

MON
621.39928
N973
2013



UNIVERSIDAD NACIONAL DE INGENIERÍA
RECINTO UNIVERSITARIO SIMÓN BOLÍVAR
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

INFORME FINAL DEL TRABAJO MONOGRÁFICO PARA OPTAR AL TÍTULO DE INGENIERO EN
ELECTRÓNICA

“DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO Y ALARMA CONTRA
INTRUSO EN EL DEPARTAMENTO DE ELECTRONICA DE LA FEC - UNI.”

AUTORES:

Saúl Otoniel Núñez Zeledón.
Milton José Zeledón Espinoza.

TUTOR:

M. Sc. Camilo Roosevelt Lindo Carrión

ENTIDAD QUE PROMUEVE:

Dirección de Bienestar Estudiantil.
Vice Rectoría de I+D.

Febrero del 2013

Managua, Nicaragua

DEDICATORIA

A mi madre.
Saúl Núñez

A mi madre por su esfuerzo y apoyo incondicional.
A mis maestros por dedicarse a nuestra formación.
Milton Zeledón

RESUMEN

Este trabajo monográfico tiene el propósito de brindar una alternativa de solución al problema de seguridad que afectaba al departamento de electrónica de la FEC-UNI, la cual radica en pérdidas de equipos y materiales de los profesores debido a la falta de control del personal que ingresa al local. De las opciones evaluadas para dar solución al problema se optó por realizar un proyecto de I&D que consiste en un sistema de control de acceso y alarma contra intruso ajustado a los requerimientos del departamento.

Para implementar la solución se utilizó el sistema de desarrollo SmartGLCD 240x128, esta cuenta con una pantalla táctil, microcontrolador integrado (PIC18F8722), un puerto USB, lector de memorias microSD y puertos de Entrada/Salida disponibles para monitorear y controlar dispositivos externos.

Se diseñó un sistema de control de acceso que utiliza como credencial una clave de seis dígitos. Para poder ingresar, cada docente debe autenticarse a través de una interfaz táctil que funciona como mecanismo de entrada/salida de datos.

El sistema también es capaz de: monitorear los detectores de intruso e incendio instalados, evaluar su estado y activar las alarmas local o remota (implementada utilizando módulos de radiofrecuencia RFPIC). La alarma local se utiliza para alertar a los docentes durante las horas laborales, la alarma remota se utiliza para avisar al CPF (Cuerpo de Protección Física) durante las horas no laborales.

El sistema es capaz de crear un registro de eventos (accesos permitidos y alarmas) en formato de Excel y almacenarlo en la microSD, para lograrlo se precisa de un RTC que proporciona información de hora/fecha al sistema.

Se adoptó el método científico como guía durante todas las etapas del trabajo monográfico, el resultado que se obtuvo fue un sistema control de acceso y alarma contra intrusos instalado y optimizado para proteger el departamento, el cual actualmente es más seguro generando tranquilidad y confianza en los docentes usuarios del sistema.

INDICE DE CONTENIDOS

I. INTRODUCCION.....	1
II. OBJETIVOS	2
OBJETIVO GENERAL.....	2
OBJETIVOS ESPECÍFICOS	2
III. JUSTIFICACION	3
IV. MARCO TEORICO	5
CAPITULO 1: SEGURIDAD ELECTRONICA.....	5
1 SISTEMAS DE SEGURIDAD ELECTRONICA.....	6
1.1 SISTEMAS DE CONTROL DE ACCESO	6
1.1.1 Credenciales	6
1.1.2 Lectores	8
1.1.3 Panel de control de campo	9
1.1.4 Cerraduras electromagnéticas	11
1.2 SISTEMAS DE ALARMA CONTRA INTRUSO	15
1.2.1 Dispositivos de detección.....	15
1.2.2 Panel de control de alarmas	20
1.2.3 Sistemas de señalización.....	23
1.3 SISTEMAS DE ALARMA CONTRA INCENDIO	27
1.3.1 Detector de humo.....	27
CAPITULO 2: PLATAFORMA DE DESARROLLO SMARTGLCD 240X128	28
2 SMARTGLCD 240X128 BOARD	28
2.1 PANTALLA TÁCTIL.....	28
2.2 MICROCONTROLADOR PIC18F8722.....	31
2.3 MODULO USB – UART	33
2.4 LECTOR DE TARJETA MICROSD.....	35
CAPITULO 3: ANALISIS Y PRESENTACION DE RESULTADOS.....	36
3 METODOLOGIA ADOPTADA	36
3.1 ANALISIS.....	36
3.1.1 Condiciones de seguridad del departamento de electrónica.....	36
3.1.2 Requerimientos del sistema de seguridad	38
3.2 DISEÑO DEL UN SISTEMA DE SEGURIDAD ELECTRONICA.....	39
3.2.1 Consideraciones de diseño.....	39
3.2.2 Descripción general del sistema	40
3.2.2.1 Subsistema de Control de Acceso.....	41

3.2.2.1.1 Selección de los principales componentes de Control de Acceso.....	41
3.2.2.2 Subsistema de Alarmas.....	46
3.2.2.2.1 Selección de los principales componentes de Alarma de Intruso.	47
3.2.2.2.2 Hardware de subsistemas de Control de Acceso y Alarmas ..	51
3.2.2.2.3 Algoritmo para los subsistemas de Control de Acceso y Alarma	65
3.2.2.2.4 Alimentación de los Subsistemas de Control de Acceso y Alarma	68
3.2.2.3 Subsistema de Señalización Remota	70
3.2.2.3.1 Selección de principales componentes de Señalización Remota.....	71
3.2.2.3.2 Alimentación del Subsistema de Señalización Remota	74
3.2.2.3.3 Algoritmo propuesto para el subsistema de Señalización Remota.....	75
3.3 IMPLEMENTACION DEL PROTOTIPO.....	77
3.3.1 Programación de los MCUs	77
3.3.1.1 Compilador mikroBASIC PRO for PIC v4.6	77
3.3.1.2 Desarrollo del programa de control del PIC18F8722.....	79
3.3.1.3 Elaboración de la interfaz grafica con Visual GLCD	85
3.3.1.4 PROTEUS 7.10	88
3.3.1.4.1 Simulación y depuración de errores con ISIS (MMC, RTC, GLCD)	88
3.3.1.5 Resultados de la programación del SmartGLCD	89
3.3.2 Diseño y Fabricación del Hardware requerido	94
3.3.3 Instalación y montaje del sistema	95
3.4 PRUEBAS DE FUNCIONAMIENTO Y CORRECCION DE ERRORES.....	97
3.4.1 Resultados	99
3.4.2 Costos del prototipo	100
CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES.....	101
BIBLIOGRAFIA.....	103
ANEXOS.....	104

LISTA DE FIGURAS

Figura 1. Credenciales de un control de acceso electrónico.	7
Figura 2. Lectores de un control de acceso electrónico.	9
Figura 3. Cerradura electromagnética.	11
Figura 4. Montaje de lámina metálica en Soporte Z.	12
Figura 5. Arquitectura de un control de acceso basado en PC.	14
Figura 6. Control de acceso autónomo Promi1000.	14
Figura 7. Contacto magnético.	17
Figura 8. Tamaño de una zona de detección.	19
Figura 9. Resistor de fin de línea.	22
Figura 10. Detector de humo fotoeléctrico.	27
Figura 11. SmartGLCD 240x128 Board.	28
Figura 12. Conexión entre PIC18F8722, RA6963 y Controlador de Panel.	30
Figura 13. Diagrama en boques del PIC18F8722.	32
Figura 14. Diagrama de conexión del modulo USB UART integrado.	34
Figura 15. Diagrama de conexión del lector de tarjeta microSD integrado.	35
Figura 16. Planta arquitectónica del departamento de electrónica.	37
Figura 17. Diagrama en Bloques del Sistema de Seguridad Electrónica.	40
Figura 18. Diagrama en Bloques del Subsistema de Control de Acceso.	41
Figura 19. Cerradura electromagnética ECL-ACC300.	44
Figura 20. Reloj de Tiempo Real DS1307.	45
Figura 21. Diagrama en Bloques del Subsistema de Alarmas.	47
Figura 22. Detector de movimiento BV-300.	48
Figura 23. Detector de humo FSA-410B.	49
Figura 24. Sirena audible SD15WULF.	50
Figura 25. Sirena piezoeléctrica con luz estroboscópica PSR.	51
Figura 26. Diagrama de circuito del SmartGLCD240x128 Board.	52
Figura 27. Conexión entre un detector y un canal de entrada.	54
Figura 28. Conexión entre un pulsador y un canal de entrada.	54
Figura 29. Canal de entrada de la tarjeta de interfaz.	55
Figura 30. Diagrama de circuito de la interfaz de entrada.	56

Figura 31. Canal de salida a relevador.	57
Figura 32. Canal de salida a transistor MOSFET.	60
Figura 33. Canal de salida a transistor BJT.	61
Figura 34. Diagrama de circuito de la interfaz de salida.	62
Figura 35. Diagrama de circuito de la tarjeta de control del DS1307.	63
Figura 36. Algoritmo propuesto para subsistemas de Control de Acceso y Alarma.	67
Figura 37. Fuentes de alimentación conmutadas a) CFM40T-02. b) S-60-12.	69
Figura 38. Diagrama en bloques del Subsistema de Señalización Remota.	70
Figura 39. Diagrama de circuito de la interfaz de recepción de alarmas.	73
Figura 40. Fuente de alimentación con cargador de batería ST-2406-2.	75
Figura 41. Algoritmo propuesto para el subsistema de señalización remota, a) Programación del rPIC12F675F, b) Programación del PIC16F676.	76
Figura 42. Entorno de programación de mikroBASIC PRO for PIC v4.6.	78
Figura 43. Menú de herramientas de mikroBASIC PRO.	79
Figura 44. Estructura modular del programa del PIC18F8722.	80
Figura 45. Gráficos en lógica negativa para Visual GLCD.	85
Figura 46. Menú de configuración de Visual GLCD.	86
Figura 47. Coordenadas de la imagen editada.	86
Figura 48. Código de BASIC generado por GLCD Bitmap Editor.	87
Figura 49. Pantalla de usuario (Acceso Permitido).	87
Figura 50. Simulación del SmartGLCD240x128Board.	89
Figura 51. Pantalla de inicio.	89
Figura 52. Teclado alfanumérico.	90
Figura 53. Código invalido.	90
Figura 54. Pantalla de usuario.	90
Figura 55. Pantalla de ingreso.	91
Figura 56. Pantalla de administrador.	91
Figura 57. Configuración del RTC.	91
Figura 58. Gestión de cuentas.	92
Figura 59. Sistema armado.	92

Figura 60. Registro de eventos compatible con Microsoft Excel.	93
Figura 61. Tarjetas electrónicas fabricadas.	94
Figura 62. Ubicación de los componentes del sistema de seguridad.	96
Figura 63. Pantallas de autenticación anteriormente propuestas utilizando: a) Teclado numérico, b) Teclado alfanumérico.	98
Figura 64. 1: Filtro vertical, 2: Electrodo (sus formas determinan los pixeles que se mostraran), 3: Cristales líquidos, 4: Electrodo común, 5: Filtro horizontal, 6: Superficie reflectante (no incluida con pantalla retroiluminada).	106
Figura 65. Diagrama en bloques del RA6963.	107
Figura 66. Panel táctil resistivo.	109
Figura 67. Estructura de un panel táctil resistivo.	110
Figura 68. Gradiente de voltaje de una capa resistiva.	110
Figura 69. Controlador de panel táctil resistivo.	111
Figura 70. Dimensiones de memorias SD, miniSD y microSD.	115
Figura 71. Modulo transmisor rfPIC12F675.	118
Figura 72. Diagrama de circuito del rfPIC12f675.	118
Figura 73. Diagrama en bloques del transmisor rf12F675.	119
Figura 74. Codificación PWM con modulación ASK.	120
Figura 75. Formato de transmisión del protocolo Keelog.	120
Figura 76. Organización de la palabra de código.	121
Figura 77. Modulo receptor rfRXD0420.	122
Figura 78. Diagrama de circuito del rfRXD0420.	122
Figura 79. Filtro de onda superficial (SAW Filter).	123
Figura 80. Señal RSSI.	124
Figura 81. Comparación entre el voltaje de referencia y RSSI.	125
Figura 82. Procedimiento de programación del transmisor.	126
Figura 83. Bus I2C.	128
Figura 84. Lógica de trasmisión de datos en un bus I2C.	129
Figura 85. Señalización Start y Stop de un bus I2C.	129
Figura 86. Esquema de transmisión de datos del protocolo I2C.	130
Figura 87. Formato de Trasmisión/Recepción entre Maestro - Esclavo.	130

