar, solo se debe conectar el registro Enable y los 4 bits más altos del LCD, con esto se puede enviar mensajes sin inconvenientes. El circuito de conexión selo puede observar en la figura IV.64

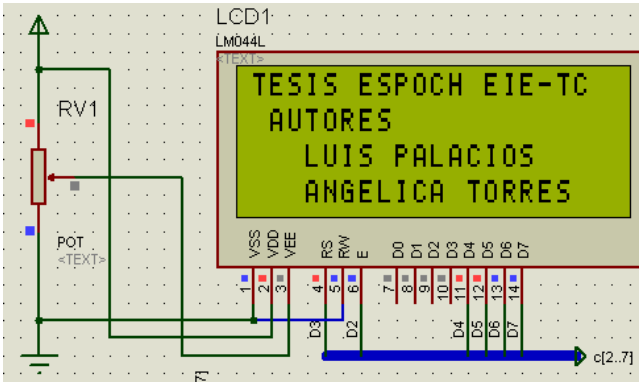


Figura IV.64. Conexión de LCD 20x4 a 4 bits

Con este dispositivo facilita al usuario la manipulación del sistema ya que presenta mensajes fáciles de interpretar, como por ejemplo *ingrese la clave*presentando la ventaja de una menor resistencia de parte del usuario al manipular el sistema

4.3.4 ASIGNACIÓN DE PUERTOS DEL MICROCONTROLADOR 16F877A

El microcontrolador tiene cuarenta puertos que está dividido en 5 grupos, estos se han asignado de la siguiente manera:

Tabla IV.IV. Asignación del Puerto A del sistema de Seguridad

Puerto A	DESCRIPCION	E/S
PORTA.0	Diodo Led indicador de Encendido	S
PORTA.1	Dido Led Indicador, ingreso de carácter desde Teclado	S
PORTA.2	Activación de chicharra	S
PORTA.3	Activación de la Sirena	S
PORTA.4	No asignado	-
PORTA.5	Activar relé para Iluminación	S

Tabla IV.V. Asignación del Puerto B del sistema de Seguridad

Puerto B	DESCRIPCION	E/S
PORTB.0	Fila A del teclado	S
PORTB.1	Fila B del teclado	S
PORTB.2	Fila C del teclado	S
PORTB.3	Fila D del teclado	S
PORTB.4	Columna 1 del teclado	E
PORTB.5	Columna 2 del teclado	E
PORTB.6	Columna 3 del teclado	E
PORTB.7	Columna 4 del teclado	E

Tabla IV.VI. Asignación del Puerto C del sistema de Seguridad

Puerto C	DESCRIPCION	E/S
PORTC.0	Sensor de zona 1	E
PORTC.1	Sensor de zona 2 (Magnético de apertura)	E
PORTC.2	Sensor de zona 3 (Magnético de apertura)	E
PORTC.3	Sensor de zona 4 (Movimiento)	E
PORTC.4	Led Indicador de zona 1	S
PORTC.5	Led Indicador de zona 2	S
PORTC.6	Led Indicador de zona 3	S
PORTC.7	Led Indicador de zona 4	S

Tabla IV.VII. Asignación del Puerto D del sistema de Seguridad

Puerto D	DESCRIPCION	E/S
PORTD.0	No asignado	
PORTD.1	No asignado	
PORTD.2	Habilitación (E) del LCD 20 x4	E
PORTD.3	Selección de Registros (RS) del LCD 20 x4	E
PORTD.4	Bus de datos Bidireccional	E
PORTD.5	Bus de datos Bidireccional	E

PORTD.6	Bus de datos Bidireccional	E
PORTD.7	Bus de datos Bidireccional (Bit más significativo)	E

Tabla IV.VIII. Asignación del Puerto E del sistema de Seguridad

Puerto E	DESCRIPCION	E/S
PORTE.0	Activación de la relé del teléfono	S
PORTE.1	Generación de tono DMTFOUT	S
PORTE.2	No asignado	

4.3.5 CIRCUITO DE CONEXION DEL SISTEMA DE SEGURIDAD

Una vez establecido los elementos con los circuitos que intervienen en el sistema, así mismo los pines del microcontrolador que se utilizarán, se visualiza el diagrama de conexión del sistema de seguridad con todos sus elementos en la figuraIV.65 la simulación se lo ha realizado en Proteus.

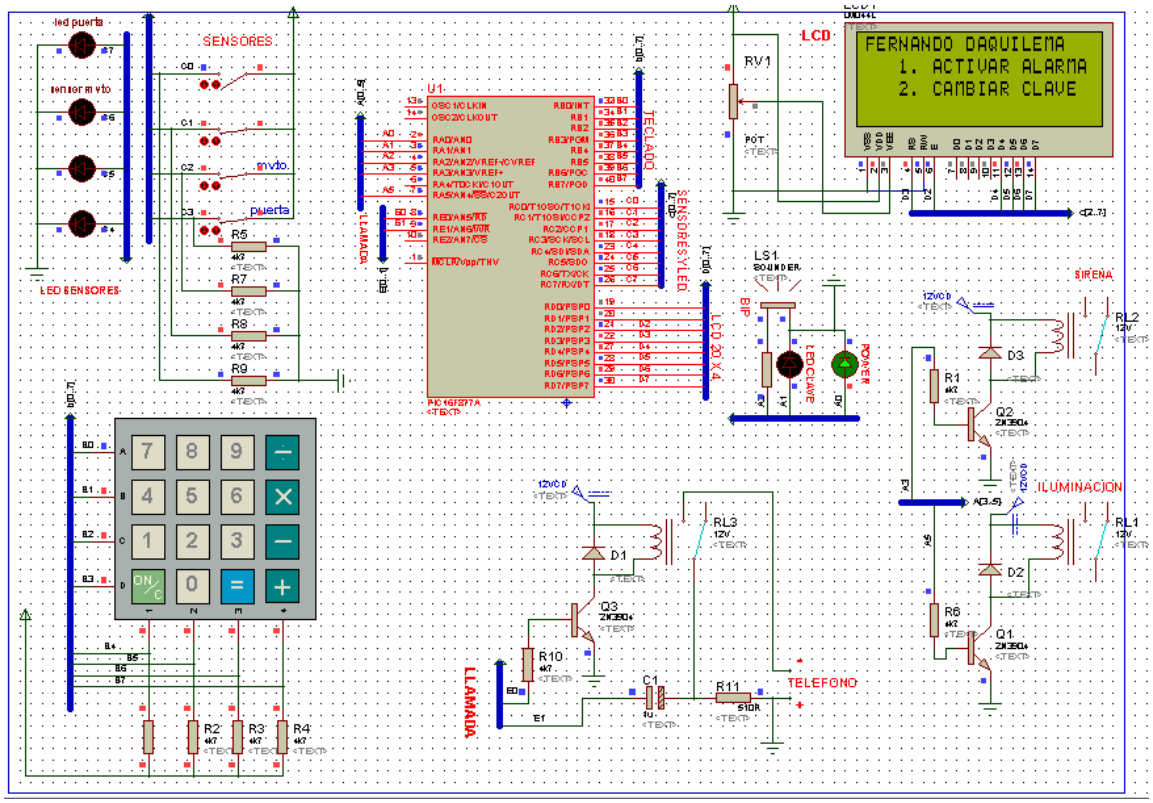


Figura IV.65. Circuito de conexión del Sistema de Seguridad

4.4 ELABORACIÓN DEL SOFTWARE DEL SISTEMA DE SEGURIDAD

El programa que se grabará en el µC en otras palabras en la etapa de procesamiento, en donde se desarrollará un software en base a los circuitos, a las señales recibidas y a la señales de salida para satisfacer los requerimientos anteriormente establecidos.

4.4.1 ETAPA DE PROCESAMIENTO

Una vez detallados que dispositivos y que señales van a ingresar al microcontrolador, así como que salidas vamos activar, pasamos a la etapa de procesamiento, la cual va analizar las señales de entrada y nos accionara los diferentes actuadores.

Para esta etapa se ha utilizado el microcontrolador 16F877A, tiene 40 pines los cuales 33 puertos pueden funcionar como entrada o salida, es fácil de encontrar en el mercado, económicamente es muy accesible, existen software para la programación, por lo que acopla perfectamente a nuestras necesidades.

4.4.2 DIAGRAMAS DE FLUJO

Una vez detallados lo requerimientos y los puertos del microcontrolador que se va utilizar así como qué función desempeña cada puertos, se ha desarrollado el algoritmo el cual nos servirá de base para la programación del microcontrolador en el sistema de seguridad (Ver Anexo 2).

- **Diagrama de flujo de la opción menú**

Se visualizará la pantalla con las opciones de activación de alarma y cambio de clave, las cuales serán seleccionadas mediante el teclado. (Ver anexo 3)

- **Diagrama de flujo ingreso de clave**

El ingreso de clave de cuatro dígitos se lo realizará mediante el teclado, este entrega un valor en la variable **num** que está relacionada con el valor correspondiente a la tecla presionada y lo compara con la variable nuevo1, 2, 3, 4 respectivamente, que son las que están almacenada en la memoria EEPROM del PIC, así también se desarrolla un control anti rebote que sirve para que no tome lectura varias veces la misma variable. (Ver anexo 4)

- **Diagrama de flujo de los sensores y actuadores**

Aquí se realiza un control de los sensores, si uno cambia de estado se activara la sirena y la iluminación, así mismo se activará un temporizador para que pueda ingresar la clave y desactivar la alarma, en el caso que el temporizador a llegado al final del conteo se realizara la llamada de emergencia a una central de monitoreo. (Ver anexo 5)

- **Diagrama de flujo cambio de clave**

Si en la opción menú se eligió el cambio de clave, primero solicitara que se ingrese la clave actual y luego se podrá ingresar la nueva clave, la cual será almacenada en la memoria EEPROM del PIC.
El Ingreso de la nueva clave se lo realizará mediante el teclado, el cual al presionarlo devuelve una variable **num** cada vez que se oprima la tecla, estas variables será almacenada en los registros del cero al tres de la EEPROM del µC, este proceso se repite hasta que se ingrese 4 dígitos, y se guarde en los registros 0, 1, 2, y 3 de la memoria EEPROM del PIC (Ver anexo 6)

4.4.3 PROGRAMA DEL SISTEMA DE SEGURIDAD

Con los algoritmos detallados, los requerimientos y las señales que se debe manejar de los diferentes circuitos, se ha procedido a realizar el programa en un lenguaje de alto nivel, utilizando software Microcode. Aquí se detallara las variables que se utilizaran, los alias de cada puerto del µC, los diferentes procedimientos utilizados, en si está el código del programa.

4.4.4 COMANDOS PRINCIPALES DEL PROGRAMA

En el software microcode, por ser un lenguaje de alto nivel, existen comandos que nos facilitan la programación y tienen una sintaxis que se debe seguir para que funcione correctamente. A continuación se detallará los comandos más importantes, así como la función que cumple dentro del programa del sistema de seguridad

- **Instrucción ADCON**

ADCON1 = 7 se Utiliza para hacer digitales todos los pines del puerto A y del puerto E

- **Instrucción LCDOUT**

LCDOUT Sirve para mostrar ítems en la pantalla de cristal liquido, se utiliza escribiendo LCDOUT, luego $FE, y el comando. En la siguiente tabla se muestra los comandos más utilizados para manejar el modulo LCD.

Tabla IV.VIX. Comandos más utilizados para manejar modulo LCD

Comando	Operación
$FE,1	Limpia el visor LCD
$FE,80	Mueve el cursor al inicio de la primera línea
$FE,C0	Mueve el cursor al inicio de la segunda línea
$FE,94	Mueve el cursor al inicio de la tercera línea
$FE,D4	Mueve el cursor al inicio de la cuarta línea

A continuación se detalla la instrucción desempeñando diferentes funciones dentro del programa:

- LCDOUT, $FE, 1 Limpia le visor LCD
- LCDOUT $FE, $C4, "CLAVE CORRECTA" Visualiza en la 5ta posición de la segunda línea la palabra “CLAVE CORRECTA”

- LCDOUT $FE, $9C,DEC NUM Visualiza en 9 posición de la tercera línea, el valor decimal de la variable NUM

Con estos y otros comandos LCDOUT, nos ayuda a visualizar mensajes que sean de fácil interpretación para el usuario, con la finalidad de ayudar al manejo del sistema de seguridad

- **Instrucciones EEPROM – READ - WRITE**

La Memoria EEPROM o memoria de lectura de programación y borrado eléctrico no es volátil, lo que quiere decir que la información almacenada en esta, no se borra si se corta la alimentación.

EEPROM Permite grabar datos en la memoria que lleva el mismo nombre, los cuales se irán posesionando en cada una de las celdas del microcontrolador, recuerde que el PIC 16F877a tiene 256 espacios de memora, cada celda maneja un byte. La sintaxis se lo indica con el siguiente ejemplo:

- EEPROM 5, [3,"K",9,12] indica colocar en memoria EEPROM, dirección 5 el número 3, dirección 6 la letra K es decir el numero 75, aunque en el programa PicKit2 (Grabador de PIC) lo veremos como 4B, esto porque está en sistema hexadecimal, continuando la dirección 7 se guarda el numero 9 y así sucesivamente

READ Esta instrucción permite leer los datos que se encuentra en la memoria EEPROM, y guardar el contenido de las celdas en una variable previamente definida por el usuario. La sintaxis se lo detalla con el siguiente ejemplo.

- READ 0, A Significa que lea lo que contiene la dirección cero de la memoria EEPROM y guarde en la variable A
- READ 1, B Significa que lea lo que contiene la dirección uno de la memoria EEPROM y guarde en la variable B

WRITE Esta instrucción permite escribir o sobrescribir una dirección o celda de la memoria EEPROM. La sintaxis se lo indica con el siguiente ejemplo

- WRITE 7, A indica que la dirección 7 de la memoria EEPROM se borra y se carga con el valor que tiene la variable A

El manejo de estas instrucciones nos facilita dentro de la programación para realizar el cambio de clave del sistema.

- **Instrucción DMTFOUT**

Esta instrucción genera tono DMTF (Dual – Tono Multifrecuency) como los que producen las teclas del teléfono fijo o celular, este tono es el envió de 2 frecuencias, 1 baja y una alta, que pertenecen a una tecla del teléfono. El grupo de frecuencias se detalla en la siguiente tabla:

Tabla IV.X. Frecuencias DMTF correspondiente a cada tecla

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

DMTFOUT Genera automáticamente los tonos duales correspondientes a cada tecla y los envía cada una a intervalos de 50 milisegundos. La sintaxis se lo detalla con un ejemplo:

- DMTFOUT PORTA.4, [2,6,0,2,5,2,5], indica sacar por el puerto A.4, las frecuencias correspondientes a los números 2, 6, 0, 5

Esta instrucción se utiliza para realizar la llamada de emergencia cuando el sistema ha sido alterado

- **Instrucción GOTO, GOSUB**

Goto Permite apuntar a cierta parte del programa donde se le asignado una etiqueta, continuar con las líneas de programación después de la misma

Gosub Apunta a cierta parte del programa donde esta asignada la etiqueta, guardando su dirección de retorno es decir cumple la subrutina y regresa a la siguiente línea donde se quedo.

4.4.5 PROCEDIMIENTOS RELEVANTES DEL PROGRAMA DEL SISTEMA DE SEGURIDAD

- **OPCION MENU**

Se visualizara el menú en donde está, el nombre de la institución y como opciones a escoger se encuentra, la activación de la alarma, y el cambio de clave, el cual será seleccionado al presionar la tecla 1 o 2 del teclado, la opción escogida se lo almacenara en una variable O

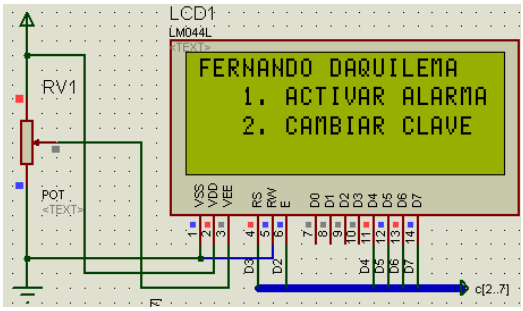


Figura IV.66. Visualización del menú del sistema de seguridad

```
MENU
  LCDOUT $FE,1
        LCDOUT $FE, $80, "FERNANDO
DAQUILEMA"
         LCDOUT $FE, $C3, "1. ACTIVAR
        ALARMA"
         LCDOUT $FE, $97, "2. CAMBIAR
        CLAVE"
         PAUSE 1000
        GOTO OPCIONMENU
GOTO MENU
```

```
OPCIONMENU:
LOW A : HIGH B : HIGH C : HIGH D
   PAUSE 100
    IF UNO = 0 THEN
GOSUB CONTROLTECLA
GOSUB CONTROLSENSOR
      O = 1
      GOTO TECLAUNO
    ENDIF
IF DOS = 0 THEN
GOSUB CONTROLTECLA
      O = 2
GOTO TECLAUNO
    ENDIF
GOTO MENU
```

- **INGRESO DE CLAVE**

Una vez seleccionada la opción 1 o 2 se solicitara el ingreso de la clave, para esto primero se toma lectura de los valores de la memoria EEPROM y se los asigna en las variables NUEVO 1, NUEVO2, NUEVO3, NUEVO4, para proceder a comparar con los números que se ingresan mediante el teclado, el valor del teclado se almacena en la variable NUM. Si uno de los números es ingresado erróneamente, se irá al procedimiento FALSO donde espera que termine de ingresar la clave para dar un mensaje de clave errónea.

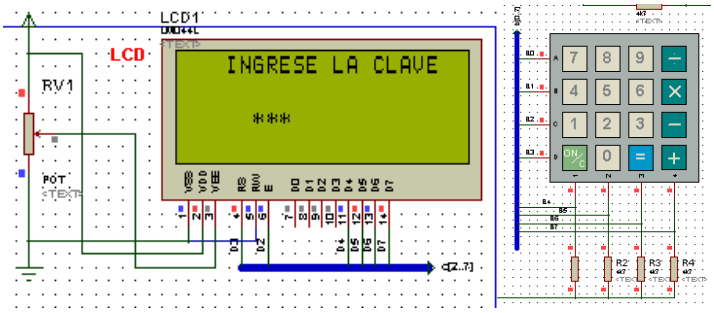


Figura IV.67. Ingreso de Clave

```
EEPROM 0, [1,2,3,4]
RESET:
   READ 0, NUEVO1
   READ 1, NUEVO2
READ 2, NUEVO3
   READ 3, NUEVO4
GOTO INICIO


TECLADOS:
GOSUB TECLADO
```

```
TECLAUNO:
   LCDOUT $FE, $83, "INGRESE LA CLAVE"
GOSUB TECLADO
GOSUB CONTROLTECLA
   IF NUM = NUEVO1 THEN
      LCDOUT $FE, $99, "*"
GOTO TECLADOS                ENDIF
GOTO FALSO


   GOSUB CONTROLTECLA
   IF NUM = NUEVO2 THEN
```

```
LCDOUT $FE, $9A, "*"
      GOTO TECLATRES
   ENDIF
GOTO FALSO1

TECLATRES:
   GOSUB TECLADO
   GOSUB CONTROLTECLA
IF NUM = NUEVO3 THEN
      LCDOUT $FE, $9B,"*"
GOTO TECLACUATRO
   ENDIF
GOTO FALSO2

TECLACUATRO:
GOSUB TECLADO
   GOSUB CONTROLTECLA
   IF NUM = NUEVO4 THEN
         LCDOUT $FE, $9C,"*
         LCDOUT $FE, $C4, "CLAVE
CORRECTA"
         if y = 3 OR Y = 4 then
                  LCDOUT $FE, $C1,
"ALARAMA DESACTIVADA"
                  GOTO INICIO
         ENDIF
          IF O = 1 THEN TEMPORIZADOR
         if O= 2 then GRABAUNO
         goto INICIO
 ENDIF
GOTO FALSO3
```

- **CAMBIO DE CLAVE**

En la opción dos, del menú, se puede seleccionar el cambio de clave, para realizar esta operación lo primero que solicitara es el ingreso de la clave actual, si coincide pedirá ingresar la nueva clave para esto proceso se necesita escribir en memoria EEPROM utilizando para esto el comando **WRITE** que escribe en memoria la nueva clave cuatro dígitos, y el comando **READ** que lee lo que tiene la memoria y asigna a los valores a las variables correspondientes para luego proceder a compararlos.

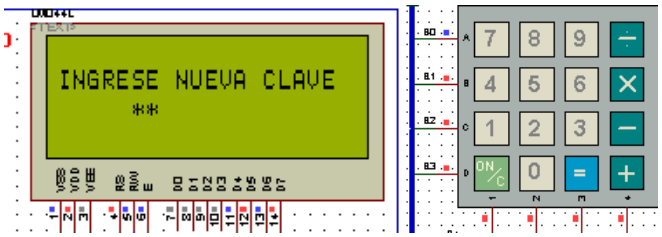


Figura IV.68. Ingreso de Nueva Clave

GRABAUNO:

LCDOUT $FE, $C0, "INGRESE NUEVA CLAVE"
GOSUB TECLADO
GOSUB CONTROLTECLA
LCDOUT $FE, $99, "*"
write 0, NUM

GRABADOS:

GOSUB TECLADO : GOSUB CONTROLTECLA
LCDOUT $FE, $9A, "*"
write 1, NUM

GRABATRES:

GOSUB TECLADO : GOSUB CONTROLTECLA
LCDOUT $FE, $9B, "*"
write 2, NUM

GRABACUATRO:

GOSUB TECLADO : GOSUB CONTROLTECLA
write 3, NUM
LCDOUT $FE, $9C, "*"
LCDOUT $FE, $C5, "CLAVE INGRESADA"
GOTO RESET

RESET:

READ 0, NUEVO1
READ 1, NUEVO2
READ 2, NUEVO3
READ 3, NUEVO4
GOTO INICIO

- **SENSORES Y ACTUADORES**

Una vez ingresada la clave correctamente se irá a un temporizador de salida, es el cual permite que el usuario abandone el área protegida, una vez finalizado el temporizador se va a comparar el estado de los sensores, como estos trabajan en un estado positivo, se compara si ha cambiado de estado, en otras palabras detecta si pasa de 1L a 0L, si sucede esto se pasara a un temporizador de entrada (Temporizador 2) una vez finalizado, pasa a un temporizador 3 que es donde se activa la sirena y la iluminación por un lapso de 1 minuto antes de realizar la llamada de emergencia, si no se ha desactivado la alarma, antes que culmine este temporizador, procede a realizar el llamado a un número telefónico predeterminado

SENSORES:

```
   IF Z1 = 1 THEN
      HIGH LEDZ1
GOTO TEMPORIZADOR2
   ENDIF
```

```
   IF Z2 = 0 THEN
      HIGH LEDZ2
GOTO TEMPORIZADOR2
   ENDIF
```

```
IF Z3 = 0 THEN
      HIGH LEDZ3
GOTO TEMPORIZADOR2
   ENDIF
```

```
 IF Z4 = 0 THEN
  HIGH LEDZ4
GOTO TEMPORIZADOR2
   ENDIF
   Y = 3
GOSUB DESCONECTAR
GOTO SENSOREs
```

TEMPORIZADOR3:

```
      LCDOUT $FE,1
LCDOUT $FE, $83, "SENSOR ACTIVADO"
pause 1500
```

```
   LCDOUT $FE,1
   IF J1 = 2 THEN GOTO LLAMADAPHONE
  FOR I = 1 TO 50 ;
      Y = 5 : K = I
```

```
        P = 50 - I
LCDOUT $FE, $D4, "TIEMPO RESTANTE  ",
DEC P
        PAUSE 1000
        HIGH SIRENA : HIGH ILUMINACION
GOSUB DESCONECTAR
      NEXT
GOTO LLAMADAPHONE

LLAMADAPHONE:
HIGH RELEPHONE
   PAUSE 1000
   LCDOUT $FE,1 : PAUSE 20
LCDOUT $FE, $C0, "LLAMADA D
EMERGENCIA"
PAUSE 1500
   DTMFOUT LLAMADA, [2,6,0,0,5,4,5]
   PAUSE 5000
   FOR T = 1 TO 80
      SOUND LLAMADA,[100,10,50,10]
   NEXT
   LOW RELEPHONE : PAUSE 200
LL = 1
GOSUB DESCONECTAR
```

DISEÑO DE HARDWARE Y SOFTWARE DEL SISTEMA DE CONTROL DE ACCESO

Antes de la analizar los circuitos que intervienen, así como el software que se desarrollo, es de vital importancia detallar los requerimientos del sistema.

4.5 REQUERIMIENTOS DE SISTEMA DE CONTROL DE ACCESO.

Una vez analizado el nivel de seguridad en el sistema de control de acceso que se solicita en el colegio Fernando Daquilema, se establecieron los siguientes requerimientos:

- El sistema dispondrá de un visor (LCD 20x4) que facilite al usuario la interpretación de mensajes del sistema, estos serán:
    - Solicitud de ingreso de clave
    - Información del ingreso de clave, y verificación de huella dactilar satisfactoria o fallida
    - Información si la puerta se abrió

- Cambio de claves del usuario normal, así como del master
- Ingreso de nueva huella dactilar
- Borrado de huella Dactilar

- Para la verificación de una persona, se utilizara un NIP que será ingresado por un teclado matricial 4x4, y para un nivel de seguridad alto se ha incorporado un detector de huella dactilar FIM3040-LV que se acopla perfectamente a las necesidades. Con estos dos métodos se controla el acceso, si los dos son superados exitosamente la persona estar permitida ingresar al rectorado

- Se dispondrá de dos claves, una de usuario y una de máster. Con la de usuario y la verificación de la huella se permitirá el ingreso al rectorado de la institución, y con la clave master y la verificación de la huella ingresamos a las opciones de control en donde podemos modificar los siguientes parámetros:
  - Cambio de claves de usuario o master
  - Ingreso de huella digital
  - Borrado de una huella digital.

- Para ingresar al rectorado se colocara una cerradura eléctrica de 12vcd, que será controlado desde el sistema.

4.6 DISEÑO DEL HARDWARE DEL SISTEMA DE CONTROL DE ACCESO

Con los requerimientos establecidos y con finalidad de obtener una clara visión de los elementos que estarán presentes en el sistema de control de acceso, se ha desarrollado el diagrama de bloques (ver en la Figura IV.68), que hace referencia al sensor óptico detector de huellas como periférico de entrada y salida, teclado solo de entrada, LCD y la cerradura como periféricos de salida.

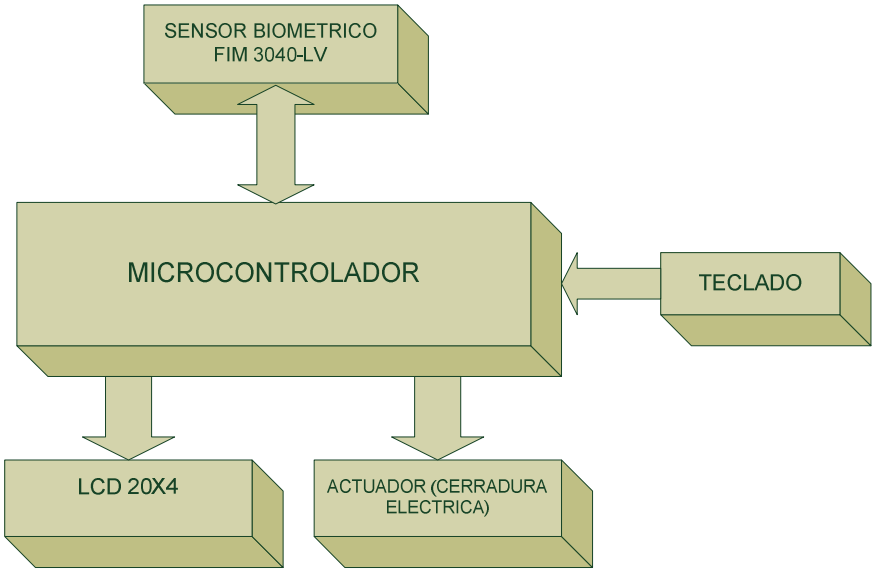


Figura IV.69. Diagrama de Bloques del Sistema de Control de Acceso

Con este diagrama se detallara los diferentes circuitos que intervienen en cada bloque

- **CIRCUITO DEL TECLADO**

El teclado que se utilizara es 4x4, permitirá el ingreso de las claves al usuario el funcionamiento, el circuito de conexión es el mismo que se detallo en el apartado 4.3.2

- **CIRCUITO DEL LCD 20X4**

El LCD 20x4 con Backligh, permitirá visualizar los diferentes mensajes de comunicación con el usuario, el funcionamiento y el circuito de conexión es el mismo que se detalló en el apartado 4.3.3

- **CIRCUITO DE CONEXIÓN DE CERRADURA ELECTRICA**

Para la apertura automática de la puerta controlada, se utilizara una cerradura eléctrica de 12VCD, el circuito de conexión y el funcionamiento del mismo se detalla en el apartado 4.3.3, tomándose en consideración que se remplazara la sirena por la mencionada cerradura.