Figura 88. Lógica de transmisión de datos en un Bus SPI.	132
Figura 89. Bus SPI.	133
Figura 90. Diagrama en bloques del Puerto Serial Sincrono Maestro (SPI).	133
Figura 91. Procedimiento para transferir el Netlist de ISIS a ARES.	135
Figura 92. Diseños de los PCB. a) Interfaz de Entrada, b) Interfaz de Salida, c) Interfaz de Recepción de Alarma, d) Tarjeta de Control de Reloj.	136
Figura 93. Representación 3D de los diseños de la Figura 92.	137
Figura 94. Impresión en filmina de un circuito impreso (revelado invertido).	138
Figura 95. Tarjeta de cobre preparada para su exposición a los Rayos UV.	139
Figura 96. a) Tiempo de exposición de 600 segundos, b) Tarjeta en proceso de revelado después de la insolación.	139
Figura 97. a) Tarjeta inmersa en Percloruro Férrico, b) Proceso de perforación de puntos de montaje (Broca de 0.75mm).	140

LISTA DE TABLAS

Tabla 1: Detectores de intruso para uso exterior.	16
Tabla 2: Principales características de las Pantallas Inteligentes propuestas.	42
Tabla 3: Características técnicas de la cerradura seleccionada.	43
Tabla 4: Principales características de los RTC propuestos.	45
Tabla 5: Principales características de Sensores de Movimiento propuestos.	47
Tabla 6: Principales características de los Sensores de Humo propuestos.	49
Tabla 7: Principales características de las Alarmas Interiores propuestas.	50
Tabla 8: Principales características de Alarmas para uso exterior propuestas.	51
Tabla 9: Consumo de los componentes de Control de Acceso y Alarmas.	68
Tabla 10: Especificaciones técnicas de las fuentes de alimentación seleccionadas.	69
Tabla 11: Principales características de los módulos transmisores propuestos.	71
Tabla 12: Principales características del modulo receptor rfRXD0420.	72
Tabla 13: Consumo de componentes del subsistema de Señalización Remota.	73
Tabla 14: Costos de implementación del prototipo.	100
Tabla 15: Descripción de los pines del RA6963.	108
Tabla 16. Voltajes de salida del controlador de panel táctil resistivo.	113

I. INTRODUCCION

El presente trabajo monográfico consiste en brindar una alternativa de solución a la problemática existente en el Departamento de Electrónica de la FEC¹, la cual radica en la inseguridad de los equipos informáticos (PC², UPS³, mouse) y documentos académicos (libros) entre otros, que se encuentran en el local.

Este local, junto a los equipos antes mencionados han sido asignados a los docentes del departamento, sin embargo desde hace seis años los profesores han sufrido muchas pérdidas de bienes, lo cual les ha generando desconfianza. Esto ha provocado que muchos profesores opten por cargar con sus bienes, otros simplemente ya no utilizan este sitio.

Debido al carácter público del departamento y sus alrededores, frecuentemente hay personas haciendo gestiones, como consultas académicas y trámites administrativos, por tanto, es necesario implementar un sistema que controle el acceso al local para evitar que personas ajenas al departamento puedan ingresar sin el consentimiento de los docentes.

Nuestra alternativa incrementara la seguridad del local, a través del diseño e implementación de un sistema de seguridad electrónico que controlará el acceso al departamento, además de realizar la gestión de alarma contra intrusos y notificar al personal de seguridad de la UNI⁴ en caso de que se detecten anomalías.

¹ FEC: Facultad de Electrotecnia y Computación

² PC: Personal Computer

³ UPS: Uninterrupted Protection System

⁴ UNI: Universidad Nacional de Ingeniería

II. OBJETIVOS

Objetivo General

Brindar una alternativa de solución a la problemática de seguridad del departamento de electrónica de la FEC - UNI para garantizar un ambiente de trabajo seguro, mediante el diseño e implementación de un sistema de seguridad electrónica usando la tecnología de microcontroladores PIC, cuyo desempeño será evaluado a través de pruebas con el sistema instalado.

Objetivos Específicos

1. Diseñar e implementar un sistema de control de acceso y alarma contra intrusos con las siguientes funciones:
 - i. Control de acceso al Departamento de Electrónica de la FEC-UNI.
 - ii. Detección de intrusos en horarios que el acceso no está autorizado.
 - iii. Detección indicios de incendios.
 - iv. Generación un registro de eventos de acceso y alarma con posibilidad de transferirse y visualizarse en una PC.
 - v. Alerta al CPF ante cualquier evento que atente contra la seguridad del local a través de una señal de alarma remota.
2. Implementar una fuente de alimentación ininterrumpida (UPS) para respaldar el suministro energético del sistema durante cortes de energía.
3. Evaluar el desempeño de la alternativa de solución a través de pruebas prácticas con el sistema instalado.

III. JUSTIFICACION

Según el cuestionario realizado a los docentes del departamento de Electrónica de la FEC-UNI, en los últimos síes años se han perdido artículos de este local.

El jefe del departamento, el decano y el personal de seguridad también se ven afectados por esta problemática, debido a que ellos reciben los reclamos en orden jerárquico por parte de los profesores. Es evidente que se necesita resolver este problema para que el departamento de electrónica sea mas seguro.

Después de analizar esta situación proponemos diseñar e implementar un sistema de seguridad electrónico formado por un control de acceso y un sistema de alarma contra intruso adaptado a los requerimientos particulares del local.

Este proyecto proporcionara un ambiente de trabajo seguro a los docentes que utilicen este local y evitara la incómoda situación de cargar diariamente los materiales utilizados en su labor docente. También beneficiara indirectamente al jefe del departamento y decano debido a que este sistema mantendrá resguardados los materiales y equipos del local, controlando el acceso y almacenando información (hora, fecha y usuario) de los eventos de entrada/salida. Beneficiará a los autores debido a que con este trabajo monográfico podremos obtener el título de Ingeniero electrónico, además de la satisfacción personal de haber contribuido a resolver un problema social.

Pondremos a disposición de la comunidad universitaria los resultados producidos por nuestra investigación, que constituirán un conjunto de conocimientos en el campo de la seguridad electrónica y programación de microcontroladores, los cuales pueden ser utilizados como referencia para futuros proyectos o investigaciones.

También se pretende comprobar si este sistema puede tener aplicaciones potenciales en oficinas y residencias, para lo cual hemos solicitado asesoría al personal técnico de la Empresa **Seguridad C y B**. Si así fuera, este sistema

podría ser propuesto como un prototipo de sistema de seguridad electrónico ante el CONICYT⁵ para su respectiva aprobación y certificación.

⁵ CONICYT: Consejo Nacional de Ciencia y Tecnología

IV. MARCO TEORICO

CAPITULO 1: SEGURIDAD ELECTRONICA

La seguridad es un tema de relevancia social debido al incremento de la delincuencia que existe actualmente [Philip 1998, P.3].

Los delincuentes son más sutiles que antes y siempre utilizan nuevas técnicas para adentrarse en los establecimientos y vehículos con bienes de valor.

Esto ha obligado a las empresas que brindan servicios de seguridad privada, que constantemente mejoren sus técnicas de operación utilizando tecnología moderna en la protección de bienes y prevención de incidentes.

Uno de los avances tecnológicos que ha revolucionado la industria de seguridad es el desarrollo de la electrónica, sus invenciones en materia de seguridad han dado origen a un nuevo campo en la ingeniería conocido como Seguridad Electrónica [Robert 2007, P.vii].

La Seguridad Electrónica desarrolla dispositivos y sistemas capaces de realizar tareas de seguridad utilizando componentes electrónicos. Su principal objetivo dentro de un programa de seguridad es realizar los procesos de detección de intrusos, restricción de acceso a áreas no autorizadas y prevención de incidentes [Robert 2007, P.53].

Los primeros sistemas estaban enfocados a la detección y el control de acceso, sin embargo debido a la facilidad de integración y disminución de costos de los sistemas electrónicos pronto se integraron los sistemas contra incendios.

Este trabajo monográfico se basa en el diseño e implementación de un sistema de seguridad electrónica. Para tener una mejor comprensión de los resultados de este proyecto se presentan los fundamentos teóricos que conforman la base de conocimientos que fueron empleados durante su desarrollo.

1 SISTEMAS DE SEGURIDAD ELECTRONICA

La Seguridad Electrónica es un mecanismo de ayuda para que los oficiales de seguridad a realicen su trabajo de forma rápida y eficiente [Philip 1998, P.4].

Estos sistemas utilizan componentes electrónicos para detectar intrusos, indicios de incendio, intentos de robo de artículos protegidos, entre otros. Su deber es avisar al usuario del sistema (ocupantes, personal de seguridad) cuando se presenta un evento que quebranta la seguridad del local, para que este tome las acciones correctivas necesarias.

Existen varias soluciones que se ofrecen en el mercado, las cuales se pueden integrar para formar una solución de seguridad completa. Dentro de las más comunes tenemos:

- Sistemas de control de acceso electrónico.
- Sistemas de alarma contra intrusos.
- Sistemas de alarma de incendios.
- Sistemas contra incendios.
- Circuito cerrado de televisión (CCTV).
- Inspección electrónica de artículos.
- Estación Central de Monitoreo o Centro de Control de Seguridad.

1.1 SISTEMAS DE CONTROL DE ACCESO

Es una forma de controlar electrónicamente el acceso de personas a un área restringida. En estos sistemas se puede definir quién puede tener acceso, en que horario y a que áreas está autorizado su ingreso utilizando una base de datos que guarda el registro de los usuarios del sistema [Robert 2007, P.1-2].

Componentes de un sistema de control de acceso [Access Control, 2012]:

1.1.1 Credenciales

Las credenciales son un mecanismo de identificación que se utiliza para tener acceso a un área determinada dentro de un edificio.

Según el modo de autenticación empleado, las credenciales se pueden clasificar en las siguientes categorías:

1. Algo que el usuario conoce, como una clave, un PIN (Personal Identification Number).
2. Algo que el usuario puede llevar como una tarjeta RFID (Radio Frequency Identification), magnética, inteligente, entre otras.
3. Algún rasgo físico del usuario como su huella dactilar, la geometría de su mano, reconocimiento del iris, la retina y reconocimiento de voz.

En la figura 1 se presentan ejemplos prácticos de las credenciales que utilizan los sistemas de control de acceso de uso comercial.



a) Acceso por PIN.

b) Tarjetas de acceso RFID, de proximidad y Smartcard.



c) Autenticación biométrica, huella dactilar (1), geometría de la mano (2) y reconocimiento de retina (3).

Figura 1. Credenciales de un control de acceso electrónico.

1.1.2 Lectores

Los lectores se utilizan para obtener los datos de identificación de los usuarios del sistema, no toman la decisión de permitir/denegar el acceso, su función es mandar el número de identificación del usuario al panel de control para que se verifique si su acceso está autorizado en la base de datos [Card Reader, 2011].

La tecnología de un lector en un sistema de control de acceso está determinada por el tipo de credencial utilizado, dentro de los más comunes se encuentran:

El teclado: Este periférico utiliza una matriz de interruptores electrónicos para mandar información al panel de control. En los sistemas de control de acceso se utilizan para ingresar una clave o un PIN al sistema, los podemos encontrar en versión hardware o implementados por software en pantallas táctiles.