- **CIRCUITO DE CONEXIÓN DEL SENSOR DACTILAR FIM 3040LV**

El sensor FIM3040-LV es de tipo óptico se utilizará para obtener la huella digital del personal y permitir el acceso solo a los que estén registrados. Se utilizo el JUMPER 3 para realizar las conexiones de control y comunicación, sus pines están distribuidos de la siguiente manera:

Tabla IV.XI. Pines del Jumper 3 del sensor FIM3040-LV

PIN	Nombre	Descripción
1	VCC	Alimentación 3.3V
2	EXT_RXD	Sirve para la comunicación serial (RS-232). Recibe las señales desde el host
3	EXT_TXD	Sirve para la comunicación serial (RS-232). transmite las señales al host
4	EXT_PASS	Es una salida externa que sirve para indicar el éxito de autenticación
5	EXT_FAIL	Es una salida externa que sirve para indicar el fallo de la autenticación
6	EXT_ENROLL	Es una salida externa que guarda la huella dactilar sin la ayuda de la comunicación serial
7	EXT_DELETE	Es una salida externa que borra huella dactilar sin la ayuda de la comunicación serial
8	EXT_IDENTIFY	Es una salida externa que identifica la huella dactilar sin la ayuda de la comunicación serial
9	GND	Conexión a tierra

Con los pines del JUMPER 3, se analizan las condiciones de operación de entrada y salida, exclusivamente desde el 4 al 8, que son los que proporcionan la información necesaria para manipular el sensor.

Tabla IV.XII. Condiciones de Operación de E/S de los Pines del Jumper3

PIN	Nombre	Dirección	Estado Inicial	Activación del Estado
4	EXT_PASS	Salida	Apagado	Encendido (500 ms)
5	EXT_FAIL	Salida	Apagado	Encendido (500 ms)
6	EXT_ENROLL	Entrada	Encendido	Apagar (más de 30 ms)
7	EXT_DELETE	Entrada	Encendido	Apagar (más de 30 ms)
8	EXT_IDENTIFY	Entrada	Encendido	Apagar (más de 30 ms)

Con Tabla IV.XIIse determina que cuando la verificación de una huella es exitosa o fallida, encenderá el pin por 500ms, y para ingresar, borrar y verificar una huella se necesitara apagar estos puertos. Tomando en consideración lo mencionado se considerara a los pines 4 y 5 como entradas al µC, y los pines 6, 7 y 8 como salidas del mismo.

Se tomara en cuenta que el sensor FIM3040-LV necesita una alimentación de 3.3VCD, las entradas del jumper3 trabajan con este voltaje, y el microcontrolador funciona con 5VCD. Por lo que el circuito de conexión quedara como se ve en la Figura IV.70.

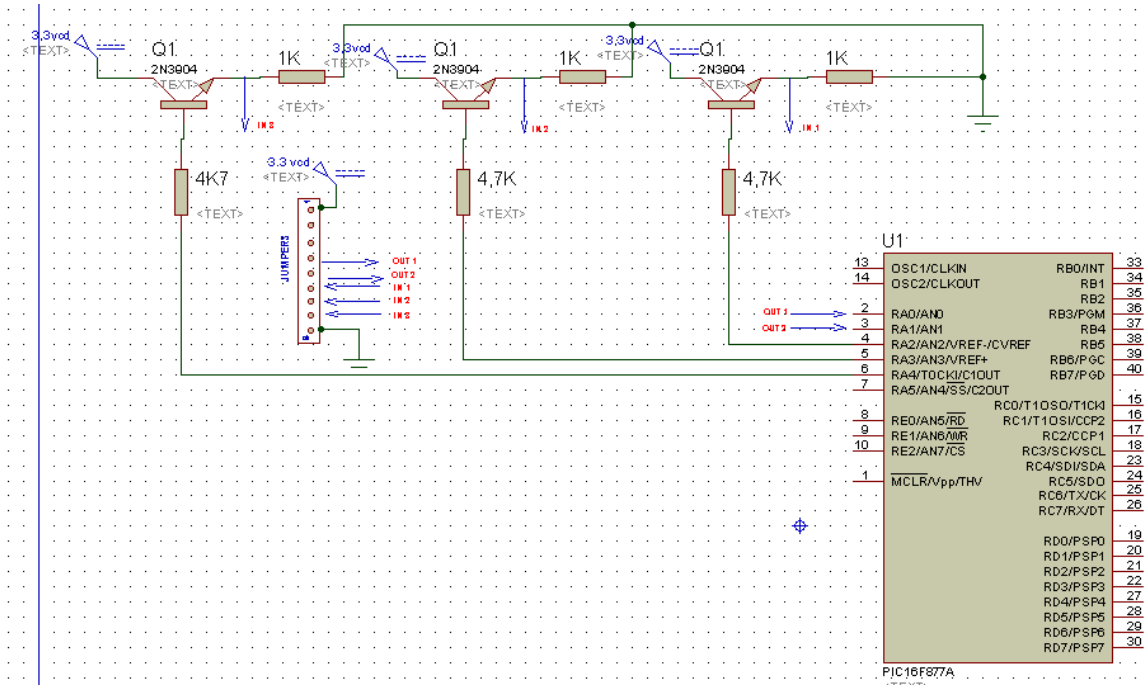


Figura IV.70. Circuito de conexión del Jumper 3 del FIM 3040-LV

ASIGNACION DE PUERTOS DEL MICROCONTROLADOR EN EL SISTEMA DE CONTROL DE ACCESO

El microcontrolador que se utilizara es el 16F877A es el mismo que se utilizara en el sistema anterior tiene cuarenta puertos que está dividido en 5 grupos, estos se han asignado de la siguiente manera:

Tabla IV.XIII. Asignación del Puerto A del sistema de control de acceso

Puerto A	DESCRIPCION	E/S
PORTA.0	PIN 4 DEL JUMPER SENSOR FIM 3040-LV (huella satisfactoria)	E
PORTA.1	PIN 5 DEL JUMPER SENSOR FIM 3040-LV (huella fallida)	E
PORTA.2	PIN 6 DEL JUMPER SENSOR FIM 3040-LV (Ingreso de huella)	S
PORTA.3	PIN 7 DEL JUMPER SENSOR FIM 3040-LV (borrado de huella)	S
PORTA.4	No asignado	-
PORTA.5	Sensor de la Puerta	E

Tabla IV.XIV. Asignación del Puerto B del sistema de control de acceso

Puerto B	DESCRIPCION	E/S
PORTB.0	Fila A del teclado	S
PORTB.1	Fila B del teclado	S
PORTB.2	Fila C del teclado	S
PORTB.3	Fila D del teclado	S
PORTB.4	Columna 1 del teclado	E
PORTB.5	Columna 2 del teclado	E
PORTB.6	Columna 3 del teclado	E
PORTB.7	Columna 4 del teclado	E

Tabla IV.XV. Asignación del Puerto C del sistema de control de acceso

Puerto C	DESCRIPCION	E/S
PORTC.0	PIN 8 DEL JUMPER SENSOR FIM 3040-LV (verificación de huella)	E
PORTC.1	Cerradura Eléctrica	S
PORTC.2	No asignado	-
PORTC.3	No asignado	-
PORTC.4	No asignado	-
PORTC.5	No asignado	-
PORTC.6	Selección de Registros (RS) del LCD 20 x4	E
PORTC.7	Habilitación (E) del LCD 20 x4	E

Tabla IV.XVI. Asignación del Puerto D del sistema de control de acceso

Puerto D	DESCRIPCION	E/S
PORTD.0	No asignado	-
PORTD.1	No asignado	-
PORTD.2	No asignado	-
PORTD.3	No asignado	-
PORTD.4	Bus de datos Bidireccional	E
PORTD.5	Bus de datos Bidireccional	E
PORTD.6	Bus de datos Bidireccional	E

PORTD.7	Bus de datos Bidireccional (Bit más significativo)	E

Tabla IV.VII. Asignación del Puerto E del sistema de control de acceso

Puerto E	DESCRIPCION	E/S
PORTE.0	Led Power (encendido)	S
PORTE.1	Activación de chicharra	S
PORTE.2	Led de Chicharra	-

CIRCUITO DE CONEXIÓN DEL SISTEMA DE CONTROL DE ACCESO

Una vez establecido los circuitos de conexión de los diferentes elementos así como los puertos del µC que están asignados, el circuito de conexión del sistema se visualiza en la Figura IV.70.; este circuito esta simulado en ISIS 7

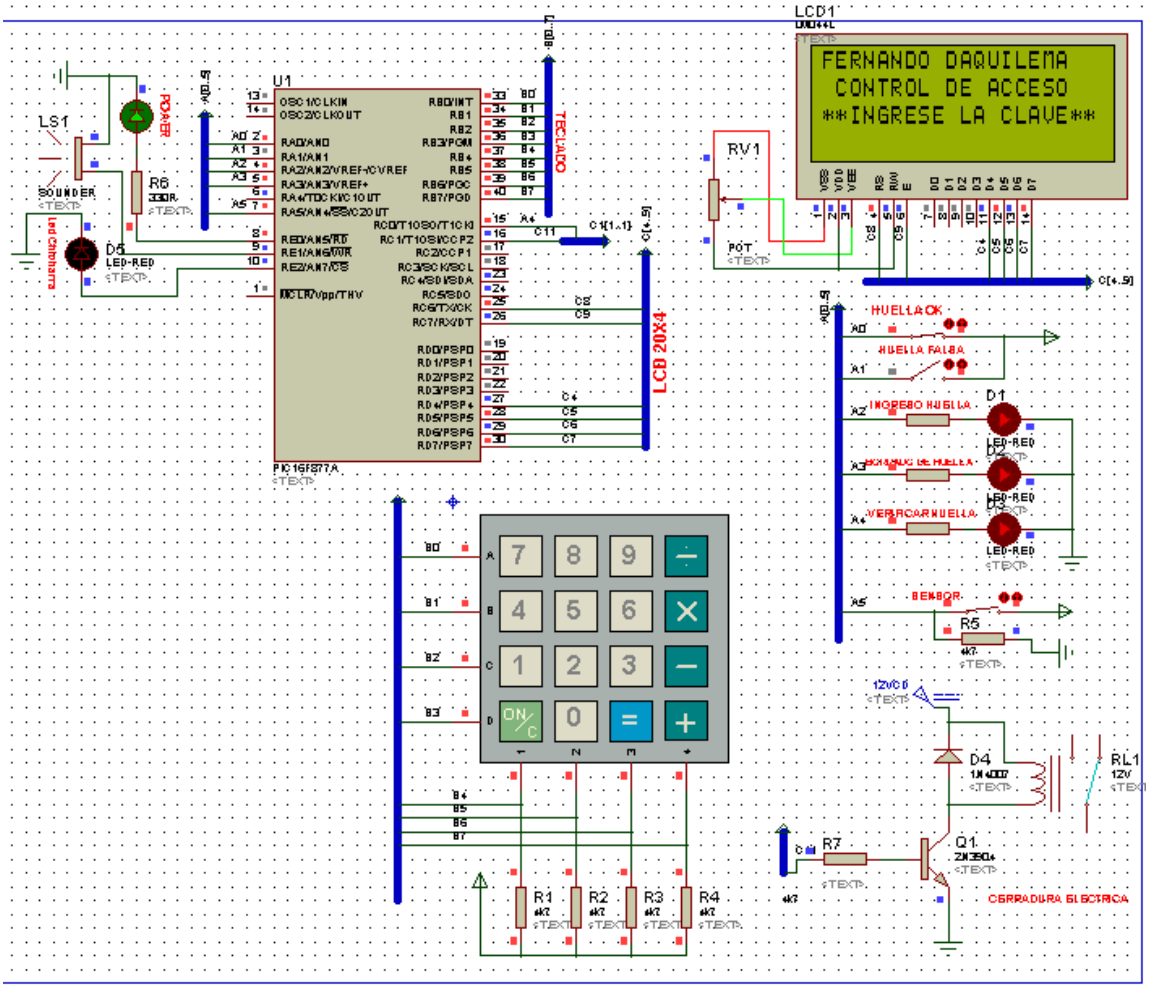


Figura IV.71. Circuito de Conexión del Sistema Control de Acceso

4.7 DISEÑO DEL SOFTWARE CONTROL DE ACCESO

Una vez establecidos los circuitos que serán implementados, así como los requerimientos del control de acceso, se ha procedido primeramente a desarrollara el diagrama de flujo que servirá de base para realizar el programa que será grabado en el microcontrolador.

4.7.1 DIAGRAMAS DE FLUJO

El diagrama de flujo que se utilizo como base para la programación detalla el funcionamiento del sistema de una manera fácil de interpretar, cabe recalcar que aquí no se visualizan las variables del programa. (Ver anexo 7)

- **Diagrama de Flujo Ingreso de Clave y verificación de huella**

Se realiza la obtención de la clave de cuatro dígitos mediante el barrido del teclado, se comparar si la clave es de usuario, máster o errónea, cabe resaltar que el proceso es similar al detallado en el apartado 4.4.2 y su diagrama de flujo esta en el anexo 3. En los dos primeros casos se solicitara que se coloque el dedo en el sensor de huellas para obtener una lectura de la misma. Si la huella coincide se procederá abrir la puerta si es usuario o caso contrario se visualizara las opciones del control de acceso en donde esta: 1. Cambiar clave, Ingresar huella Digital, Borrar huella digital. El diagrama de flujo se desarrollara a partir del ingreso de la clave (Ver anexo 8)

- **Diagrama de Flujo de cambio de clave**

Una vez que se ingresado la clave master y se ha verificado la huella, se desplegará las opciones de control, la primera es el cambio de clave, esta puede ser de usuario o la misma master, la mudanza de clave se lo realiza mediante el teclado, ingresando cuatro dígitos que corresponderán al a nueva clave. Para esto se trabaja con la memoria EEPROM del microcontrolador para almacenar estos cambios, el diagrama de flujo quedara de la siguiente manera (ver anexo 9)

- **Diagrama de flujo de Ingreso de Huella Digital**

En las opciones de control, al seleccionar ingresar huella digital, permitirá agregar una nueva huella, todo el proceso de lectura y verificación se lo realiza en el modulo de FIM3040-LV, lo que tendremos que realizar es interpretar el valor que nos da el lector biométrico. Por lo que cuando el ingreso es correcto se encenderá dos veces el pin 4 del jumper3, esta es la información que debemos interpretar en el programa. (Ver anexo 10)

- **Diagrama de Flujo de Borrado de huella Digital**

La tercera opción del control es el borrado de la huella digital, al igual que el caso anterior todo el proceso lo realiza el lector biométrico, pero la diferencia es que cuando se borra la huella, la información es que el Pin 4 del jumper3 se enciende, caso contrario el pin5 del mismo jamper se enciende. Con esto se realizado el diagrama de flujo (ver anexo 11)

4.7.2 PROGRAMA DEL SISTEMA DE CONTROL DE ACCESO

Con los algoritmos detallados, los requerimientos y las señales que se debe manejar de los diferentes circuitos, se ha procedido a realizar el programa en un lenguaje de alto nivel, utilizando

software Microcode. Aquí se detallara las variables que se utilizaran, los alias de cada puerto del µC, los diferentes procedimientos utilizados, en si esta el código del programa.

Los comandos principales del sistema de control de acceso son los mismos que se detallo en el apartado 4.3.4 a excepción del DMTFOUT.

4.7.3 PROCEDIMIENTOS RELEVANTES DEL PROGRAMA DEL SISTEMA DE CONTROL DE ACCESO

- **INGRESO DE CLAVE Y VERIFICACION DE HUELLA**

Cuando el sistema en esta en funcionamiento nos solicitara el ingreso de la clave de cuatro dígitos, el cual se lo realiza mediante el barrido del teclado, este nos regresa la variable **num** con el valor digitado y se procede a comprara los con los valores ingresados con los de la memoria EEPROM, que están en las variables **NUEVO** Y **MASTER,** se utiliza 2 variables de control **U y M.** Una vez finalizada el ingreso correcto de la clave se procederá a verificar si es clave de usuario (U=4), master (M=4) o errónea, en caso de los dos primeras verificara la huella digital para abrir la puerta o dirigirse a las opciones del usuario

Figura IV.72. Ingreso de Clave y Verificación de Huella

TECLAUNO:

```
  LCDOUT $FE, $83, "INGRESE LA CLAVE"
  IF NUM = NUEVO1 THEN
    U = U+1
LCDOUT $FE, $9B, "*"
GOTO TECLAUNOM
  ENDIF
```

TECLAUNOM:

```
  IF NUM = MASTER1 THEN
    M = M+1
    LCDOUT $FE, $9B, "*"
  ENDIF
```

```
   IF U = 1 OR M = 1 THEN TECLADOS   ;
GOTO FALSO

TECLADOS:
GOSUB TECLADO : GOSUB CONTROLTECLA
IF NUM = NUEVO2 THEN
U = U+1 : LCDOUT $FE, $9C, "*"
GOTO TECLADOSM
   ENDIF

TECLADOSM
   IF NUM = MASTER2 THEN
      M = M+1 : LCDOUT $FE, $9C, "*"
   ENDIF
   IF U = 2 OR M = 2 THEN TECLATRES
GOTO FALSO1

TECLATRES:
GOSUB TECLADO : GOSUB CONTROLTECLA
IF NUM = NUEVO3 THEN
U = U+1 : LCDOUT $FE, $9D,"*"
GOTO TECLATRESM
COMPARARCLAVE:

IF U = 4 THEN
   LCDOUT $FE, $C4, "CLAVE CORRECTA"
   LCDOUT, $FE, $C2, "COLOQUE EL DEDO"
LOW VERIFICAR
   PAUSE 2000
   HIGH VERIFICAR
   FOR I = 0 TO 8000
   ENDIF

TECLATRESM:
   IF NUM = MASTER3 THEN
      M = M+1 : LCDOUT $FE, $9D,"*"
   ENDIF
   IF U = 3 OR M = 3 THEN TECLACUATRO
GOTO FALSO2

TECLACUATRO:
GOSUB TECLADO : GOSUB CONTROLTECLA
   IF NUM = NUEVO4 THEN
      U = U+1 : LCDOUT $FE, $9E,"*"
GOTO TECLACUATROM
   ENDIF

TECLACUATROM:
   IF NUM = MASTER4 THEN
M = M+1 : LCDOUT $FE, $9E,"*"
ENDIF
   IF U = 4 OR M = 4 THEN COMPARARCLAVE
GOTO FALSO3
IF FALLA = 1 THEN
         LCDOUT $FE, $C2, "NO EXISTE
HUELLA"
         GOTO INICIO
ENDIF

      IF CORRECTA = 1 THEN
         LCDOUT $FE, $C1, "HELLA ES
CORRECTA"
```

```
    ENDIF
  NEXT

  IF CORRECTA = 0 OR FALLA = 0 THEN
LCDOUT, $FE,1 : PAUSE 20
```

```
    LCDOUT $FE, $C1, "NO SE LEE HUELLA"
    PAUSE 2000
GOTO INICIO
  ENDIF
```

- **INGRESO DE HUELLA DIGITAL**

La segunda opción de control de acceso es el ingresar la huella digital, esta se almacenara en el FIM3040-LV, para esto se manda un 0L (LOW INGRESAR) al pin 6 del jumper 3 del lector biométrico, con esto se solicita que se coloque el dedo para su lectura, el lector envía dos señales de verificación satisfactoria por el pin 3 que significa que se ingreso correctamente esto lo controlamos con la variable **HC**, caso contrario envía una señal de **FALLA** lo con lo cual la huella no quedara almacenada en la memoria, .

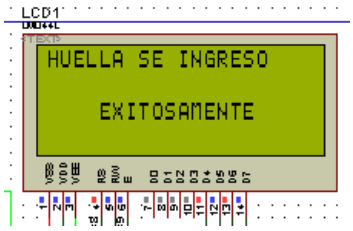


Figura IV.73. Ingreso de Huella digital

```
INGRESAR_HUELLA:
  LCDOUT, $FE, $C2, "COLOQUE EL DEDO"
LOW INGRESAR
  PAUSE 2000
  HIGH INGRESAR
  PAUSE 1000
  FOR I = 0 TO 6000  ;
    IF CORRECTA = 1 THEN
      HC = HC+1
```

```
    IF HC = 1 THEN
      LCDOUT, $FE,1
      LCDOUT, $FE, $C0, "PRIMERA
      LECTURA"

  ENDIF
      IF HC = 2 THEN
        LCDOUT, $FE,1
LCDOUT, $FE, $C2, "HUELLA SE INGRESO"
```

```
        LCDOUT, $FE, $98,
"EXITOSAMENTE"

        PAUSE 3000
GOTO INICIO
ENDIF
    ENDIF

    IF FALLA = 1 THEN
        LCDOUT, $FE,1
LCDOUT, $FE, $C2, "NO SE PUEDE LEER"
        LCDOUT, $FE, $96, "HUELLA
DACTILAR"
        PAUSE 2500
GOTO INICIO
    ENDIF
  NEXT
  LCDOUT, $FE,1
LCDOUT, $FE, $C2, "NO SE PUEDE LEER"
  LCDOUT, $FE, $96, "HUELLA DACTILAR"
  PAUSE 3000
GOTO INICIO
```

- **BORRADO DE HUELLA DIGITAL**

La tercera opción de control de acceso es el ingresar la huella digital, esta se almacenara en el FIM3040-LV, para esto se manda un 0L (LOW BORRAR) al pin 7 del jumper 3 del lector biométrico, con esto se solicitar que se coloque el dedo para su lectura, el lector envía una señal de verificación satisfactoria por el pin 3 que significa que se borro correctamente esto lo controlamos con la variable **CORRECTA**, caso contrario envía una señal de **FALLA** lo con lo cual la huella no se ha borrado de la memoria

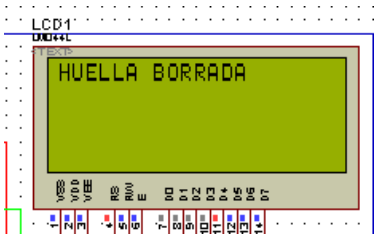


Figura IV.74. Borrado de Huella digital

```
BORRAR_HUELLA:
        LCDOUT, $FE,1 : PAUSE 20
        lcdout, $FE, $C2, "COLOQUE EL DEDO"
```

```
LOW BORRAR
   PAUSE 2000
   HIGH BORRAR
   PAUSE 1000
   FOR I = 0 TO 6000
      IF CORRECTA = 1 THEN
LCDOUT, $FE,1
            LCDOUT, $FE, $C0, "HUELLA
BORRADA"
PAUSE 3000
            GOTO INICIO
         ENDIF



      IF FALLA = 1 THEN
LCDOUT, $FE,1
            LCDOUT, $FE, $C0, "NO SE PUEDE
BORRAR"
            LCDOUT, $FE, $96, "HUELLA
DACTILAR"
            PAUSE 2500
GOTO INICIO
      ENDIF
   NEXT
   LCDOUT, $FE,1
LCDOUT, $FE, $C2, "NO SE PUEDE LEER"
   LCDOUT, $FE, $96, "HUELLA DACTILAR"
   PAUSE 3000
   GOTO INICIO
```

4.8 CIRCUITOS IMPRESOS DE LOS SISTEMAS

Una vez finalizado con la programación y verificado el funcionamiento de los circuitos de cada sistema, utilizando los programas de simulación mencionados anteriormente, se procedió a realizar los circuitos impresos necesarios, para esto se utilizo el software Ares de Proteus, la creación de las pistas se las realizo de forma manual.

En el caso del Sistema de Seguridad se realizaron 3 circuitos impresos, que corresponden a la fuente de alimentación, central de procesamiento y la etapa de respuesta o actuadores. En el Sistema de Control de Acceso se diseño un solo circuito impreso. (Ver anexo 12)

CAPÍTULO V

ANALISIS DE PRUEBAS Y RESULTADOS

Introducción

En este capítulo se presentaran las pruebas realizadas en cada uno de los sistemas desarrollados en el presente proyecto, así como los resultados obtenidos de las mismas.

5.1 DESCRIPCIÓN DE LAS PRUEBAS

Al tratarse de dos sistemas similares en permitir el acceso a personas autorizadas a zonas protegidas, pero diferentes en la manera de realizar la tarea encomendada, se han realizado pruebas de funcionamiento a nivel de software utilizando las mismas herramientas como son:

- La primera prueba se utilizo el software de ISIS 7 con el objetivo de simulara el diseño de los circuitos y comprobar la ejecución correcta del programa desarrollado para el microcontrolador.

Una vez que se ha probado el hardware y software de los sistemas, se procede a las pruebas finales que será

- Segunda prueba está dirigida al sistema de control de acceso, exclusivamente al sensor biométrico FIM3040-LV midiendo el desempeño a través de sus tasas de aceptación, tasa de falsa falso rechazo y falsa aceptación

- Y la tercera prueba esta conducido directamente al sistema de seguridad, en lo relacionado al montaje del sistema en el entorno real y verificación del funcionamiento correctamente.

5.2 PRUEBAS DEL HARDWARE Y SOFTWARE EN EL SIMULADOR PROTEUS ISIS 7

Por ser el software la base de los procesos, esta primera etapa de pruebas es la que demando un detalle meticuloso para su realización.

Para este procesose realizo el montaje de las diferentes interfaces con sus respectivos circuitos que intervienen en cada uno de los sistemas para su posterior simulación, presentándose aquí el inconveniente de que el simulador no posee el sensor biométrico, por lo que se utilizo interruptores para generar las salidas y entrada del sensor, para el sistema de seguridad se

dispone de cuatro interruptores que representa los sensores magnéticos y de movimiento del sistema de seguridad.

Una vez finalizada la etapa de montaje de los elementos se procede a cargar el programa en el microcontrolador.

5.2.1 RESULTADOS DE LA PRUEBA

Con estas pruebas se depuró el programa así como los circuitos que generaban señales erróneas o que el microcontrolador no podía procesarlas.

La principal deficiencia en la simulación radica en los cambios de clave de los sistemas, ya que estas se los almacenan en la memoria EEPROM del µC. Una vez que se ha procedido a renovar la clave se guarda esta variación mientras no se pare la simulación, si la misma es parada y se vuelve a correr, la clave que se cambió no se guarda.

Con esta insuficiencia no se puede determinar si al montarlo físicamente va a cumplir con este requerimiento.

5.3 PRUEBA DE EVALUACION DEL SISTEMA DE CONTROL DE ACCESO

Para esto se procedió a medir el nivel de confiabilidad del sensor, para lo que se utilizaron varios procedimientos de medida, los indicadores de rendimiento de mayor importancia, son los descritos a continuación.

- **CALCULO DE LA TASA DE ACEPTACION (TA)**

Para esto se tomo de cada individuo registrado en el sistema, diez huellas para verificar el porcentaje de de aceptación, se realizo 10 pruebas por cada usuario, comparándolas con las huellas almacenadas en la base de datos.

- **CALCULO DE LA TASA DE FALSO RECHAZO (FRR)**

FRR la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.Para esta se realizo 10 pruebas para cada usuario comparadas con las huellas almacenadas en la base de datos del sensor.

- **CALCULO DE LA TASA DE FALSA ACEPTACION (FAR)**

La frecuencia relativa con que un impostor es aceptado como un individuo autorizado, este índice es casi nulo.

5.3.1 RESULTADOS DE EVALUACION DEL SENSOR BIOMETRICO

- **CALCULO DE LA TASA DE ACEPTACION (TA)**

Con los resultados se puede observar que existe un alto porcentaje de que un usuario sea reconocido por el sistema.

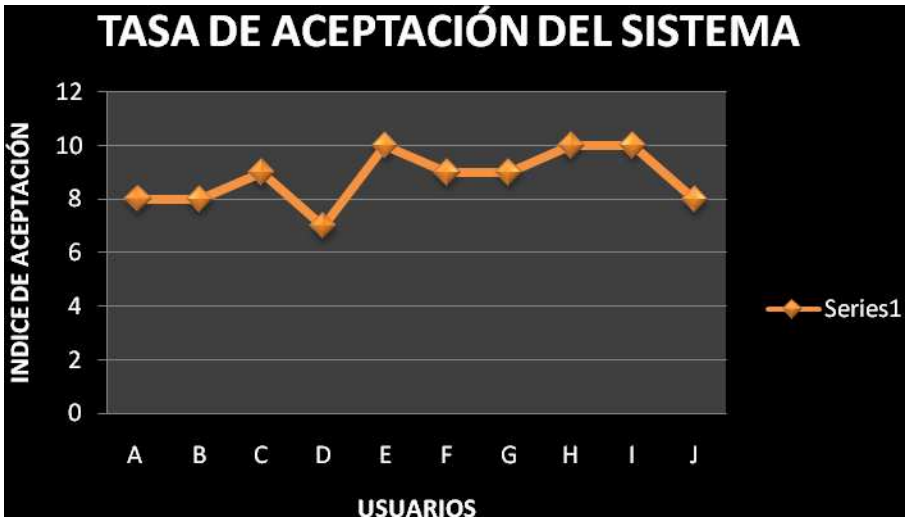


Figura IV.75. Tasa de Aceptación del Sistema

- **LA TASA DE FALSO RECHAZO (FRR)**

El resultado obtenido ha esta prueba se lo puede demostrar en la figura V.76, que existe un bajo porcentaje de que un usuario sea registrado sea rechazado