Lector de tarjetas: Este dispositivo electrónico lee el número de identificación de un usuario que contienen las tarjetas de acceso. Según el tipo de tarjeta implementado en el sistema, este puede ser un lector de código de barras, cinta magnética, tarjetas de efecto Wiegand, de proximidad o un lector de tarjetas inteligentes.

Lector biométrico: Son equipos electrónicos capaces de realizar una lectura de algún rasgo físico (huella digital, retina, geometría de la mano, entre otros) de una persona para compararlo con una muestra almacenada en la memoria del sistema, si la correlación entre estas es coherente el lector envía el número de identificación del usuario al panel.

Lectores mixtos: Utilizan una combinación de las tecnologías antes descritas para incrementar el nivel de seguridad. Los más comunes son lectores de tarjetas con teclado integrado, o lectores biométricos con lector de tarjetas, estos exigen ambos procesos de autenticación.

Los lectores son fabricados en diversos modelos con el acabado y calidad que se requiere en los distintos ambientes de trabajo. La figura 2 muestra cinco ejemplos de los lectores que ofrece la industria de seguridad.



a) Teclado (Lector de PIN o clave).



b) Lector de tarjetas.



c) Lector de huella dactilar.



d) Lectores mixtos dactilar – tarjeta, dactilar – teclado.

Figura 2. Lectores de un control de acceso electrónico.

1.1.3 Panel de control de campo

En este panel se encuentran los componentes electrónicos necesarios para controlar uno o varios puntos de acceso.

Las partes principales que conforman a un panel de control de campo son:

El controlador electrónico: Es el cerebro del sistema, lo podemos encontrar implementado utilizando un MCU (Microcontroller Unit) o MPU (Microprocessor Unit), en su memoria reside un algoritmo de control capaz de interpretar los

datos recibidos desde los lectores para compararlos con los que están en la base de datos del sistema y permitir/denegar el acceso en función de la hora, fecha, área solicitada y número de identificación del usuario.

También se encarga de enviar la señal eléctrica para abrir/cerrar la puerta y guardar en un registro de cada evento de ingreso.

Reloj de tiempo real (RTC): Es un reloj/calendario dentro de un IC (circuito integrado) que proporciona la hora y fecha con exactitud para utilizarla en un sistema con MPU/MCU. Su base de tiempo la establece un cristal de cuarzo y para garantizar su desempeño utiliza una batería de respaldo.

Memoria: Es un dispositivo para guardar información digital, se puede leer/escribir eléctricamente utilizando un MPU/MCU. Su función es almacenar la base de datos de los usuarios y el registro de accesos, para lograrlo el controlador realiza las operaciones de lectura/escritura durante el procedimiento de autenticación.

Interfaz de entrada: Para realizar la adquisición de los datos provenientes de lectores, botones de salida/reinicio, contactos magnéticos, entre otros el panel de control utiliza un circuito electrónico dedicado a recolectar y acondicionar las señales de entrada para su lectura en el controlador.

Interfaz de salida: Proporciona un acoplamiento seguro entre componentes eléctricos, ópticos y electromecánicos para realizar las funciones que comanda el controlador. Por ejemplo energizar una alarma audible, señal lumínica, un zumbador, una cerradura electromagnética, entre otras.

Interfaz de comunicación: En edificios con considerables cantidades de usuarios generalmente se implementa una solución basada en PC/servidor. La interfaz de comunicación es un módulo dedicado a soportar el protocolo de comunicación utilizado entre el panel de control de campo y el servidor.

Su función principal es garantizar una vía de acceso a la información registrada en los equipos que forman parte del sistema.

1.1.4 Cerraduras electromagnéticas

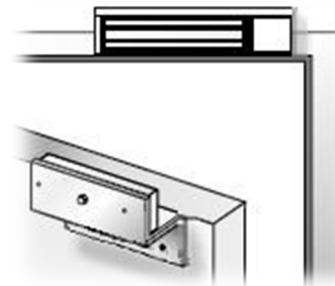
Las cerradura electromagnética es un dispositivo de boqueo para puertas, su funcionamiento se basa en el principio del electromagnetismo [Bill 2008, P.181].

Estas cerraduras tienen dos componentes básicos: un electroimán y una lámina rectangular de metal ferroso (Figura 3, ilustración “a”).

Para garantizar un buen desempeño el electroimán se instala en el marco y la lámina de metal en el cuerpo de la puerta, así como se muestra en la ilustración “b” de la figura 3, de manera que al cerrar la puerta, la lámina metálica queda frente al electroimán. Al energizar adecuadamente el electroimán (12/24V_{DC}) este genera una fuerza magnética capaz de sujetar la lámina metálica y mantener la puerta cerrada de manera segura. Típicamente la fuerza de atracción es de 300 – 3000 libras según lo requiera la aplicación.



a) Cerradura electromagnética.



b) Instalación en puerta de vidrio.

Figura 3. Cerradura electromagnética.

Para montar la cerradura en puertas de vidrio se requiere de un accesorio conocido como **soporte Z**, en la figura 3, ilustración “b” se muestra cómo se utiliza este soporte para el montaje.

Un soporte Z es una lámina rígida de metal en forma de una Z diseñada para el montaje y alineamiento de cerraduras electromagnéticas. Obsérvese la figura 4.



Figura 4. Montaje de lámina metálica en Soporte Z.

Ventajas cerraduras electromagnéticas

- Accionamiento remoto a través de un interruptor o desde un panel de control de acceso.
- Bajo consumo de energía, normalmente entre 3 - 8 Vatios.
- Dejan libre la puerta ante una falta del suministro eléctrico o cuando se activa una alarma de fuego, esto es requerido en por el código de seguridad para edificios de los Estados Unidos de América.

Desventajas de las cerraduras electromagnéticas

- El costo es entre 4 – 10 veces mayor que una cerradura mecánica convencional.
- Se debe instalar baterías de respaldo para energizar el sistema y mantener segura la puerta cuando falle la fuente de energía comercial.

Las cerraduras electromagnéticas no son recomendadas en aplicaciones de máxima seguridad, fueron diseñadas para proteger puntos de acceso en áreas internas al edificio. La instalación de una cerradura electromagnética se debe realizar del lado interno al área protegida, para evitar que sus cables de alimentación queden expuestos y puedan ser cortados.

Funcionamiento de un control de acceso basado en PC/Servidor

Considere un edificio de oficinas en donde se utiliza un sistema de control de acceso basado en PC/Servidor (ver figura 5), el administrador del sistema le asigna a cada usuario una credencial. Para ingresar a las diferentes áreas del edificio, los usuarios presentan su credencial ante un lector (ubicados en cada punto de acceso), este adquiere el número de usuario y lo envía al panel de campo donde se da el proceso de autenticación. [Robert 2007, P.2]

El panel de control compara el número de identificación del usuario con los de la lista de acceso de su memoria para verificar si está autorizado su ingreso a esa área. Si no lo encuentra (pasa cuando un usuario ingresa por primera vez, no ha ingresado en un largo tiempo), el panel de control se comunica con el servidor en donde se encuentra la base de datos completa de todos los usuarios del sistema. Al encontrarlo en su lista de acceso, el servidor envía los datos al panel de control para que este le conceda/deniegue el ingreso en función de su nivel de acceso y horarios. Si el panel de control permite el acceso, se libera la puerta por unos 5 - 10 segundos aproximadamente, conectando (cerradura eléctrica) o desconectando (cerradura electromagnética) la alimentación eléctrica de la cerradura utilizada, durante este tiempo se ignora la señal que indica que la puerta está abierta para evitar una falsa alarma.

Si el acceso a esa área es denegado por falta de autorización o uso de credenciales falsas, se mantendrá bloqueada la puerta y se genera algún tipo de alarma. De igual forma el panel guarda en su historial de acceso los datos del usuario con la hora, fecha y área que ingreso o el intento de ingreso que fue denegado.

Este archivo forma parte de una base de datos completa que cada panel de control envía periódicamente al servidor para su almacenamiento y administración. La principal utilidad de su almacenamiento es controlar las horas de llegada/salida de los trabajadores, ayudar a encontrar un culpable de robo, prevenir intentos de asaltos, entre otros.

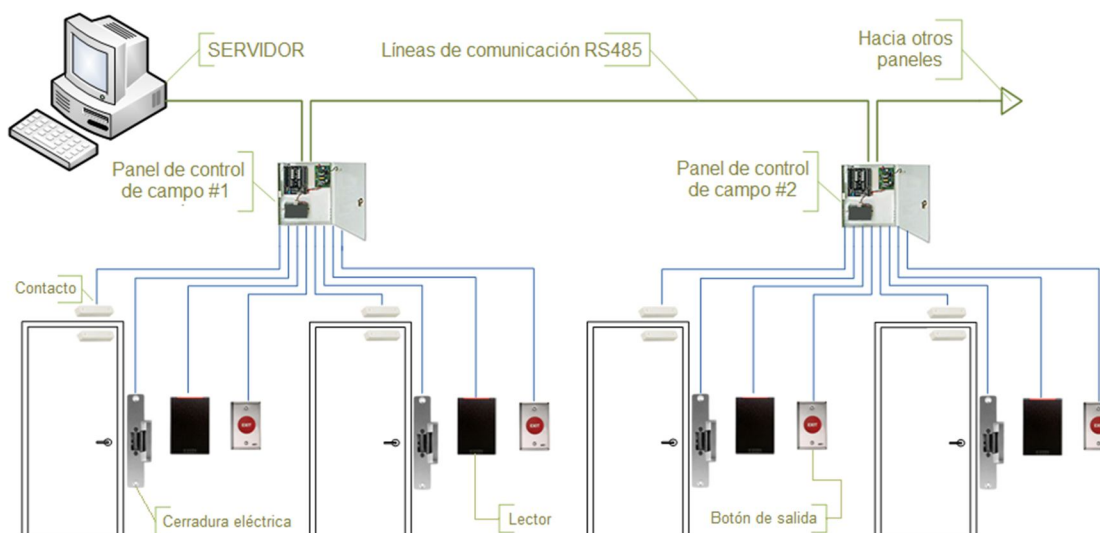


Figura 5. Arquitectura de un control de acceso basado en PC.

Funcionamiento de un control de acceso autónomo

La industria de seguridad ha desarrollado controles de acceso a diferentes escalas según la aplicación. El mercado nicaragüense demanda con mayor frecuencia sistemas autónomos de escala baja, la principal razón es el bajo costo y la capacidad de ampliación que estos equipos ofrecen.

Los controles autónomos operan bajo la misma filosofía de control que los demás sistemas, con la diferencia que no requieren un servidor ni red de datos. Su memoria es de mayor capacidad, esta puede almacenar hasta 1000 usuarios, 1000 eventos, controlan de 1 – 2 puertas en un equipo compacto tal como el **Promi1000** de SECURITY SYSTEMS PROVIDERS (ver figura 6).



Figura 6. Control de acceso autónomo Promi1000.

1.2 SISTEMAS DE ALARMA CONTRA INTRUSO

Los sistemas de alarma son parte fundamental de todo programa de seguridad, debido a que realizan la tarea principal: “Detección” [Robert 2007, P.53].

Estos sistemas utilizan sensores electrónicos para detectar a los intrusos que ingresan a un área protegida por el sistema y notifican a sus usuarios para que se ejecute una respuesta física ante tal evento.

Para comprender mejor este tema se exponen los componentes principales de un sistema de alarma contra intrusos.

1.2.1 Dispositivos de detección

Son equipos electrónicos diseñados para detectar cambios físicos provocados por un intruso en su área de cobertura. Estos cambios pueden ser energía infrarroja (IR), perturbación electromagnética, discontinuidad eléctrica, bloqueo de haz IR, impacto sísmico, desplazamiento, desbalance de presión entre otros.