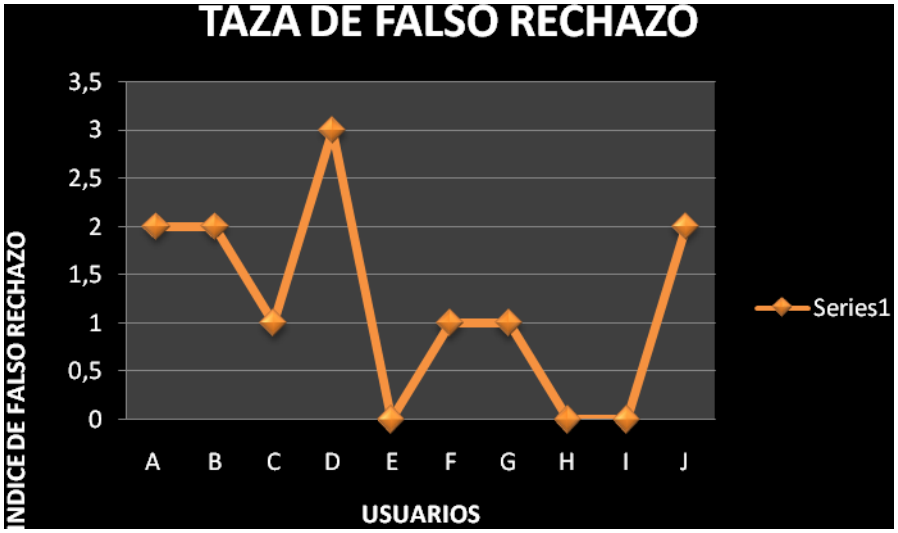


Figura IV.76. Tasa de Falso Rechazo

- **CALCULO DE TOTALES**

  En el gráfico de la figura V.77, se observa de una manera más clara como se comporta el sistema en base a las consideraciones anotadas anteriormente

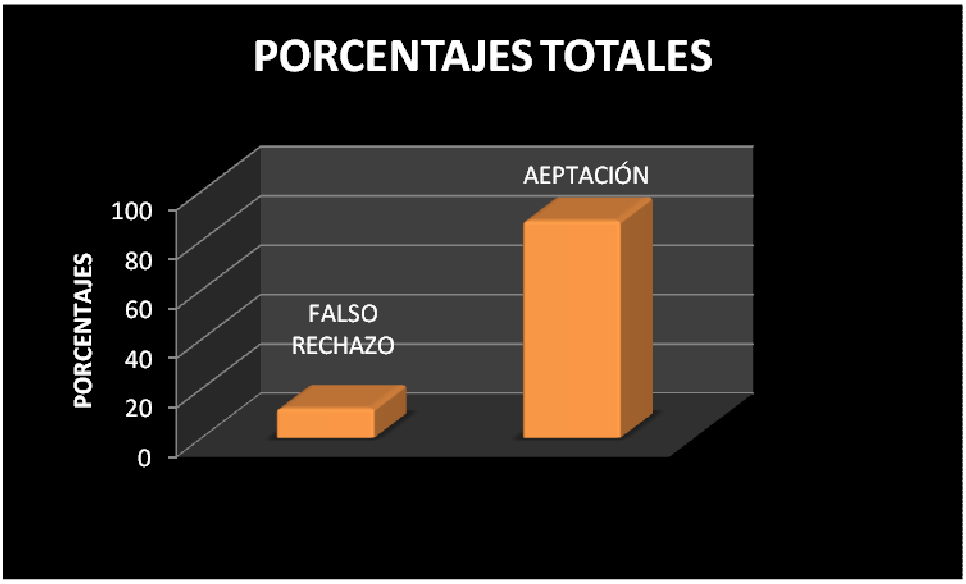


Figura IV.77. Porcentajes Totales

5.4 PRUEBAS EN EL SISTEMA DE SEGURIDAD

Luego de comprobar el funcionamiento del hardware se graba el programa al sistema para realizar las pruebas en el entorno real.

Lo primero que se realizo es situar el sistema en el área a proteger, se ubico la central de procesamiento en un lugar oculto y de difícil acceso, la central de mando donde se encuentran el LCD, el teclado y los indicadores (diodos LED) se lo situó en un lugar de fácil llegada para los usuarios, el sensor de movimiento se lo ubico en la esquina superior para tener un patrón de radiación mayor, el sensor magnético se los coloco en las puertas, y la sirena se la ubico fuera del área protegida y en un lugar abierto, para que las ondas sonoras se transmitan por el aire sin obstáculos.

Figura V.78 Ubicación del sensor PIR

Figura V.79 Ubicación del sensor Magnético

Una vez ubicados los elementos, se procedió a la interconexión de los mismos para determinar si existe comunicación entre las diferentes etapas.

Figura V.80 conexión de elementos

5.4.1 RESULATADOS DE LAS PRUEBAS EN EL SISTEMA DE SEGURIDAD

Una vez conectado las diferentes etapas, se enciende el sistema, el cual presentaráun menú en el LCD para activar la alarma o cambiar la clave, al seleccionar esta solicitará la clave de ingreso el cual será digitada a través del teclado.

Figura V.81 Visualización del Menú

Figura V.82 Visualización de ingreso de clave

Una vez ingresada correctamente la clave entrara a un temporizador de salida el cual permite al personal autorizado abandonar el área protegida antes que los sensores se activen.

Figura V.83 Temporizador de Salida

Una vez que estos sensores se han activado empiezan a detectar cualquier anomalía, si uno de estos cambia de estado es decir si se detecta movimiento o se abre la puerta se dispara temporizador de entrada de 25 segundos para desactivar la alarma

Figura V.84. Temporizador de Salida

Una vez culminado el tiempo de entrada, se activara la sirena, y se encenderán las luces, esta es una manera disuasoria ante la presencia de ladrones. Y finalmente entra a un temporizador de pánico donde se da un tiempo de 60 segundos para desactivar la alarma caso contrario se realiza la llamada de emergencia a un teléfono designado por las autoridades de la institución.

Figura V.85. Temporizador de Pánico

Una elección de vital importancia es el cambio de calve, que se lo realiza al seleccionar la opción dos del menú, se ingresara la clave anterior y luego procederá solicitar la nueva clave.

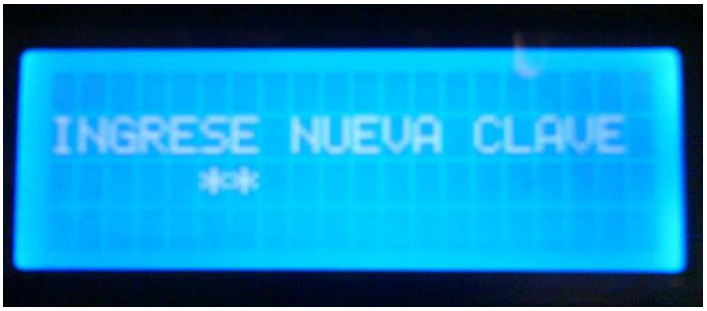


Figura V.86. Ingreso de nueva clave

El sistema da un tiempo de 5 segundos para digitar un número, caso contrario visualiza un mensaje de tiempo excedido y se bloque el teclado

Figura V.87. Tiempo excedido

Mediante las pruebas realizadas a los sistemas y los resultados obtenidos se ha elevado el nivel de seguridad en el área a proteger, este control se lo realiza tanto cuando el personal que labora en el mencionado sitio está presente, mediante el sistema de control de acceso y cuando no lo está mediante el sistema de seguridad.

En consecuencia se ha incrementado el nivel de confianza de las autoridades respecto a la protección, demostrándose así que en la actualidad la seguridad electrónica no es un lujo, es una necesidad.

CONCLUSIONES

1. El diseño y construcción del sistema de seguridad y control de acceso, resulta factible y viable en ejecución, la particularidad de hacerlo con microcontroladores genera la facilidad de programar rápidamente requisitos particulares propios de la institución.

2. El microcontrolador utilizado en los sistemas, fue seleccionado por tener una capacidad elevada de memoria, debido a que la programación del mismo se lo realizo en un lenguaje de alto nivel, consumiendo fundamentalmente este recurso.

3. Al utilizar la memoria EEPROM del microcontrolador para la clave de los sistemas, presenta una protección cuando el usuario genera un cambio de las mismas, ya que estas se quedan almacenadas aun si existieran cortes de energía

4. La incorporación del LCD en los sistemas tiene la meta de facilitar el manejo de estos, mediante la visualización de mensajes fáciles de interpretación por parte del usuario.

5. El monitoreo mediante la red telefónica pública, transforma un simple sistema de alarma en un sistema de seguridad.

6. El sensor PIR Conmet realiza una distinción de objetos que generan radiación infrarroja, por lo que no se activara con la presencia de animales.

7. El sensor óptico detector de huellas dactilares FIM3040-LV, al tener una tarjeta procesadora donde se almacena las huellas digitales, facilita la interpretación de las mismas, mediante señales lógicas enviadas y recibidas por la interfaz de conexión externa JP3.

8. El diseño tanto del software y el hardware resultó ser uno de los pilares fundamentales en el desarrollo del presente proyecto, con la meta de simplificar el circuito a su mínima

expresión, y realizar la programación en un lenguaje de alto nivel facilitando la interpretación del programa

RECOMENDACIONES

1. Consultar la disponibilidad en el mercado local de los materiales a ser utilizados para alcanzar el objetivo propuesto.

2. Realizar pruebas de funcionamiento de los sensores independientemente, para evitar errores en las señales que envían.

3. Ubicar el sensor PIR Conmet en lugar estratégico, libre de obstáculos para generar un mayor alcance en la detección de radiación infrarroja

4. La fuente alimentación en el sistema de seguridad, consta de una batería de gel adicional, para evitar que el sistema deje de funcionar en cuando exista corte de energía en la red eléctrica publica

5. La etapa de procesamiento (Central) del sistema de seguridad, se debe colocar en un lugar oculto, seguro y de difícil alcance para evitar manipulación de personal no autorizado.

6. El ingreso y borrado de huellas digitales en el sistema de control de acceso, está dirigido por una sola persona responsable de la seguridad del área a proteger, el cual tendrá una clave master para ingresar a la opciones de control

7. Al ubicar la huella dactilar en el lector biométrico, este debe estar libre de humedad o de suciedades para obtener una lectura adecuada y evitar posibles fallos como negar el acceso a personal autorizado

RESUMEN

Se Diseño sistemas de seguridad y control de acceso mediante microcontroladores para el colegio Fernando Daquilema de la ciudad de Riobamba, para elevar el nivel de seguridad en las áreas criticas de la institución, inspeccionando el ingreso a las zonas cuando el personal esté o no laborando.

Se utilizo varias herramientas como Pickit2 de Microchip, en lo relacionado al software se empleo. ISIS para la simulación del diseño y Ares en lo relacionado a elaboración de circuitos impresos ambos de Labcenter Electronics. En los sistemas de seguridad y control de acceso se utilizaron en gran parte los mismos elementos como son: PIC 16F877A para el procesamiento de información, LCD 20x4 para visualización de mensajes, teclado matricial de 4x4 para ingreso de claves, la diferencia del primero esta en los sensores magnéticos, sensor de movimiento PIR COMET, sirena de 30 Watios y en el segundo esta el sensor biométrico FIM3040-LV utilizado para extracción de huella dactilar. La activación de estos se lo realizara por medio de claves de cuatro dígitos, y al ser allanada una zona sin autorización, se encenderán los diferentes actuadores que darán aviso de esta anomalía.

Se obtuvo como resultado una protección de las áreas protegidas, elevando el nivel de seguridad tanto interno como perimetralmente, cumpliendo una función disuasoria ante cualquier allanamiento de personal no autorizado.

Se concluye que dichos sistemas tienen un monitoreo constante de una zona determinada, brindando confiabilidad a los usuarios y disminuyendo la resistencia de uso.

Se recomienda la utilización de los sistemas de seguridad y control de acceso, en áreas donde se encuentra equipo tecnológico, documentación importante o vienes que al ser hurtados, generen una gran pérdida económica o insustituible.

SUMMARY

Design security systems and access control through microcontrollers for the college Fernando Daquilema in the city of Riobamba, to raise the level of security in the critical areas of the institution, by inspecting the admission to the areas where staff are or not working.

We used several tools such as Pickit2 Microchip, as it relates to the software used. SUMMARY Design security systems and access control through microcontrollers for the college Fernando Daquilema in the city of Riobamba, to raise the level of security in the critical areas of the institution, by inspecting the admission to the areas where staff are or not working. We used several tools such as Pickit2 Microchip, as it relates to the software used. In the security systems and access control used in much the same elements: PIC 16F877A for information processing, LCD 20x4 for viewing messages, matrix keyboard of 4x4 to key presses, the difference in the first one is in the magnetic sensors, PIR motion sensor COMETA, sirena 30 Watts and the second is the biometric sensor FIM 3040-LV complete manual control used for extraction of fingerprint. Activation of these are done through the four-digit codes, and being raided an area without authorization, will illuminate the various actuators that give notice of this anomaly. The result was protection of protected areas, raising the level of internal and perimeter security, provided a deterrent to any unauthorized raid.

We conclude that these systems have a constant monitoring of a given area, offering users reliability and decreasing the wear resistance.

We recommend the use of security systems and access control in areas where technological equipment, important documents and come to being stolen, generate a large economic loss or irreplaceable.

ANEXOS

ANEXO 1.

DATASHEET NITGEN FIM3040-LV

FIM30xx

NITGEN
Standalone with built-in CPU

1. General Descriptions

FIM30xx is a low-price stand-alone Fingerprint Identification Device with many excellent features. It provides benefits such as high identification performance, low power consumption and RS-232 serial interface with the various commands for easy integration into a wide range of applications. It is a durable and compact device with fingerprint identification module containing NITGEN optics-based fingerprint sensor inside.

2. Target Application

Door-lock system
Safe Box
Simple Access Controller
Vehicle Control
ATM , POS
And more

3. Basic Feature

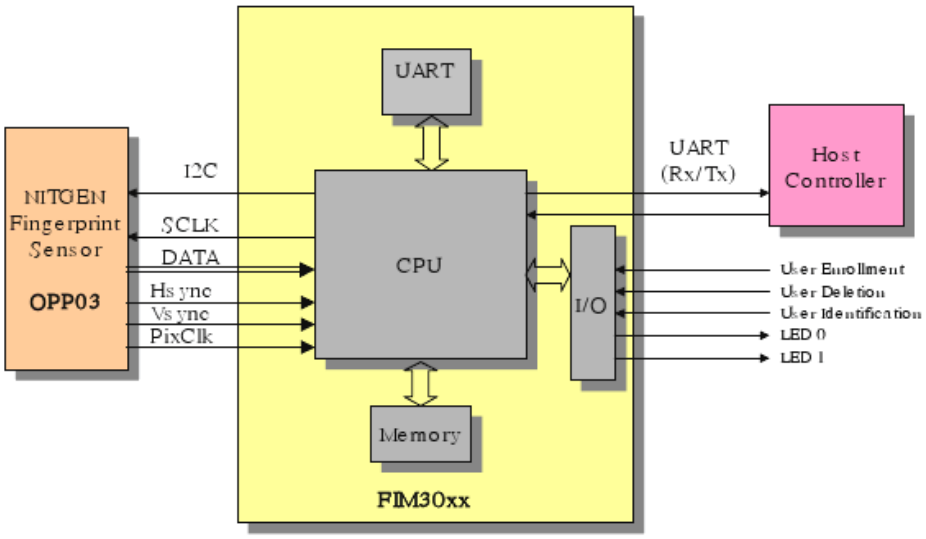
Hardware Specification

ITEM		FIM3030-LV	FIM3040-LV	FIM3030-HV	FIM3040-HV
Board Spec.	CPU	ADSP-BF531			
	DRAM	8Mbyte SDRAM			
	Flash ROM	1Mbytes			
Dimension		43 x 60 [mm^2]			
Sensor		OPP03	OPP04	OPP03	OPP04
Supply Voltage		3.3 ± 0.3 [V]		5.0± 0.5 [V]	
Current Consumption		**(Idle) 55 ~ (Op.) 210 [mA]**	**(Idle) 60 ~ (Op.) 200 [mA]**	**(Idle) 55 ~ (Op.) 210 [mA]**	**(Idle) 60 ~ (Op.) 200 [mA]**
Operating Temperature		-20 ~ 60 [℃]			
Humidity		~ 90 [% RH]			
ESD Tolerance		B/D: ±10 [KV] (indirect) Sensor Finger contact Area: ±20 [KV] (air)			
Communication Channel		RS-232 Speed: 9600 ~ 115200 [bps]			
External I/O		3 Key Input 2 Result Output			

Operation Specification

ITEM	FIM3030-LV/HV FIM3040-LV/HV
Capture Speed	0.2(normal) / 0.7(secure) sec
Verification Speed (Normal Mode)	1.0 [sec] (Capture + Extract + Match)
Boot Up Time	Max. 0.5 [sec]
Data Encryption Method	AES for saving data

4. Block Diagram

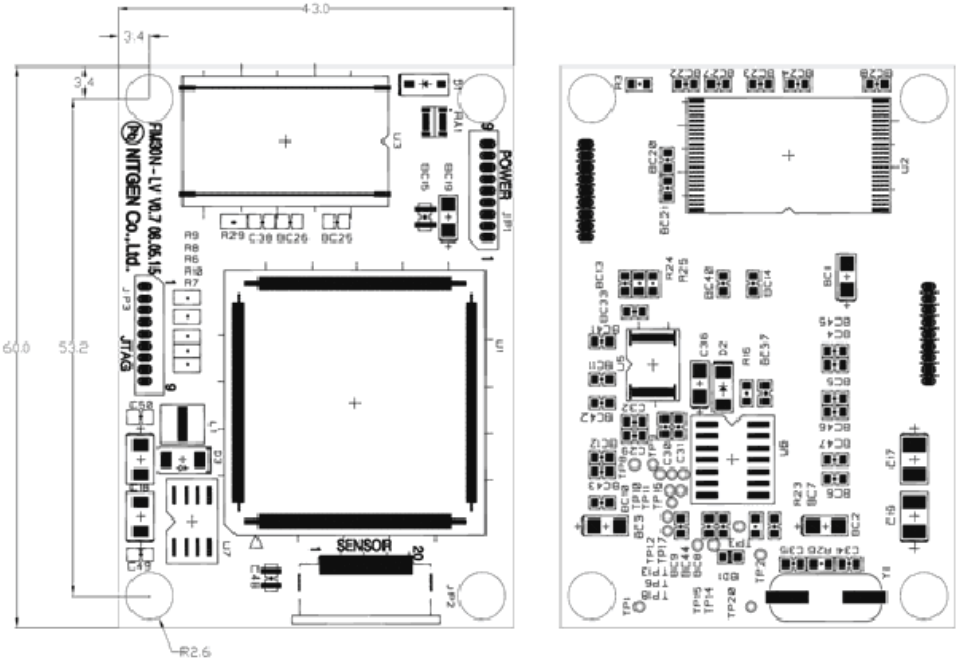


RS-232C communication data consist of 8-bit data, no parity, 1-bit start-bit and 1-bit stop-bit.

6. Technical Data

6.1. Physical Characteristics

The Feature of Board



FIM3030-LV/FIM3040-LV

6.2. External Port

- **External Interface Connection (JP1)**

Pin	Pin Name	Description
1	VCC	3.3 V (FIM30xx-LV) / 5 V (FIM30xx-HV)
2	RXD	RS-232 Rx receiving signal from host
3	TXD	RS-232 Tx transmitting signal to host
4	SUCCESS	Output for indicating authentication success
5	FAIL	Output for indicating authentication fail
6	Enroll_Key	Input to enroll fingerprint without RS-232 communication
7	Delete_Key	Input to delete user without RS-232 communication
8	Identify_Key	Input to identify user without RS-232 communication
9	GND	Ground

I/O Port Operation Condition (included in JP1)

Pin	Name	Direction	Initial State	Active State
4	EXT_PASS	Out	Low	High (500 ms)
5	EXT_FAIL	Out	Low	High (500 ms)
6	EXT_ENROLL	In	High	Low (more 30ms)
7	EXT_DELETE	In	High	Low (more 30ms)
8	EXT_IDENTIFY	In	High	Low (more 30ms)

- **20-Pin Sensor Connection (JP2)**

Pin	Name	States	Description
1	GND	POWER	Sensor Ground
2	VCLK	IN	Sensor Clock
3	VCC	POWER	Sensor VCC (3.3V)
4			Reserved
5			Reserved
6	VSYNC	IN	Vertical Sync.
7	HSYNC	IN	Horizontal Sync.
8	SDATA0	IN	Sensor Data 0
9	SDATA1	IN	Sensor Data 1
10	SDATA2	IN	Sensor Data 2

11	SDATA3	IN	Sensor Data 3
12	SDATA4	IN	Sensor Data 4
13	SDATA5	IN	Sensor Data 5
14	SDATA6	IN	Sensor Data 6
15	SDATA7	IN	Sensor Data 7
16	SDA	IN/OUT	I2C Data
17	SCL	OUT	I2C Clock
18	SLED	OUT	Sensor LED
19	PIXCLK	IN	Pixel Clock
20	GND	POWER	Sensor Ground

- **JTAG (JP3)**

Pin	Pin Name	Description
1	VCC	3.3 Volt Power
2	N/A	N/A
3	nSRST	JTAG control pin
4	TDO	JTAG control pin
5	TDI	JTAG control pin
6	nTRST	JTAG control pin
7	TCK	JTAG control pin
8	TMS	JTAG control pin
9	GND	Ground

* JP1 (JTAG connector) is used only for development or emergency recovery.

6.4. Electrical Characteristics

Parameter	MIN.	TPY.	MAX.	UINTS
Power				
Supply current		210		mA
Supply Voltage (FIM30xx-LV)	3.0	3.3	3.6	V
Supply Voltage (FIM30xx-HV)	4.5	5	5.5	V
RS-232				
Output Voltage Swing	±5.0	±5.4		V
Input Voltage Range	-15		+15	V
Maximum data rate			115,200	BPS

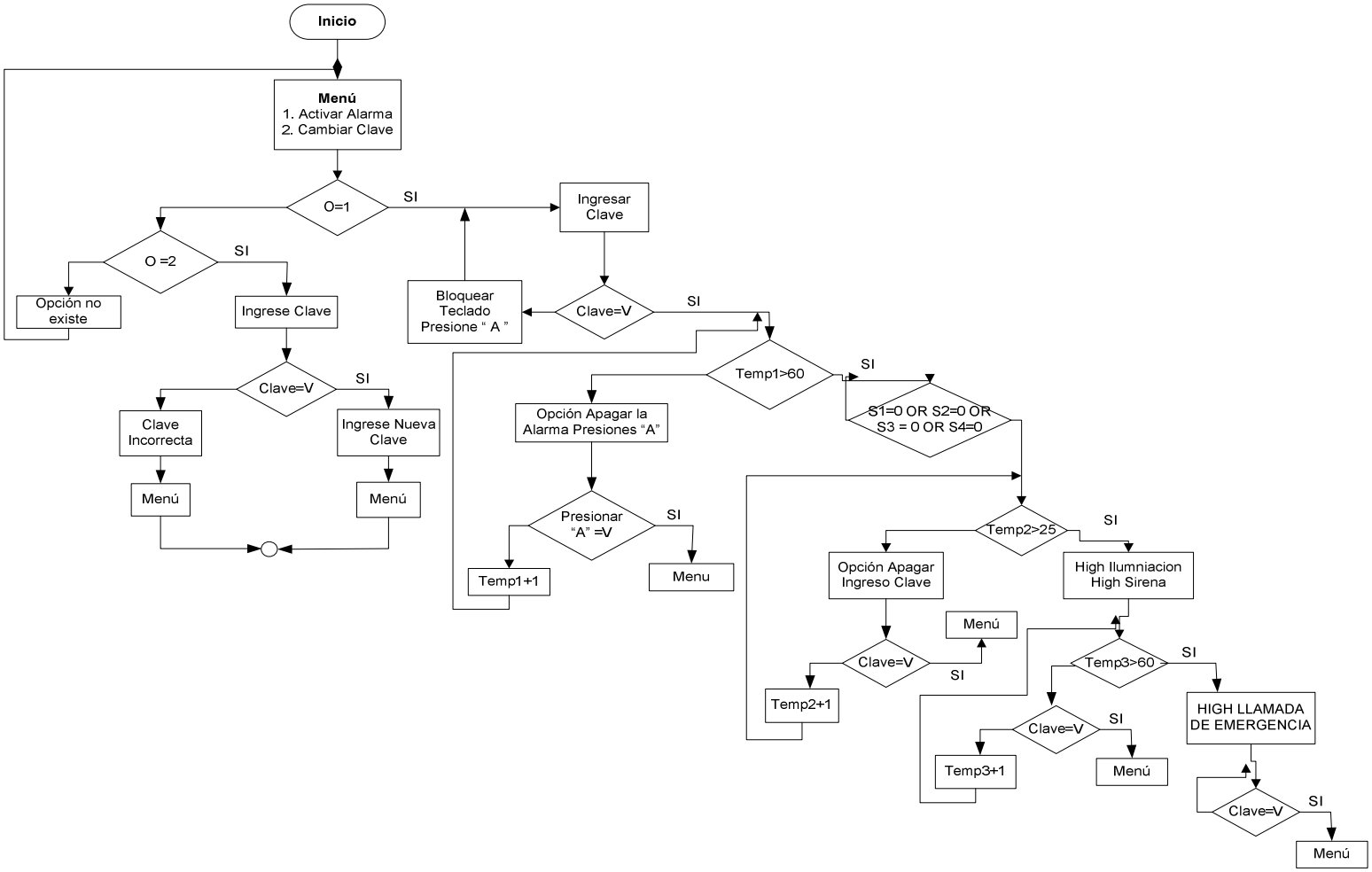
7. Ordering Information

FIM3030 (with OPP03) Ordering Guide

Ordering Number	Supply Voltage	Max. Users
FIM3030-LV	3.3V	100
FIM3030-HV	5V	100
FIM3040-LV	3.3V	100
FIM3040-HV	5V	100

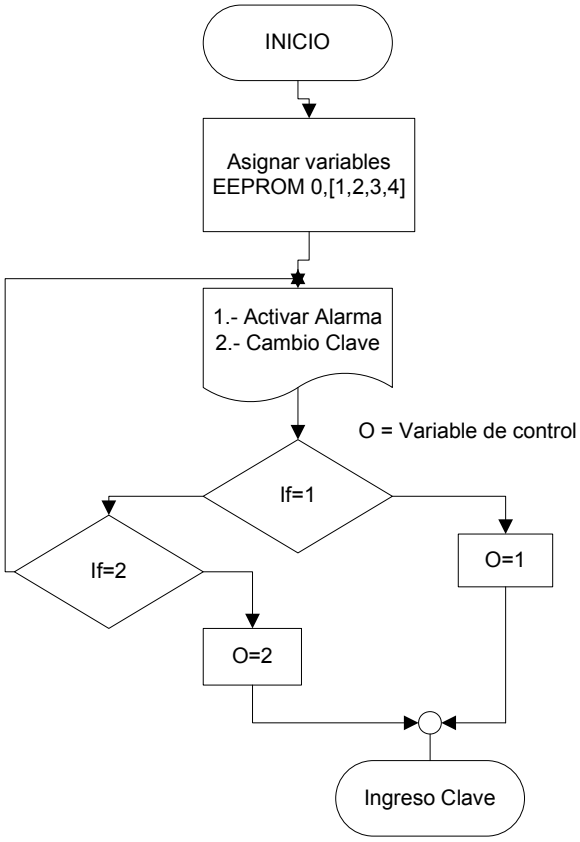
ANEXO 2.

DIAGRAMA DE FLUJO DEL SISTEMA DE SEGURIDAD



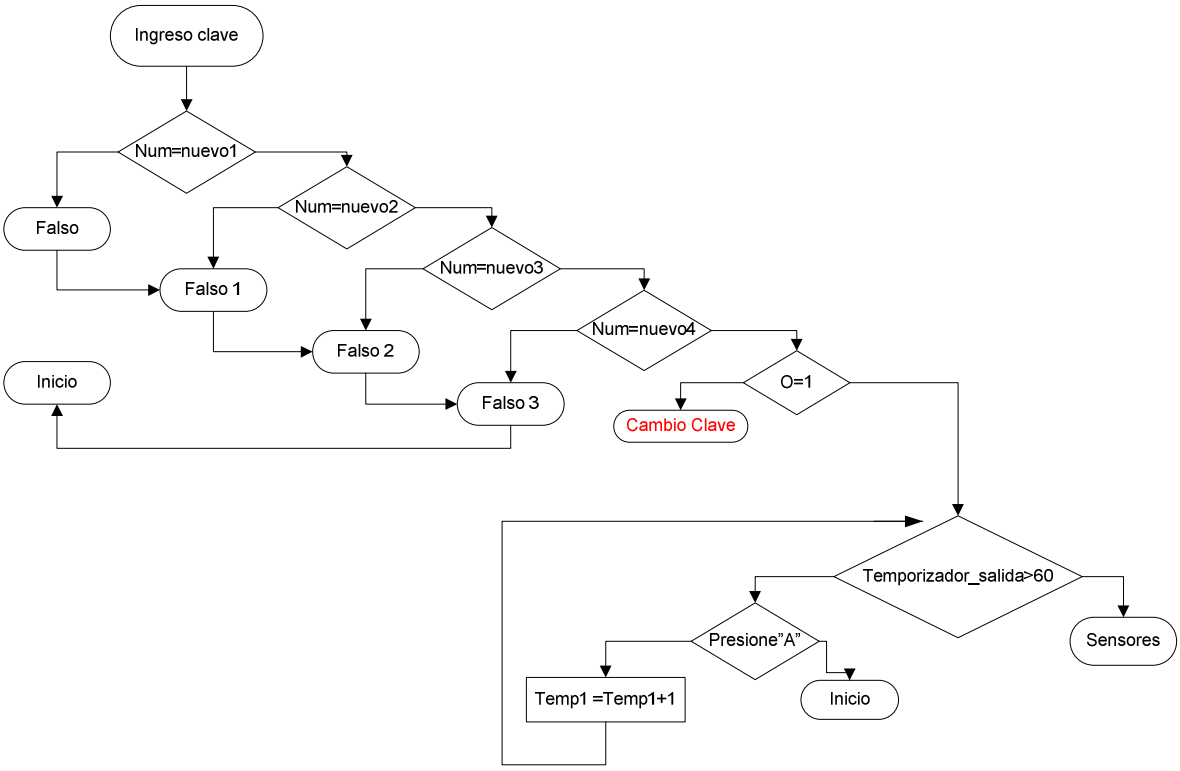
ANEXO 3.