Para detectar estos cambios, los sensores implementan diferentes tecnologías de acuerdo con el aspecto físico a determinar.

La selección de los dispositivos de detección impacta directamente en la calidad del sistema, por esta razón se debe analizar cuidadosamente el escenario en donde se instalaran y las fortalezas/debilidades que cada tecnología ofrece para la aplicación, esto permitirá desarrollar un sistema con mayor probabilidad de detección y menor incidencia de falsas alarmas [Gerard 2003, P.48].

Todo dispositivo de detección, sofisticado o no, cuando detecta un evento, este realiza el cierre/apertura de un contacto eléctrico, el cual es supervisado por un panel de control a través de un circuito de lazo cerrado [Robert 2007, P.54].

Existen dos escenarios que nos permiten clasificar los sensores de seguridad en: Sensores para exteriores e interiores.

Sensores para exteriores

Estos sensores se encargan de resguardar áreas externas al edificio, las cuales tienen fuentes potenciales de falsas alarmas (arboles, mascotas entre otros), por lo que se hace practico el uso de CCTV para el reconocimiento de las alarmas. Las principales tecnologías empleadas están en la tabla 1 [Robert 2007, P.97].

Tabla 1: Detectores de intruso para uso exterior.

Principio	Funcionamiento	Aplicación
Microondas	Generan un patrón de campo electromagnético que detecta al intruso cuando este lo perturba.	Patios, parqueos etc.
Rayo IR	Forman una barrera invisible de luz IR que cuando es bloqueada por un intruso, el sistema lo detecta y alarma.	Portones, pasillos, etc.
Fibra óptica	Utilizan un cable de fibra oculto, cuando alguien lo pisa, se dobla e interrumpe el paso de la señal y alarma.	Alta seguridad
Sísmico	Incorporan un sensor piezoeléctrico que se oculta en el suelo, bajo tensión mecánica este produce una corriente eléctrica, ejemplo: Cuando un intruso camine sobre él.	Alta seguridad

Sensores para interiores

Las áreas internas de un edificio son ambientes fáciles de controlar, en ellas se instalan sensores diseñados para interiores que deben detectar a un individuo antes de adentrarse o al ingresar a un área protegida [Robert 2007, P.103].

Existen tres categorías en las que podemos agrupar a los sensores para interiores, estas son:

Interruptor de protección

Es un dispositivo diseñado para resguardar puntos de acceso como puertas, ventanas, rejillas, persianas y portones entre otros. Existen varios tipos de interruptores de protección tales como: micro-interruptores, interruptores de mercurio y el más común, el contacto magnético [Gerard 2003, P.49].

El contacto magnético consiste en un par de láminas metálicas de material robusto dentro de un tubo de vidrio sellado herméticamente. Las láminas están ubicadas de manera que sus terminales (bañados en oro) quedan ligeramente superpuestos pero sin tocarse [Robert 2007, P.104].

Para accionar el contacto se ubica un imán cerca del interruptor, el cual atrae las láminas, lo que causa contacto físico entre ellas (cierre del contacto eléctrico). Cuando el imán se retira, la elasticidad de las láminas metálicas hace que regresen a su posición inicial (contacto abierto).

Por lo tanto un detector magnético se implementa en dos partes:

1. Un imán permanente de alta fiabilidad que se instala en la parte móvil de la puerta, ventana, entre otros.
2. El interruptor (conocido como reed relay) que dispone de dos terminales para la conexión con el panel de control, este se fija al marco de la puerta.

Mientras la puerta está cerrada el contacto permanece cerrado, y se abre cuando un intruso ingresa por la puerta y separa el imán del reed relay.

Los contactos magnéticos se encuentran disponibles en diferentes modelos, que incluyen variantes en dimensiones, materiales de construcción, mecanismo de accionamiento e intervalo de operación (máxima distancia permitida para que el imán accione el interruptor).

La figura 7 muestra el mecanismo de accionamiento de un contacto magnético y su versión comercial más común de simple contacto en encapsulado plástico.

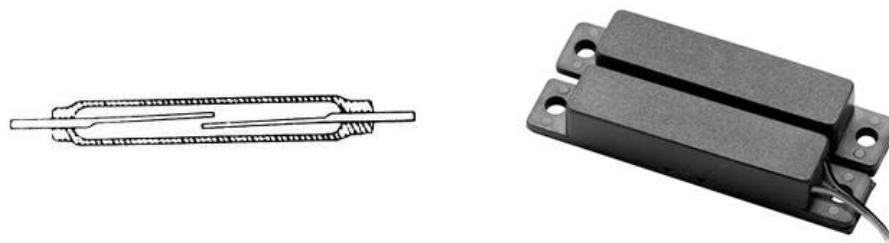


Figura 7. Contacto magnético.

Sensores de movimiento

La presencia de una persona que se mueve por un área definida provoca cambios físicos en el ambiente, estos son analizados por los sensores de movimiento para detectar intrusos en áreas internas a un edificio.

Para cumplir esta meta se emplean diferentes tecnologías, sin embargo en este documento el enfoque está dirigido al sensor PIR (Pasivo Infrarrojo), que es el más utilizado en la industria de seguridad.

Sensor de movimiento PIR

Todo cuerpo emite energía IR cuando irradia calor (temperaturas > cero absoluto) debido al movimiento de los electrones dentro de sus átomos.

El cuerpo humano produce calor, por lo tanto irradia energía IR en la parte alta del espectro de frecuencias con una longitud de onda de $10\mu\text{m}$. En una habitación a 24°C la temperatura de la piel de una persona es de 32.5°C aproximadamente, por lo tanto genera un patrón de radiación más intenso que los demás objetos de la habitación, lo que facilita su lectura con un detector PIR.

Un sensor PIR es un dispositivo pasivo que no genera energía IR, solo la absorbe, está diseñado para percibir cambios rápidos de radiación producidos por una persona que se mueve en su área de cobertura [Gerard 2003, P.70].

Los componentes de un sensor PIR son:

Lente de Freznel: Al igual que las cámaras con sus lentes enfocan objetos a larga distancia, los lentes de freznel crean ventanas ópticas que permiten enfocar hacia el elemento sensor la radiación IR de objetos que están dentro del área de detección y rechazan la radiación de objetos que están fuera.

El lente de freznel divide el área de detección en varias zonas que se extienden como los dedos desde la palma de la mano, el tamaño de las zonas y la sensibilidad del sensor son controlados por el lente, esto permite detectar objetos a larga o corta distancia [Robert 2007, P.105].

La altura, el ancho y la forma de la zona de detección dependen del elemento sensor, de la longitud focal y la distancia del punto de medición al detector.

Es importante ajustar el tamaño de la zona al del objetivo (una persona) para garantizar mayor sensibilidad a radiaciones producidas por un intruso que las ocasionadas por roedores, mascotas, entre otros). Ver ilustración en figura 8.

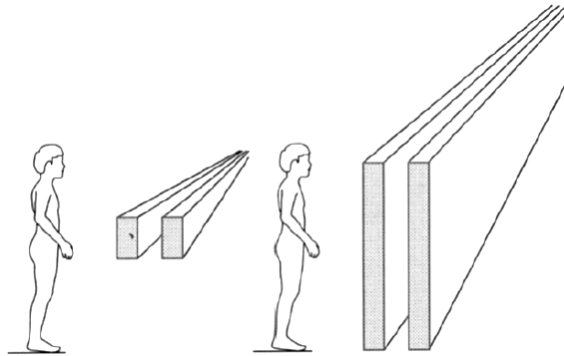


Figura 8. Tamaño de una zona de detección.

Elemento Sensor: El sensor PIR integra un elemento piroeléctrico que absorbe la energía IR irradiada por una persona y la transforma en calor. Cuando la cantidad de energía IR que recibe cambia, incrementa la temperatura en el elemento y produce electricidad.

El procesador de señales: La circuitería de procesamiento analiza las señales eléctricas que el elemento piroeléctrico produce cuando se calienta, para evaluar si fue producida por una persona y activar el circuito de alarma (un relevador).

Los sensores PIR también son diseñados para crear una pared de detección vertical, esta aplicación es conocida como detector de cortina, se utilizan para proteger ventanas. Algunos fabricantes permiten alternar entre detección por zonas o cortina con solo cambiar el lente de freznel del sensor.

Durante la instalación se deben considerar las siguientes recomendaciones:

1. La energía IR no penetra materiales como el vidrio, esto significa que un intruso se puede esconder detrás de estos objetos sin ser detectado.

2. Los PIR son más sensibles a movimientos a lo largo de las zonas, que los movimientos en dirección sensor.

Otros sensores de movimiento [Robert 2007, P.106]

Sensor de movimiento microondas: Tienen la capacidad de atravesar objetos, lo que les permite detectar intrusos detrás de paredes, mesas, entre otros. Su limitante son las falsas alarmas que generan cuando perciben a una persona en pasillos adjuntos al área de protección o el flujo de agua en una tubería de PVC.

Sensor de movimiento ultrasónico: Estos dispositivos emiten ondas ultrasónicas que cuando son reflejadas por un intruso en movimiento varían su frecuencia, el cambio es detectado por un receptor Ultrasónico. Este principio es mejor conocido como Efecto Doppler.

Existen también sensores de barrera fotoeléctricos, sensores de campo láser y mixtos que combinan dos tecnologías de detección para reducir la incidencia de falsas alarmas.

Sensores de ruptura de cristal [Robert 2007, P.108]

Acústicos: Todo vidrio al romperse produce un sonido distintivo de duración, amplitud y frecuencia determinada (4 – 6 KHz). Los sensores acústicos utilizan un filtro sintonizado para detectar estas frecuencias, al mismo tiempo miden la duración y amplitud del suceso para evaluar si fue producida por un cristal roto.

Impacto: Estos detectores se instalan directamente en la ventana y son sensibles a la sacudida que se produce en un vidrio cuando se quiebra. Generalmente utilizan un elemento piezoeléctrico muy sensible.

1.2.2 Panel de control de alarmas

El panel de control de alarmas integra un circuito electrónico capaz de monitorear el estado de los sensores, evaluar sus condiciones, identificar la zona de incidencia y notificar la información del suceso a través de los dispositivos de señalización del sistema.

Para realizar estas funciones, el panel de alarmas integra componentes que son similares a los de un panel de control de acceso, debido a que ambos sistemas comparten una arquitectura análoga a nivel de hardware. Sin embargo existen diferencias en la función de sus componentes cuando están en un panel de control de alarmas, tal como se muestra a continuación:

- El programa de control del MCU/MPU está diseñado para la gestión de alarmas de intrusos, esto cambia completamente su lógica de operación.
- El RTC provee información horaria para que se realice el armado o desarmado automático y se adjunte la hora/fecha al registro de alarma.
- La interfaz de entrada se utiliza para que el controlador lea de forma segura el estado de los sensores conectados a las diferentes zonas del panel.
- La interfaz de salida esta optimizada para energizar los dispositivos de señalización audio-visuales alámbricos e inalámbricos.
- La interfaz de comunicación envía la información de alarma y ubicación del intruso a los usuarios del sistema (centro de control de seguridad).

Circuitos de detección

Los circuitos de detección proporcionan un medio cableado para que las señales de alarma lleguen hasta el panel de control, el más utilizado por los sistemas contra intruso es el circuito de lazo cerrado, también conocido como zona.

Para comprender que es una zona, considere un conjunto de detectores de movimiento que protegen una recepción, estos se agrupan en un solo circuito de lazo cerrado que resguarda esta zona geográfica, si los sensores de las demás áreas se asocian del mismo modo, entonces será más fácil para el panel determinar la ubicación de un evento [Robert 2007, P.55].

La sectorización por zonas reduce considerablemente la cantidad de cables de interconexión entre los sensores y el panel, sin embargo, solo se recomienda agrupar equipos de un tipo que pertenecen a la misma zona geográfica.

Las zonas son vulnerables a alteraciones, por ejemplo, si se cortocircuitan los cables de un lazo de detección se puede impedir que el panel de control lea el estado real de los sensores, en este caso un intruso podría ingresar sin ser detectado [Robert 2007, P.56 - 57].

En la práctica para evitar esta situación se instala una resistencia de fin de línea después del último sensor de un lazo, tal como lo muestra la figura 9. De esta manera en condiciones normales siempre fluirá una corriente conocida a través del lazo, la cual es monitoreada por el panel de control, si alguien cortocircuita una zona del panel este detectara un incremento en la corriente de lazo y enviara una señal indicando que hay problemas en esa zona, mientras que si un sensor de la zona detecta un intruso (contacto abierto), se interrumpe el paso de la corriente eléctrica, el panel de control percibe la ausencia de corriente de lazo y notifica una alarma indicando la zona de incidencia.

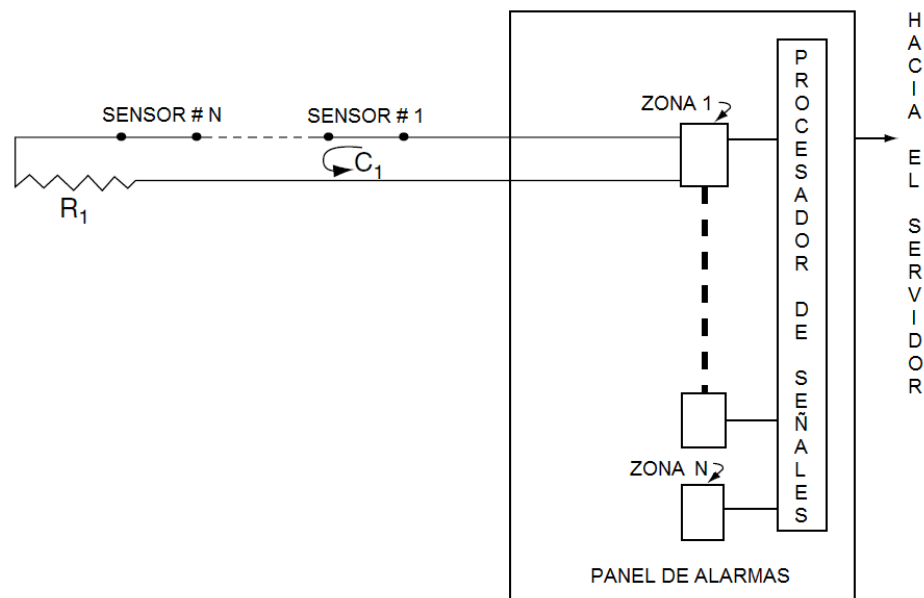


Figura 9. Resistor de fin de línea.

1.2.3 Sistemas de señalización

Los sistemas de señalización son medios electrónicos para alarmar e informar a los usuarios de un sistema de seguridad, estos se activan cuando el panel de control determina que un evento necesita evaluación y respuesta física.

Existen tres tipos de señalización empleados para realizar esta función:

Dispositivos de señalización Audible [Gerard 2003, P.164 - 167]

Son instrumentos electrónicos que producen sonidos penetrantes para anunciar un estado de alarma, su principal aplicación se encuentra en alarmas locales de residencias y edificios con vigilancia que ejecutan una respuesta inmediata.

Estos dispositivos emiten sonidos a un nivel superior a 70dB con tonos de frecuencia que crean pánico en el intruso, lo que los conduce a huir para no ser descubiertos o capturados.

Los dispositivos de señalización audible más utilizados son:

Bocina electrónica de estado sólido: Está formada por un parlante tipo bocina, un amplificador y un oscilador electrónico sintonizado a 0.8 – 1 kHz, son dispositivos altamente directivos que operan en este rango de frecuencia para reducir efectos de atenuación de sonido por la distancia.

Las bocinas electrónicas son excelentes para ambientes exteriores por su bajo consumo (400mA, 12V_{DC}), alto nivel de sonido (120dB) y bajos costos.

Sirena Piezoeléctrica: Su elemento principal es un transductor piezoeléctrico de cerámica que genera un tono alto audible cuando es energizado por una señal eléctrica cuadrada. La señal proviene de un circuito integrado de bajo consumo que opera como multivibrador biestable.

Las sirenas piezoeléctricas son utilizadas con mayor frecuencia en ambientes interiores por su corto alcance, esto se debe a la alta frecuencia de su tono el cual se ve afectado por el fenómeno de atenuación.

Parlante de cono Mylar: Están compuestos por un parlante tipo cono hecho de mylar (lamina transparente resistente a la humedad) y un imán de ferrita montado sobre un chasis redondo/cuadrado protegidos para cualquier ambiente.

Son utilizados en aplicaciones exteriores por su capacidad de transmitir múltiples tonos de baja frecuencia a largas distancias.

Dispositivos de señalización visual

Los dispositivos señalización visual se utilizan en conjunto con equipos de señalización audible para establecer con mayor determinación una fuente de alarma. Las luces de xenón intermitentes son una de las tecnologías más populares del mercado, estas se pueden encontrar por separado o integradas en señales audibles [Gerard 2003, P.170].

La fuente de luz de estos dispositivos es un tubo de vidrio con gas xenón que emite un destello brillante cuando es excitado por un alto voltaje, la intensidad de brillo depende de la cantidad de energía eléctrica que se descargue sobre el gas, típicamente su valor es de 5 Joule.

La frecuencia de intermitencia típica de una luz de xenón es de 3 Hz, para controlar los tiempos de encendido y generar el voltaje de descarga se utiliza un circuito electrónico integrado en la unidad.

La selección de una señal visual depende del grado de protección, consumo de energía y capacidad lumínica, siendo este último parámetro el más importante. Para mejorar la luminosidad, la cubierta de un indicador visual se fabrica utilizando un material acrílico translucido con una serie anillos de freznel dispuestos para maximizar la dispersión de luz hacia la fuente receptora.

Dispositivos de señalización remota

En ocasiones los sistemas de seguridad deben informar a un usuario distante sobre las condiciones en que se encuentra el sistema, para realizar este trabajo se utilizan diversos medios de comunicación alámbricos e inalámbricos.

Comunicaciones alámbricas

Las líneas telefónicas son el medio mas empleado por los sistemas de seguridad, su función es llevar la información de alarmas y el estado del sistema desde los paneles de control hasta el CCS (Centro de Control de Seguridad).

En el CCS se conectan todas las líneas a un equipo multiplexor que transforma las entradas en una línea troncal, esta salida se conecta a los equipos de monitoreo para que los operadores puedan recibir, evaluar las alarmas y contactar al personal requerido para dar respuesta rápida [Gerard 2003, P.176].

Comunicaciones inalámbricas

Las comunicaciones inalámbricas ofrecen muchos beneficios para los sistemas de seguridad, dentro de los cuales se incluyen [Robert 2007, P.133]:

- Instalaciones rápidas con menores costos de cableado.
- Acceso a ubicaciones remotas y aisladas.
- Respaldo y retransmisión de datos.

Durante varios años los enlaces inalámbricos han soportado las transmisiones entre sistemas aislados y el CCS, mientras que los sistemas SMS (Short Message Service) y marcadores automáticos GSM (Global System for Mobile Communications) se encargan de contactar directamente a los usuarios a través de su celular para informarles (por mensaje de texto o llamada pregrabada) sobre el estado del sistema.

La tecnología inalámbrica también ha desarrollado equipos de señalización inalámbricos, estos se instalan en lugares difíciles de acceder por medios cableados, entre ellos se destacan las sirenas y luces estroboscópicas inalámbricas que se utilizan en sistemas de señalización local.

Estos dispositivos utilizan transmisores y receptores de radio frecuencia para enviar la señal de alarma desde el panel hasta un punto remoto (dentro o fuera del edificio) en donde no es técnicamente viable instalar un indicador cableado.

Funcionamiento de un sistema de alarma contra intruso

La función de un sistema de alarma contra intruso es recolectar la información que detectan los sensores para enviar la ubicación y alarma de un intruso al centro de control de seguridad o usuarios del sistema [Robert 2007, P.54 - 58].

Los sensores de un área protegida se conectan en serie en un mismo lazo utilizando su contacto NC y una resistencia de fin de línea. El panel de control está diseñado para monitorear un número determinado de zonas o lazos a los que se asigna una dirección electrónica para facilitar su ubicación.

En condiciones normales el panel de control hace circular una corriente a través del lazo, cuya magnitud está determinada por la resistencia de fin de línea. Cuando un sensor detecta un intruso, este abre su contacto e interrumpe el paso de la corriente, inmediatamente el controlador percibe el cambio y determina en que zona se produjo el evento.

El panel de campo envía la dirección de la zona (en números) al servidor, en donde existe una base de datos capaz de interpretar la ubicación y el tipo de alarma del sensor. Por ejemplo el personal de seguridad no visualizará el número de la zona que se activó, en cambio recibirá un mensaje: "Movimiento en Laboratorio".

Los sistemas de alarma pueden ser configurados para realizar funciones como: guardar un registro de alarmas, generar alarmas locales o remotas (audibles, lumínicas o silenciosas), armar/desarmar el sistema automáticamente, realizar pruebas de fallos periódicamente, entre otras.

En el mercado nicaragüense son comunes los sistemas de alarma autónomos, que tienen capacidad de monitorear 8 - 32 zonas y están conectados a la red de monitoreo de las empresas de seguridad privada, estas evalúan y dan una respuesta física ante cualquier intento de robo.

1.3 SISTEMAS DE ALARMA CONTRA INCENDIO

Un sistema de alarma contra incendio funciona de manera similar a un sistema de alarma contra intruso. Ambos son análogos en su arquitectura, paneles de control, lazos de medición y dispositivos de señalización, por esta razón es común encontrar sistemas mixtos capaces de monitorear, evaluar y notificar alarmas de fuego e intruso al mismo tiempo [Robert 2007, P.73].

Sus detectores se encargan de determinar indicios de incendio en diferentes áreas antes de que se propague por todo el edificio, dentro de los sensores más comunes tenemos: detectores de humo, calor, llama, gases, entre otros.

1.3.1 Detector de humo

El sensor de humo fotoeléctrico utiliza un diodo LED (emisor) que irradia luz en una cámara oscura, tal y como lo muestra la figura 10.

Cuando las partículas de combustión entran en la cámara estas reflejan la luz hacia un diodo fotosensible (receptor), a medida que incrementa la reflexión, más corriente fluirá por el receptor provocando una alarma [Robert 2007, P.81].

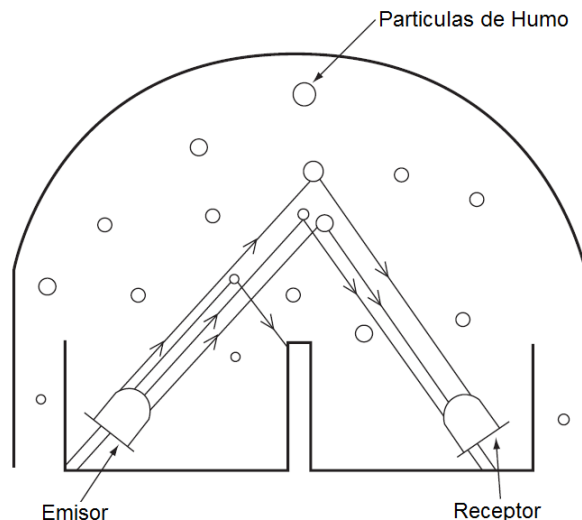


Figura 10. Detector de humo fotoeléctrico.

CAPITULO 2: PLATAFORMA DE DESARROLLO SMARTGLCD 240x128

2 SMARTGLCD 240x128 BOARD

El **SmartGlcd240x128** es un sistema para experimentar con aplicaciones gráficas, panel sensible al tacto, registros y transferencia de datos, esta se puede utilizar como una plataforma de desarrollo o un dispositivo de control final. La figura 11 muestra el aspecto físico del SmartGLCD [SmartGLCD 2011, P.4].