DIAGRAMA DE FLUJO DE OPCION MENU DEL SISTEMA DE SEGURIDAD



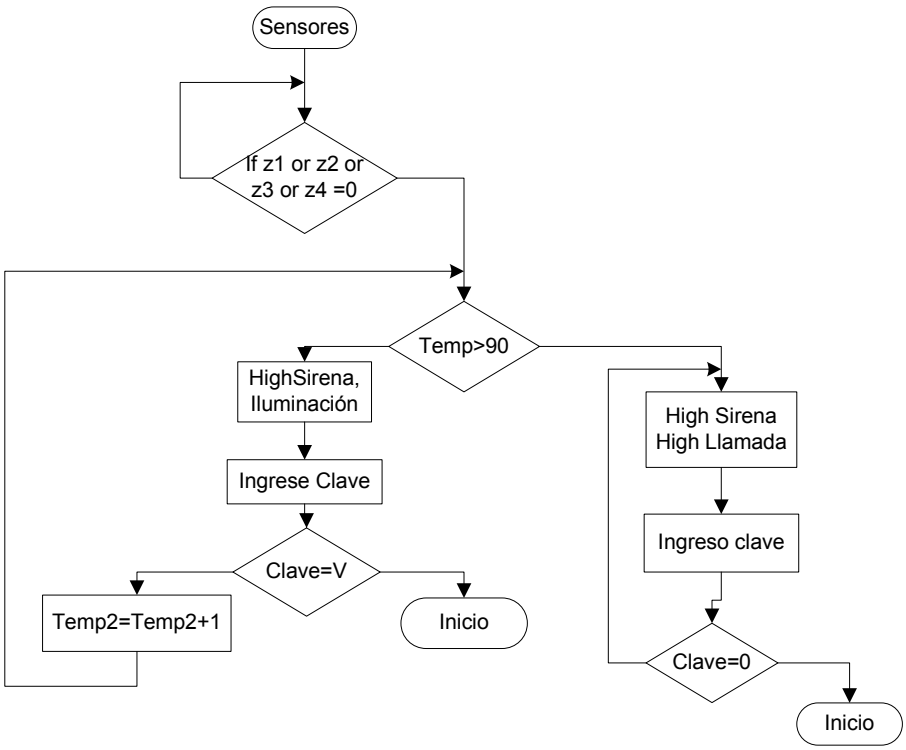
ANEXO 4.

DIAGRAMA DE FLUJO DE INGRESO DE CLAVE DEL SISTEMA DE SEGURIDAD



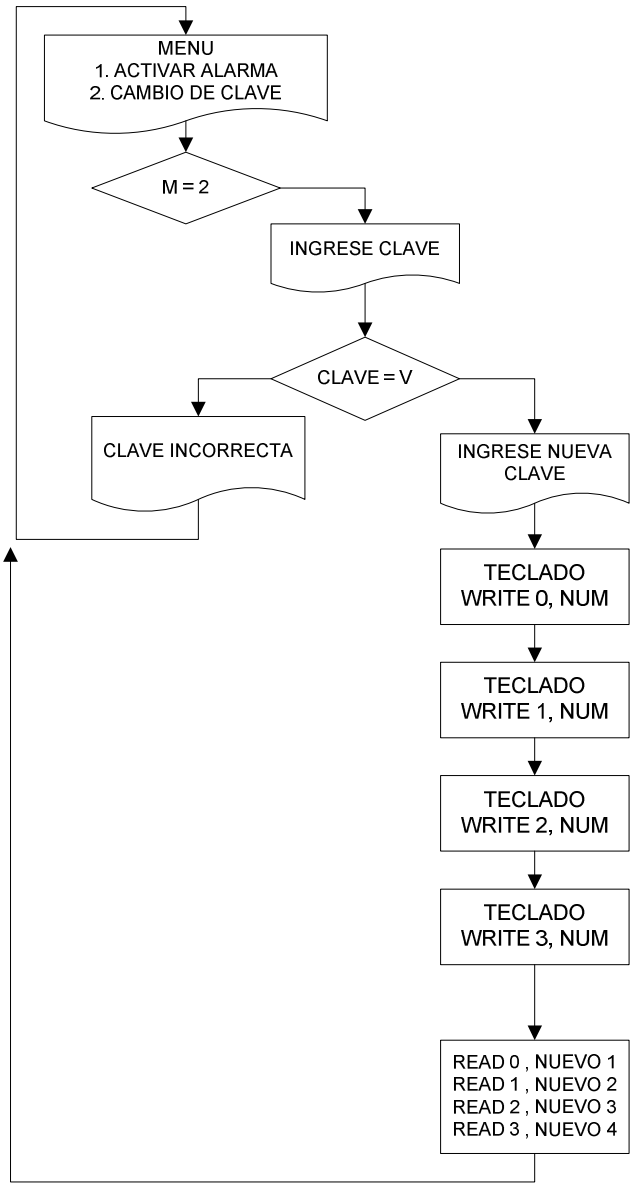
ANEXO 5.

DIAGRAMA DE FLUJO DE SESNSORES Y ACTUADORES DEL SISTEMA DE SEGURIDAD



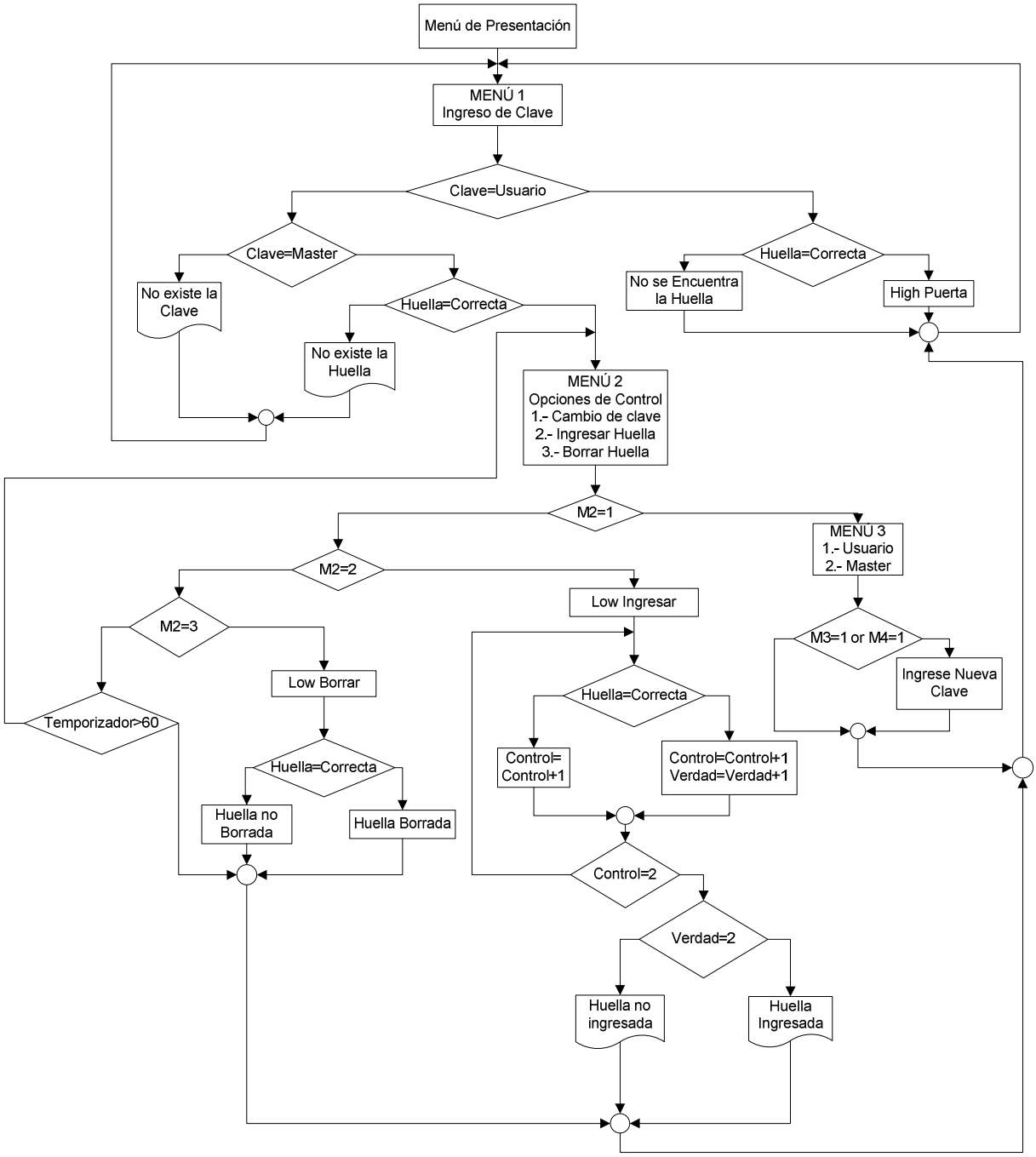
ANEXO 6.

DIAGRAMA DE FLUJO CAMBIO DE CLAVE DEL SISTEMA DE SEGURIDAD



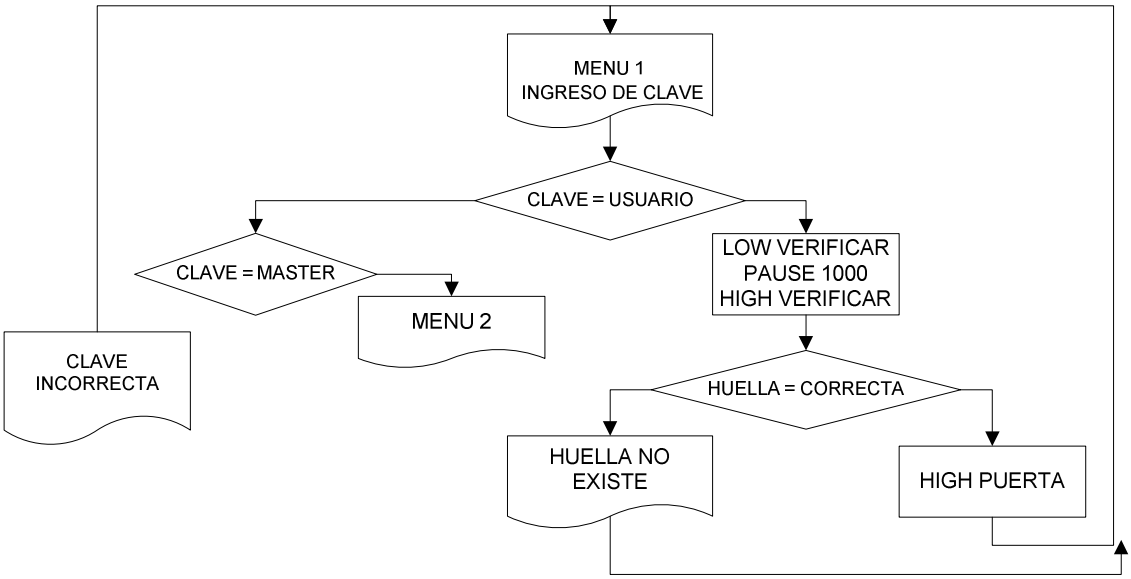
ANEXO 7.

DIAGRAMA DE FLUJO DEL SISTEMA CONTROL DE ACCESO



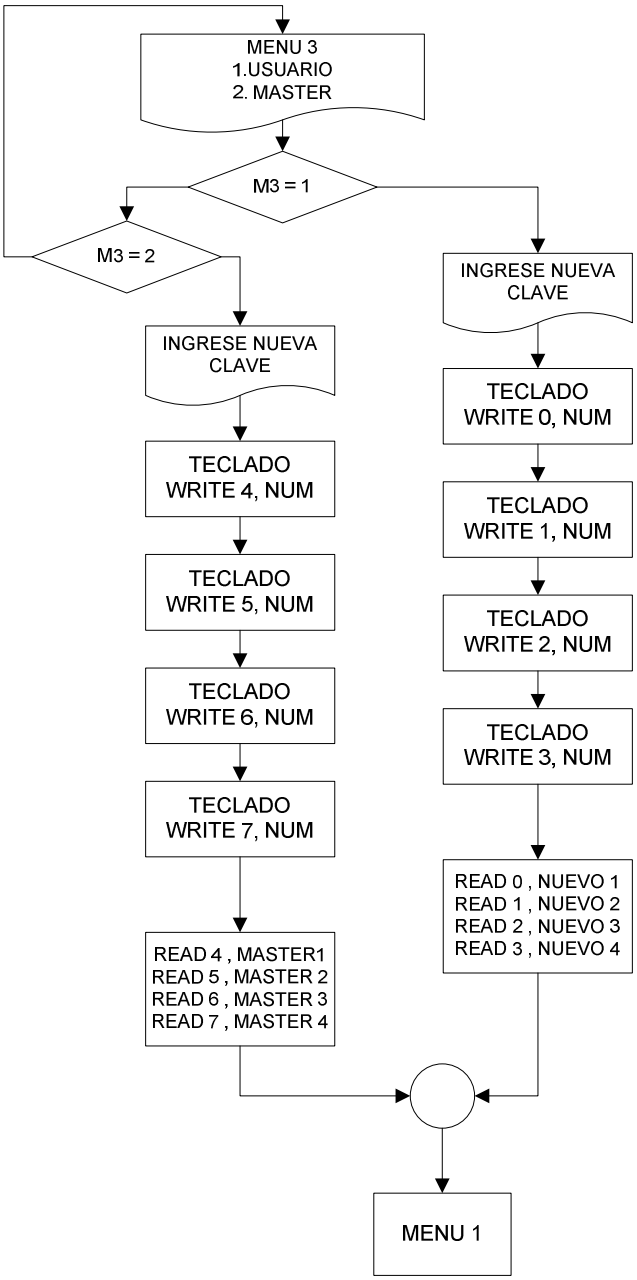
ANEXO 8.