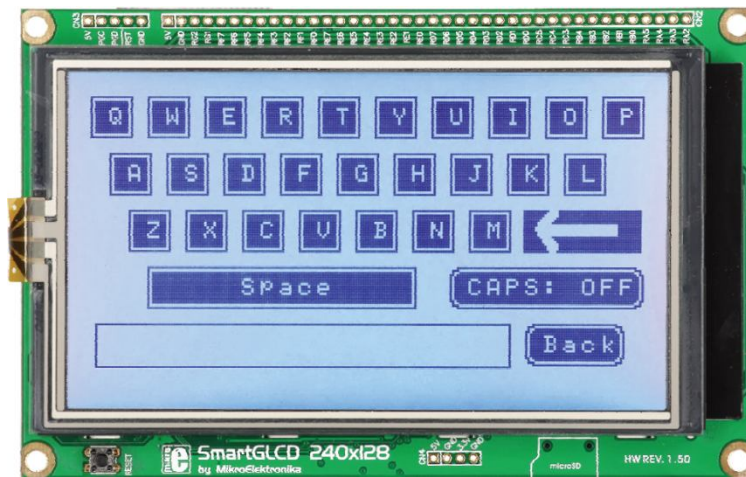


Figura 11. SmartGLCD 240x128 Board.

Este sistema esta integrado por los siguientes componentes:

- Pantalla táctil.
- Microcontrolador PIC18F8722.
- Modulo USB-UART.
- Lector de tarjeta microSD (Micro Secure Digital Card).

2.1 Pantalla Táctil

Una pantalla grafica cubierta por un panel táctil crea una sola unidad funcional llamada pantalla táctil, la cual permite ingresar y mostrar datos al mismo tiempo. Esta característica facilita la interacción con el usuario debido a que es más rápido presionar botones de función dibujados en pantalla en vez de utilizar un mouse o teclado para navegar por una aplicación [SmartGLCD 2011, P.18]. A continuación se explican los componentes principales de una pantalla táctil.

Pantalla Grafica “GLCD 240x128”

Un GLCD es una matriz de pixeles de cristal líquido que puede ser controlada eléctricamente para imprimir caracteres del código ASCII e imágenes en forma de mapa de bit. Su funcionamiento se explica detalladamente en el anexo A.1.

El **SmartGLCD** integra una pantalla grafica monocromática de 240x128 pixeles con nueve colores de retroiluminación LED (Diodo Emisor de Luz), controlador de pantalla integrado y un potenciómetro para ajuste de contraste.

Controlador de GLCD RA6963

Un controlador de pantalla grafica sirve como interfaz entre un MCU y la matriz de puntos de cristal líquido, su función es recibir los datos y comandos que le envía el MCU, traducirlos a caracteres, gráficos y funciones para dibujarlos en la pantalla [RA6963 Specification 2008, P.5].

El **SmartGLCD** integra un controlador **RA6963** el cual viene interconectado al PIC18F8722, para desarrollar una aplicación grafica en este sistema se debe definir y direccionar cada pin del PIC (Peripheral Interface Controller) así como se ilustra en la figura 12. Detalles del controlador RA6963 pueden ser vistos en el anexo A.2.

Panel táctil resistivo

Un panel táctil resistivo es un fino panel autoadhesivo muy sensible a la presión que se coloca sobre una pantalla gráfica de manera que un suave toque al panel provoca un cambio en la señal de salida [Dusan, P.1].

Este dispositivo utiliza dos láminas resistivas configuradas para entregar un voltaje proporcional a la posición en la que se presionó el panel, para determinar las coordenadas del punto bajo presión, se debe procesar el voltaje de salida de la lámina resistiva. El anexo A.3 explica cómo funciona un panel táctil y como se debe conectar para realizar su lectura.

2.2 Microcontrolador PIC18F8722

Un microcontrolador es un circuito integrado programable que contiene todos los componentes necesarios para controlar una tarea determinada, tal como un sistema de alarma, control de acceso, entre otros. También es conocido como **controlador incrustado** porque generalmente están integrados en el dispositivo que controlan, un ejemplo claro es el PIC18F8722 integrado en el SmartGLCD [Enrique 2004, P.1].

El PIC18F8722 (ver figura 13) pertenece a la familia **PIC18** de Microchip, la cual es una serie de MCU de 8 bits con capacidad de procesamiento de hasta 16 MIPS (Mega Instrucciones Por Segundo), integra periféricos avanzados (MSSP, EUSART, ADC, ECCP), soporta protocolos de comunicación complejos (TCP/IP, CAN, USB o ZigBee) y tiene un multiplicador hardware 8x8 integrado, lo que los hace ideales para aplicaciones de complejidad media [SmartGLCD 2011, P.9].

Las principales características del PIC18F8722 son:

- Memoria de programa: 128KByte
- Memoria de datos: 3936 Bytes
- Memoria EEPROM: 1Kbyte
- Velocidad de CPU: 10 MIPS
- Entradas y Salidas: 70 E/S
- Canales Analógicos: 16 CH de 10 bits (1024) de resolución.
- Comunicaciones: Serial (MSSP y EUSART), Com. Paralelo.
- Otros periféricos: CCP, temporizador, interrupciones, entre otros.

En el anexo A.5 se definen los conceptos necesarios para comprender las características del PIC18F8722.

La memoria de programa, memoria de datos y EEPROM (Electrically Erasable Programmable Read Only Memory) del PIC18F8722 le permiten almacenar suficientes rutinas de control, imágenes, datos variables, y datos constantes para desarrollar cualquier sistema de control de propósito general.

El SmartGLCD utiliza la capacidad de almacenamiento de este MCU en conjunto con sus puertos E/S, periféricos y módulos de comunicación para crear una plataforma de desarrollo capaz de monitorear variables análogas o digitales, procesarlas, almacenar datos en su memoria interna o en una microSD, realizar acciones de control, comunicarse con otros sistemas o periféricos e implementar una interfaz táctil para interactuar con sus usuarios.

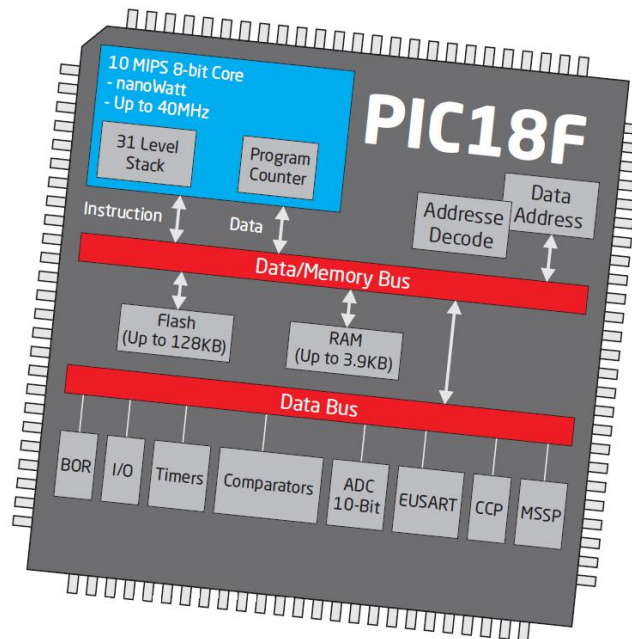


Figura 13. Diagrama en bloques del PIC18F722.

Programación del PIC18F722

Los PIC18F pueden escribir en su propia memoria de programa bajo control interno de software. Los fabricantes del SmartGLCD utilizaron esta característica para desarrollar una rutina de control que viene preinstalada en el sector de arranque de la memoria del PIC, esta rutina controla la auto programación del Microcontrolador a través del puerto USART.

Para transferir el archivo **.hex** (programa de control en código hexadecimal) desde una PC al PIC se utiliza el software **Mikrobootloader**, el cual en coordinación con el programa preinstalado en el bootloader del MCU controlan la transferencia de datos utilizando protocolo USB [SmartGLCD 2011, P.10].

2.3 Modulo USB – UART

Un modulo USB – UART sirve como interfaz entre dispositivos USB) y controladores electrónicos que soportan comunicación UART, su función es habilitar a los MCU (sin puerto USB) para que puedan interactuar con terminales USB utilizando comunicación serial asíncrona (UART) [SmartGLCD 2011, P.22].

El SmartGLCD integra un modulo USB – UART que esta compuesto principalmente por el chip **FT232RL** en conjunto con capacitores, resistores y un mini conector USB tipo B tal y como se muestra en la figura 14. Este modulo habilita la comunicación USB en el PIC18F8722 utilizando su puerto UART, de esta manera se pueden desarrollar aplicaciones para el MCU que permitan leer/escribir datos y comandos entre un dispositivo USB y el PIC.

El circuito integrado FT232RL es sin duda el componente que integra toda la tecnología requerida para convertir la comunicación UART en USB y viceversa, las características principales de este dispositivo son:

- Proporciona una interfaz de transferencia de datos entre dispositivos USB y seriales asíncronos.
- Ejecuta una completa manipulación del protocolo USB (no requiere programación de un firmware específico).
- Alcanza velocidades de transferencia desde 300 Baud hasta 1 Megabaud.
- Trae preprogramado Numero serial USB único “FTDIChip-ID” para garantizar seguridad en las aplicaciones desarrolladas.
- Integra 1024 Bits de memoria EEPROM para almacenar datos de la comunicación USB (etiquetas, configuración de E/S, N_o. serie, entre otros).
- Incluye Convertidor de nivel de voltaje de 3.3V en los pines de E/S USB.
- Integra resistores del Bus USB y señal de reloj (no requiere cristal externo) que le permiten (opcional) realizar transferencias síncronas.
- Soporta transferencias USB por volúmenes.
- Soporta dispositivos USB 1.1 y 2.0 de alta velocidad.
- Los drivers para Windows, Linux y MAC OS se pueden descargar gratis.

2.4 Lector de tarjeta microSD

Los microcontroladores pueden manipular memorias SD a través de dos protocolos: protocolo SPI y protocolo SD. SPI se utiliza con mayor frecuencia por ser libre y bien documentado, mientras que el protocolo SD es de uso exclusivo para los miembros de la SD Card Association. [Dogan 2008, P.371].

Para leer o escribir en una memoria SD se requiere trabajar con segmentos de datos de 512 Bytes, por esta razón se necesitan MCUs con suficiente memoria RAM y al menos un puerto SPI integrado tal como los PIC18F de microchip.

El SmartGLCD incorpora un lector de memoria microSD que se encuentra interconectado al puerto SPI del PIC18F8722 así como se ilustra en la figura 15. Con la ayuda de algunas librerías para gestión de datos para memorias SD se pueden realizar aplicaciones tales como: registradores de temperatura, humedad, presión, nivel o registros de eventos de acceso/alarmas, entre otros.

El voltaje de alimentación de una microSD es de $2.7 - 3.6V_{DC}$, para acoplarla con el PIC ($V_{CC} = 5V_{DC}$) se requiere de un circuito divisor de voltaje entre las líneas de control y un regulador de $5V_{DC}$ a $3.3V_{DC}$ para alimentar la memoria.

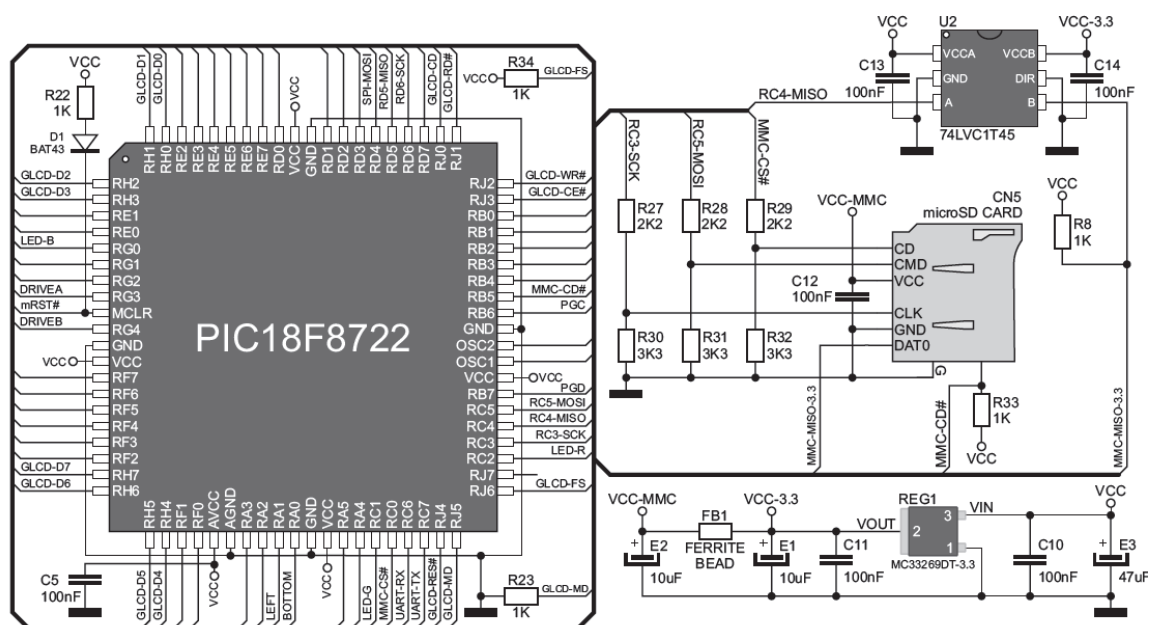


Figura 15. Diagrama de conexión del lector de tarjeta microSD integrado.

CAPITULO 3: ANALISIS Y PRESENTACION DE RESULTADOS

En este capítulo se presentan los aspectos relacionados con el diseño e implementación del sistema de alarma y control de acceso que se instaló en el departamento de electrónica, además se describe la metodología, pruebas y resultados obtenidos de la implementación del proyecto.

3 METODOLOGIA ADOPTADA

Se utilizó el **método científico** aplicado a actividades de Investigación y Desarrollo como referencia sistemática, este comprende las siguientes etapas:

3.1 ANALISIS

En esta etapa se realiza una breve descripción de la problemática que llevó a los autores a indagar sobre seguridad electrónica para proponer una solución que mejorará las condiciones de seguridad del departamento.

3.1.1 Condiciones de seguridad del departamento de electrónica

El departamento de electrónica de la FEC tiene trece puestos de trabajo que son compartidos por los docentes del departamento, cada puesto es un mueble tallado en madera que dispone de amplios depósitos, tomas de corriente, y una computadora de escritorio con conexión a internet (ver figura 16). Algunos docentes del departamento llevan sus laptops, libros y otras pertenencias, que sumados a los artículos del local forman un conjunto de bienes de valor.

Previo a la instalación del sistema se utilizaba la siguiente política de seguridad:

- Cada docente debe cargar con sus pertenencias de valor.
- El último usuario que sale debe dejar la puerta bajo llave.

Sin embargo a lo largo de los años se han registrado una serie perdidas de artículos, de los cuales no se pudo determinar un culpable. Por esta razón los autores de este trabajo monográfico consideraron que se debía de mejorar las condiciones de seguridad del local para que los docentes puedan salir a impartir sus clases con tranquilidad y sin tener que cargar sus pertenencias.



Figura 16. Planta arquitectónica del departamento de electrónica.

3.1.2 Requerimientos del sistema de seguridad

Para obtener un sistema de seguridad electrónica de calidad es importante determinar los requerimientos propios de las instalaciones, estos generalmente dependen de la infraestructura, ubicación y cultura de sus usuarios. Para el departamento de electrónica los requerimientos que se deben cumplir son:

- Controlar el acceso al departamento instalando un punto de control donde los docentes autorizados deben autenticarse.
- Determinar la presencia de intrusos que traten de ingresar al departamento cuando el sistema este armado.
- Determinar indicios de incendios que puedan producirse en el departamento.
- Generar alarmas locales para avisar a sus usuarios cuando se presenta un evento que viole la política de seguridad.
- Generar alarmas remotas en la caseta del personal de seguridad de la UNI para solicitar una respuesta física cuando un evento lo requiera.
- Registrar los eventos de acceso y alarma que se producen en el sistema con capacidad de visualizarlos y transferirlos a un PC.
- Mantener bajos costos de adquisición, mantenimiento y administración.

3.2 DISEÑO DEL UN SISTEMA DE SEGURIDAD ELECTRONICA

3.2.1 Consideraciones de diseño

Basándose en los requerimientos establecidos por el departamento de electrónica, los autores, en consenso con el tutor de este proyecto proponen que el sistema debe cumplir con los siguientes parámetros de desempeño:

- Utilizar claves de acceso como mecanismo de autenticación.
- Implementar dos tipos de cuenta: una de administrador y varias de usuario.
- La cuenta de administrador debe tener privilegios para activar/desactivar las alarmas, configurar la hora y fecha, crear, modificar y eliminar cuentas de usuario, cambiar su contraseña e ingresar al local.
- Las cuentas de usuario serán asignadas a los docentes, estas únicamente permiten ingresar al local y cambiar la clave de acceso.
- El tiempo de ingreso al local será preciso y agilizado por un zumbador.
- Los detectores de intrusos e incendio deben proteger al departamento sin que puedan ser perturbados o deshabilitados externamente.
- En presencia de un incendio se debe de liberar automáticamente la puerta de entrada y alarmar a todos los usuarios del sistema.
- La transmisión de alarmas remota se debe proteger con filtros y algoritmos de cifrado para evitar falsas señales de alarma en el receptor.
- El sistema debe ser capaz de armarse y desarmarse automáticamente siguiendo una programación de los días y horas laborales de los docentes.
- El sistema debe autoprotegerse ante cualquier intento por dañar, quitar, engañar o desenergizar sus componentes.
- Se debe crear un registro diario de los eventos de alarma y acceso, los archivos de registro se guardaran en una memoria extraíble y serán compatibles con Microsoft Excel.
- La alimentación eléctrica de los equipos debe constar con un sistema de respaldo ininterrumpido para suplir por al menos cuatro horas cuando falle el suministro eléctrico comercial.

3.2.2 Descripción general del sistema

El sistema de seguridad electrónica propuesto por los autores está compuesto por tres subsistemas: “**Subsistema de Control de Acceso**”, “**Subsistema de Alarmas**” y “**Subsistema de Señalización Remota**”. Estos operan en conjunto para formar un “**Sistema de Control de Acceso y Alarmas Contra Intruso**”.

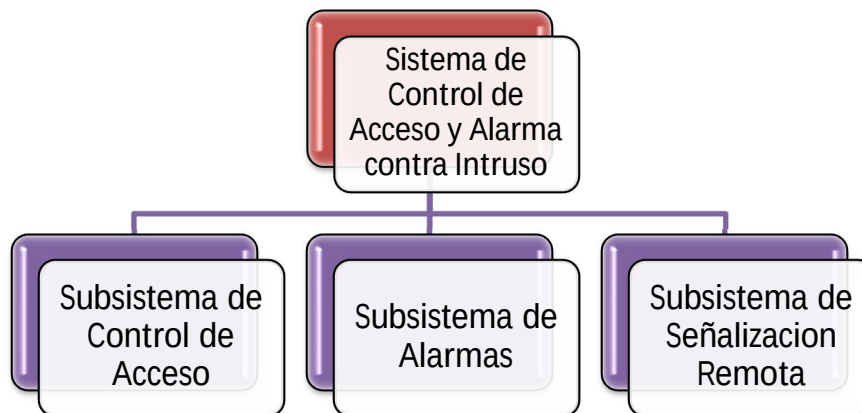


Figura 17. Diagrama en Bloques del Sistema de Seguridad Electrónica.

Cada subsistema a su vez cuenta con derivaciones más pequeñas dedicadas a realizar tareas específicas que son necesarias para la funcionalidad del sistema completo, a continuación se describe en términos generales su funcionamiento.

El subsistema de control de acceso proporciona una interfaz táctil que permite realizar el proceso de autenticación, si este resulta satisfactorio el controlador libera la puerta de acceso, controla el tiempo de entrada y guarda un registro del evento, si el acceso no es permitido la puerta permanecerá cerrada.

El subsistema de alarmas se encarga de monitorear los detectores de intruso e incendio instalados en el local, cuando el sistema está armado y se presenta una condición de alarma, el controlador determina su origen, registra el evento y activa los dispositivos de señalización para notificar a los usuarios del sistema.

El subsistema de señalización remota se encarga de transferir un estado de alarma a través de módulos de RF para poder habilitar una alarma remota ubicada en la caseta del personal de seguridad de la UNI.

3.2.2.1 Subsistema de Control de Acceso

Los autores implementaron un punto de control de acceso junto a la puerta de entrada del departamento, su función es permitir el ingreso a los docentes que están registrados en su base de datos y denegarlo a personas no autorizadas, además de llevar un registro de los eventos de acceso.

Este sistema es un control de acceso autónomo y está integrado por los componentes:

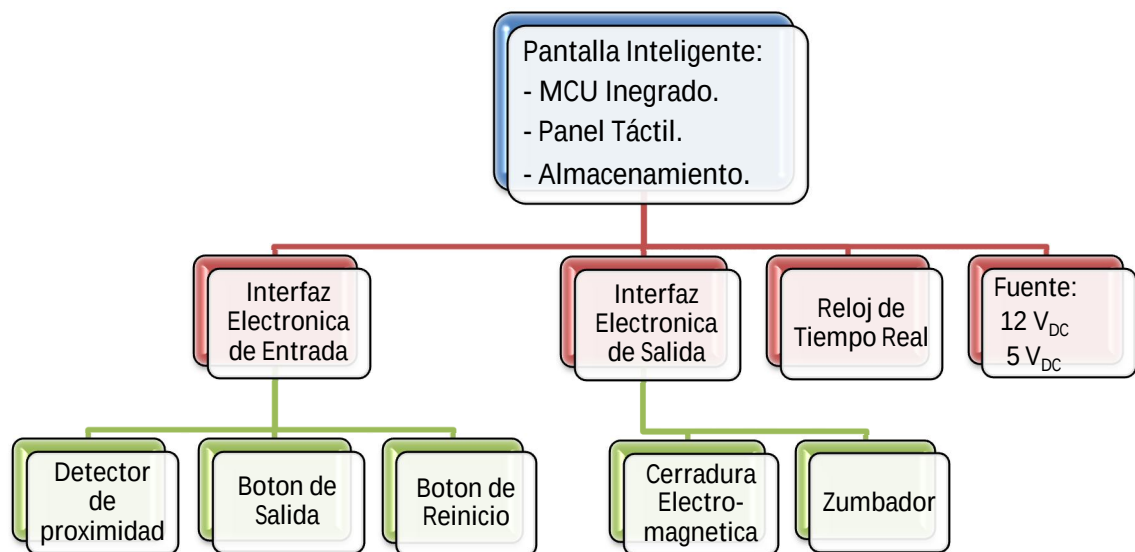


Figura 18. Diagrama en Bloques del Subsistema de Control de Acceso.

3.2.2.1.1 Selección de los principales componentes de Control de Acceso.

Pantalla Inteligente

Basados en los requerimientos del departamento y las consideraciones de diseño establecidas, los autores en consenso con el tutor optaron por utilizar una pantalla inteligente como dispositivo de control principal para todo el sistema.

Una pantalla inteligente nos permite desarrollar aplicaciones programables para interactuar con el usuario, controlar un proceso interno o externo, almacenar, procesar y transferir información, entre otras aplicaciones, todo de forma integrada en un solo sistema de control.