DIAGRAMA DE FLUJO INGRESO DE CLAVE Y VERIFICACION DE HUELLA DEL SISTEMA CONTROL DE ACCESO



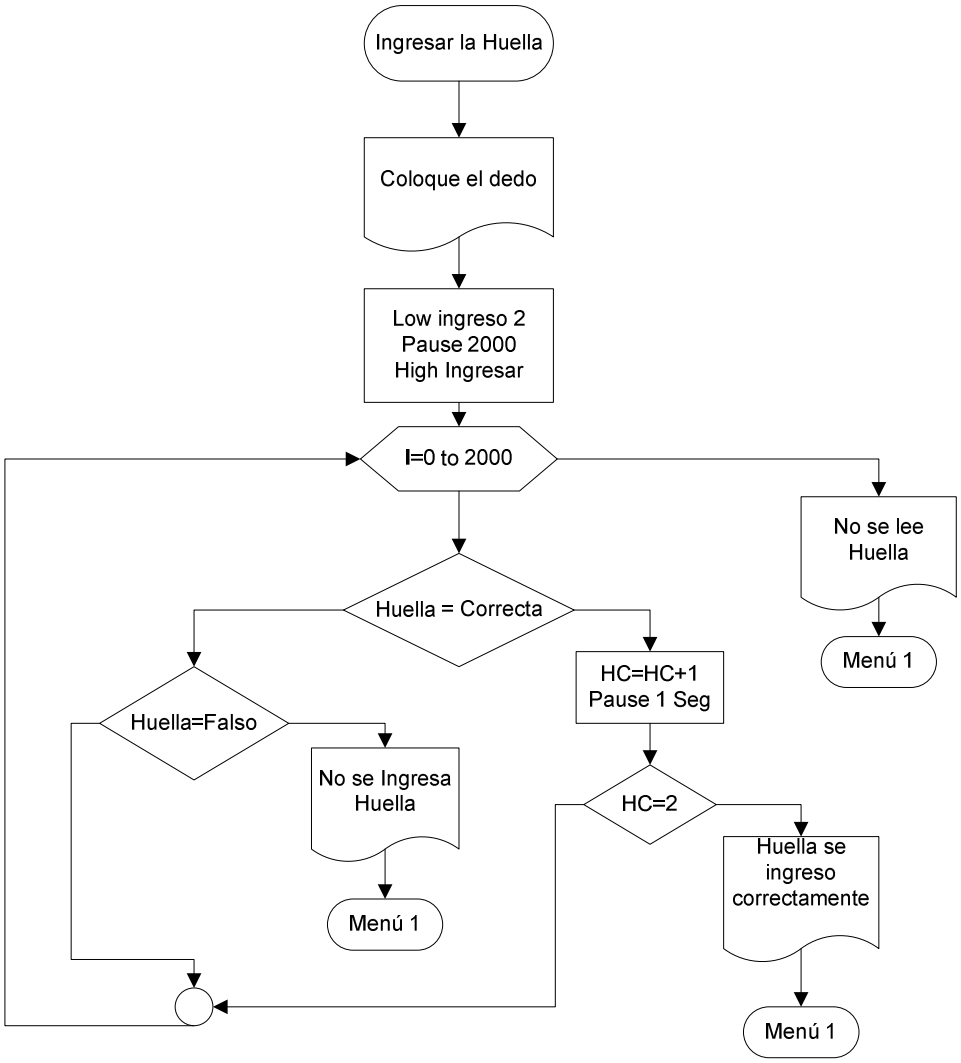
ANEXO 9.

DIAGRAMA DE FLUJO DE CAMBIO DE CLAVE DEL SISTEMA CONTROL DE ACCESO



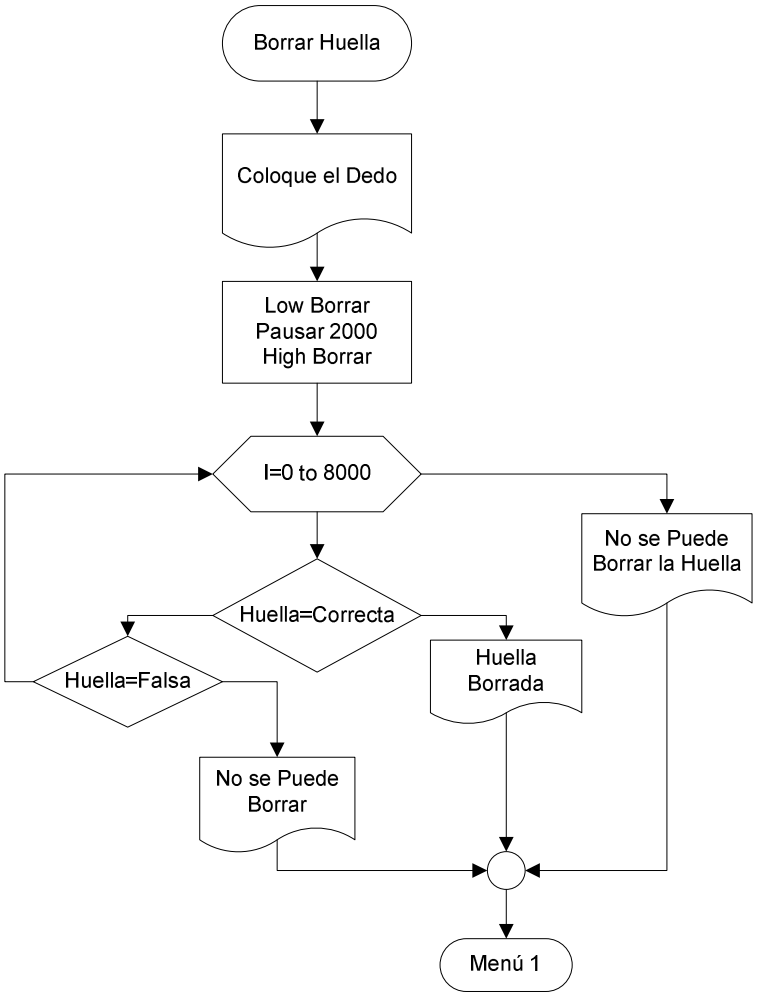
ANEXO 10.

DIAGRAMA DE FLUJO INGRESO DE HUELLA DIGITAL DEL SISTEMA CONTROL DE ACCESO



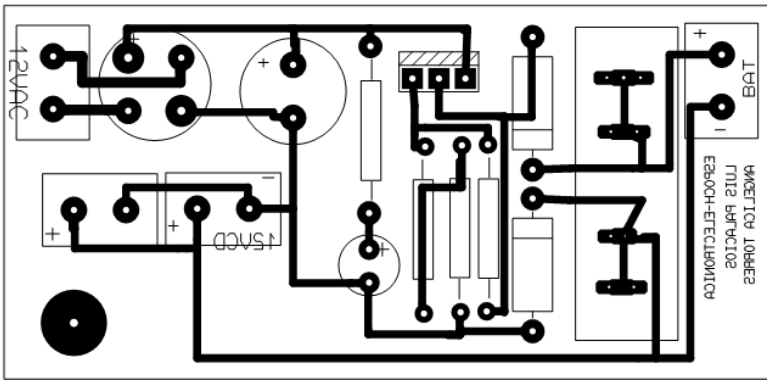
ANEXO 11.

DIAGRAMA DE FLUJO BORRADO DE HUELLA DIGITAL DEL SISTEMA CONTROL DE ACCESO

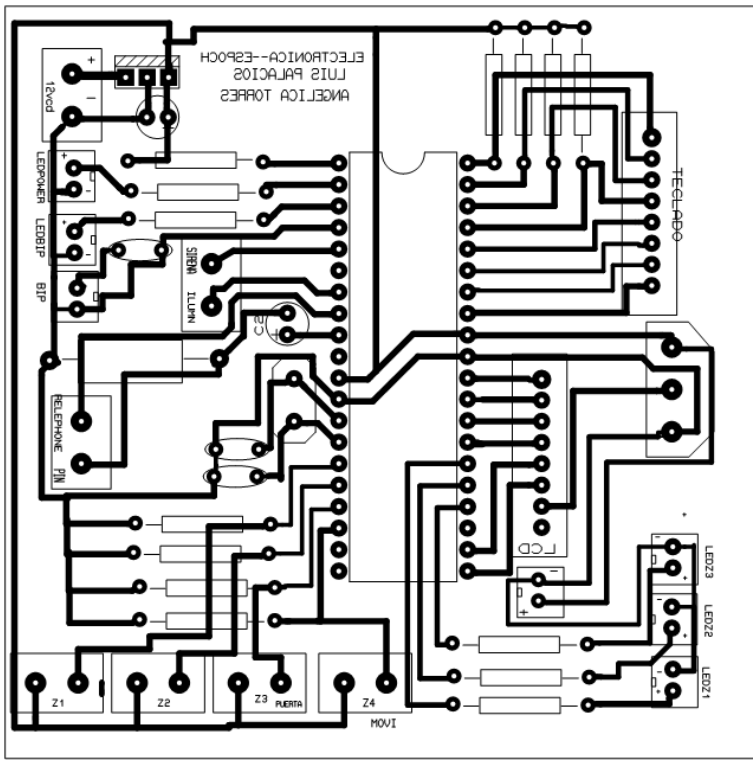


ANEXO 12.

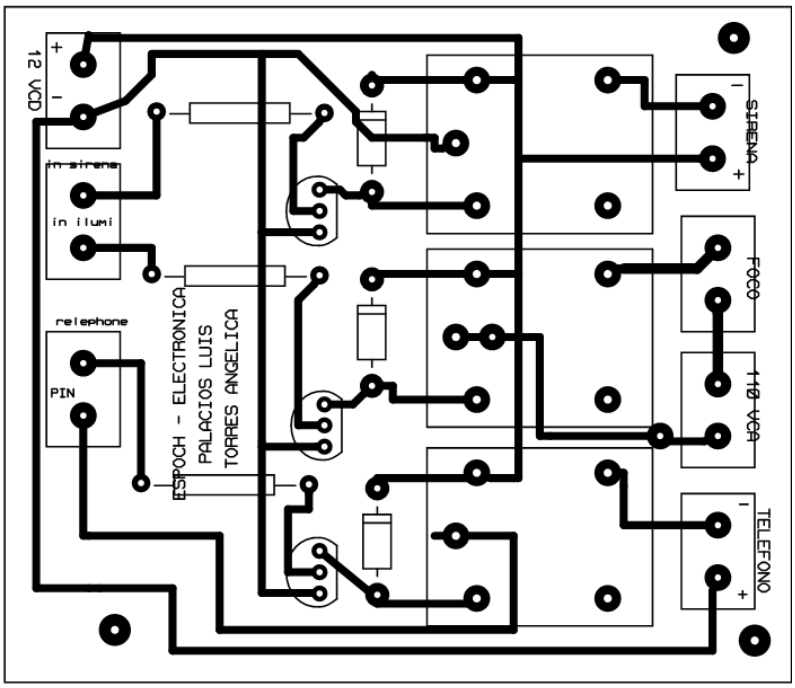
CIRCUITOS IMPRESOS DEL SISTEMA DE SEGURIDAD



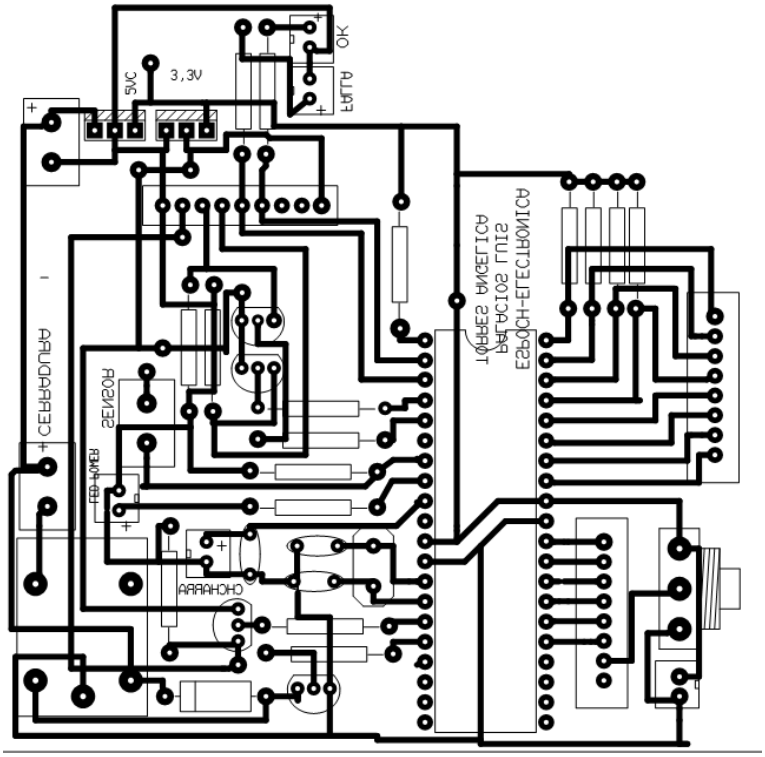
CIRCUITO IMPRESO DE LA FUENTE DE ALIMENTACION



CIRCUITO IMPRESO DE LA CENTRAL DE PROCESAMIENTO DEL SISTEMA DE SEGURIDAD



CIRCUITO IMPRESO ETAPA DE RESPUESTA DEL SISTEMA DE SEGURIDAD



CIRCUITO IMPRESO SISTEMA DE CONTROL DE ACCESO

BIBLIOGRAFÍA

1. BOYLESTAD, L. Electrónica Teoría de Circuitos. 6. ed. México DF-Mexico. Prentice Hall. 1997 pp. 115 – 213

2. COMO FUNCIONA UN PIR. http://blogdeseguridadelectronica.blogspot.com/2008/08/como-funciona-un-pir.html [En línea] [2010-11-20]

3. Corrales, Santiago. Electrónica Práctica con Microcontroladores PIC. Quito-Ecuador, 2006 177p.

4. ISIS DE PROTEUS ; (HAZAEL INDER) http://www.monografias.com/trabajos-ppt/tutorial-isis-proteus/tutorial-isis-proteus.shtml [En línea] [2011-01-28]

5. MICROCONTROLADORES ; (MERLYNCK) http://www.monografias.com/trabajos12/microco/microco.shtml [En línea] [2011-01-29]

6. REYES, Carlos. Microcontroladores PIC. 2. ed. Quito-Ecuador: Rispergraf, 2006. 210p.

7. SISTEMAS BIOMETRICOS: MATCHING DE HUELLAS DACTILARES MEDIANTE TRANSFORMADA DE HOUGH GENERALIZADA ; (MORALES DOMINGO) http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm [En línea] [2011-02-02]

8. TECNOLOGIAS DE IDENTIFICACIÓN POR HUELLA DACTILAR ; (GRAEVENITZ GERIK) http://www.applied-biometrics.com/fileadmin/download/Article_Huellas_Dactilares.pdf [En línea] [2011-02-05]

9. TUTORIAL MICROCONTROLADORES PIC ; (TORRES MIGUEL)
http://web.ing.puc.cl/~mtorrest/downloads/pic/tutorial_pic.pdf [En línea] [2011-01-20]