Debido a que existen múltiples modelos de pantallas inteligentes con diferentes características, se realizó una investigación para preseleccionar los modelos que mejor se ajustan a los requerimientos y consideraciones de diseño del proyecto.

La tabla 2 muestra tres modelos de los cuales se seleccionara el más apropiado.

Tabla 2: Principales características de las Pantallas Inteligentes propuestas.

Modelo	SmartGLCD240x128	GLT240128-422-FGW	EA EDIP240J-7LWTP
Tipo de fluido	STN	FSTN	FSTN positivo.
Resolución	240x128 pixeles	240x128 pixeles	240x128 pixeles
Retroiluminación	9 colores, RBG	Luz blanca	Luz blanca
Panel Táctil	Resistivo	Resistivo	Resistivo
MCU	PIC18F8722	Externo vía RS422	EAeDIP240-7
E/S Externas	38 A/D	-	7 Salidas
Programación	Auto	Comandos RS422	RS232, RS422
Comunicación	USB, UART, SPI, I ² C	RS422	SPI, I ² C, RS-232
Almacenamiento	MicroSD	-	EEPROM 32 KB
Alimentación	5 V _{DC}	5 V _{DC}	5 V _{DC}
Costo	\$ 120	\$ 268	\$ 255

Se seleccionó la pantalla SmartGLCD240x128 de **Mikroelectronica** por las siguientes razones:

- Su resolución y tamaño es adecuado para desarrollar una interfaz de usuario ergonómica, que permita leer/escribir datos con facilidad.
- Es capaz de generar nueve colores retroiluminación LED (RBG) configurables a nivel de software, esto permite crear rutinas que cambian el color de la pantalla para expresar el estado del sistema (Ej. Alarmas).
- Su controlador “PIC18F8722” tiene suficiente capacidad para desarrollar aplicaciones de complejidad intermedia, además es capaz de auto programarse, eliminando la necesidad de adquirir un quemador de PIC.
- Tiene mayor cantidad de E/S digitales y entradas analógicas para poder monitorear y controlar procesos externos o internos (Ej. lectura y escritura de pantalla táctil, lectura de MicroSD, monitoreo de alarmas, activación de cerraduras, entre otras).

- Soporta varios protocolos de comunicación que le permiten interactuar con sistemas tales como PCs, RTC, Memorias, Sensores, entre otros.
- Por su capacidad de leer y almacenar datos en una MicroSD se vuelve apropiada para implementar registros de eventos de acceso y alarma.
- Es un sistema de bajo coste que cuenta con el respaldo técnico de una empresa líder en el diseño de hardware y software de MCU's.

Una explicación más detallada del SmartGLCD240x128 y los subsistemas que la integran se puede encontrar en el capítulo II de este documento.

Cerradura electromagnética

Este componente se eligió considerando que el departamento está ubicado en el interior de un edificio de tres pisos (Edificio de la FEC) y para este tipo de aplicaciones se recomienda utilizar un mecanismo de bloqueo que deje la puerta libre cuando falle el sistema de alimentación eléctrica o se averíe el sistema de control de acceso, para permitir la evacuación de los usuarios.

Para esta aplicación se eligió el modelo: ECL-ACC300 de cerradura electromagnética que cumple con los requerimientos establecidos. Las características técnicas de esta cerradura muestran en la siguiente tabla:

Tabla 3: Características técnicas de la cerradura seleccionada.

Modelo	ECL-ACC300
Descripción	Cerradura Electromagnética.
Principio	Electroimán
Presión	600 Lb
Indicador	LED (Cerrado > Verde) (Abierta > Rojo)
Sensor	Detector de proximidad inductivo
Protección	Contra sobretensión (MOV)
Alimentación	"12 V _{DC} , 500 mA" o "24 V _{DC} , 250 mA"
Costo	\$ 90

Esta cerradura electromagnética se eligió de forma explícita debido a las siguientes razones:

- Su fuerza de atracción de 600 Libras permite mantener la puerta cerrada de forma segura, aun ante cualquier intento humano de abrirla forzada.
- Integra un sensor de proximidad que en conjunto con un LED proporcionan señalización eléctrica y visual sobre la posición de la puerta.
- Su capacidad de liberar la puerta ante fallos de energía eléctrica o detección de incendios le hacen adecuada para ambientes interiores.
- Está disponible en un diseño elegante de aluminio ionizado a un costo intermedio.



Figura 19. Cerradura electromagnética ECL-ACC300.

Reloj de Tiempo Real

El RTC es un dispositivo que establece la base de tiempo bajo la cual opera el sistema de seguridad, su tarea principal es proporcionar al MCU la información de hora y fecha en formato digital para que este pueda realizar las siguientes funciones:

- Mostrar la hora y fecha en pantalla.
- Armar y desarmar el sistema automáticamente.
- Establecer días feriados y años bisiestos.
- Adjuntar hora y fecha al registro de eventos.

La tabla 4 contiene las principales características de tres modelos de RTC que fueron preseleccionados para su implementación en el sistema de seguridad.

Tabla 4: Principales características de los RTC propuestos.

Característica	DS1307	PC8583	MCP7940M
Interfaz	Serie I ² C	Serie I ² C	Serie I ² C
Formato Tiempo	HH:MM:SS	HH:MM:SS	HH:MM:SS
Formato Fecha	YY:MM:DD	DW:DM:M:Y	DW:DM:M:Y
Memoria	56 Byte	240 Byte	64 Byte
Salida	Drenador abierto	Drenador abierto	Drenador abierto
Alimentación	5 V _{DC}	5 V _{DC}	5 V _{DC}
Respaldo	Batería 3 V _{DC}	No	No
Costo	\$ 5.04	\$ 3.6	\$ 0.96

Se decidió utilizar el **DS1307** de **MAXIM** por las siguientes razones:

- Su interfaz de comunicación (I²C) es soportada por el PIC18F8722.
- Opera en formato de 12/24 horas con indicador de am/pm.
- Su salida es capaz controlar un LED para indicar marcación de segundos.
- Integra circuitería de conmutación para operar desde la alimentación principal o desde una batería de respaldo.
- Existen librerías para lectura/escritura del DS1307 utilizando compiladores de PIC desarrolladas por Mikroelectrónica.



Figura 20. Reloj de Tiempo Real DS1307.

3.2.2.2 Subsistema de Alarmas

Para cumplir con la tarea de detección de intrusos e incendios los autores diseñaron un sistema de alarmas que fue implementado utilizando como dispositivo de monitoreo y control el mismo PIC18F8722 que esta integrado en el SmartGLCD. Este microcontrolador tiene suficiente capacidad para controlar ambos procesos a la vez, optimizando de esta manera los recursos de hardware y software utilizados para la implementación del sistema.

Los subsistemas de **control de acceso y de alarmas** también comparten otros medios de hardware, dentro de los cuales se encuentran:

- El Reloj de Tiempo Real.
- La Interfaz de Entrada.
- La Interfaz de Salida.
- La Fuente de Alimentación.

Al compartir estos recursos e implementar un panel de control mixto se logro ahorrar tiempo de desarrollo y ejecución, espacio en el gabinete eléctrico y sobre todo se redujeron considerablemente los costos del sistema.

Por lo tanto en esta sección no se realizara la selección de componentes de control y acondicionamiento compartidos, solo se elegirán aquellos dispositivos utilizados para la gestión de intrusos e indicios de incendios.

La figura 21 muestra los componentes del subsistema de alarmas, donde se aprecia que los componentes de control y acondicionamiento ya fueron elegidos.

Sin embargo los sensores seleccionados para realizar la tarea de detección fueron elegidos tomando en cuenta la arquitectura del departamento, sus ambientes adjuntos, iluminación natural, ventilación artificial y la distribución de los puestos de trabajos de los docentes. Considerando todos los aspectos antes descritos se puede garantizar que el proceso de detección ha sido optimizado para un ambiente como el establecido por el departamento de electrónica.

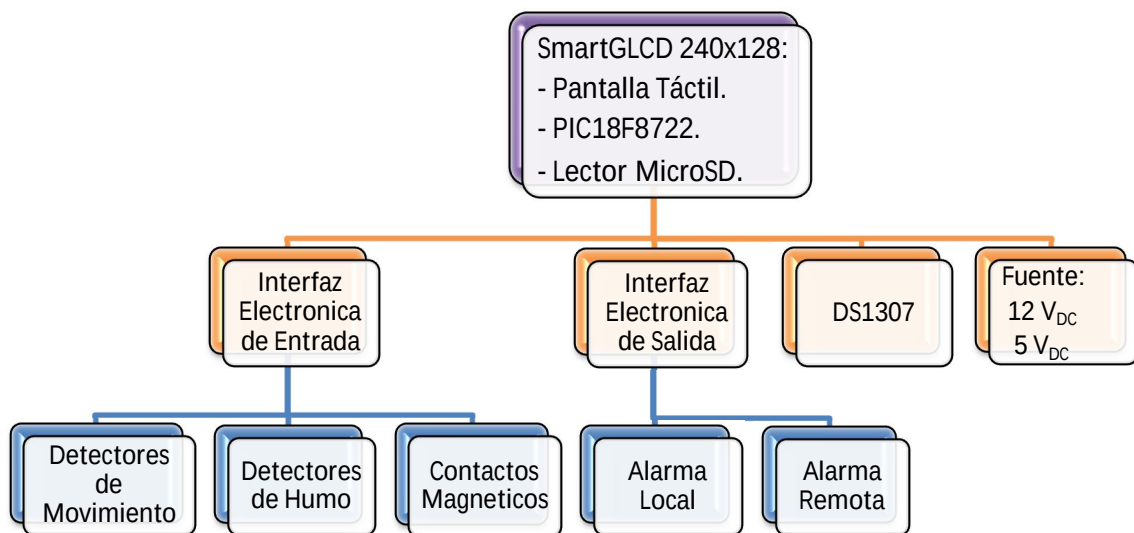


Figura 21. Diagrama en Bloques del Subsistema de Alarmas.

3.2.2.2.1 Selección de los principales componentes de Alarma de Intruso.

Sensor de movimiento

Durante la selección de este dispositivo se analizó cuidadosamente cada una de las tecnologías presentes en el mercado para determinar cuál tiene mejor desempeño en un ambiente interior como el establecido por el departamento de electrónica.

La siguiente tabla muestra las características de los tres tipos de detectores de movimiento preseleccionados para evaluar sus fortalezas y debilidades.

Tabla 5: Principales características de Sensores de Movimiento propuestos.

Característica	BV-300	ATU2000C	LC-151
Principio	PIR	Ultrasónico	Microondas/PIR
Cobertura	278.16 m ²	185.8 m ²	157 m ²
Campo de Vista	90 grados	360 grados	90 grados
Atraviesa objetos	No	Si	Si
Salida	Relevador	Relevador	Relevador
Alimentación	12 V _{DC}	24 V _{DC}	12 V _{DC}
Costo	\$ 18	\$ 212	\$ 70

Se seleccionó el detector BV-300, marca: **DSC** por las siguientes razones:

- La tecnología PIR no atraviesa objetos, esta situación es requerida para evitar falsas alarmas producto del movimiento de personas en otras áreas tales como el pasillo o salones adyacentes al departamento.
- Mayor cobertura y facilidad de instalación.
- Alimentación y salida adoptada por todos los sistemas de seguridad.
- Protección contra sobrevoltajes transitorios y estáticos.
- Excelente inmunidad a interferencia radioeléctrica.
- Distribución y soporte técnico nacional brindado por **Seguridad C&B.**
- Ampliamente utilizado en los sistemas de seguridad por su bajo coste, rápida repuesta y estilo atractivo para uso interior.



Figura 22. Detector de movimiento BV-300.

Sensor de Humo

Para detectar con precisión y prontitud la presencia de incendios en el departamento se proponen tres dispositivos de detección que realizan la misma función utilizando diferentes principios de medición.

La siguiente tabla muestra las características más importantes de cada modelo propuesto.

Tabla 6: Principales características de los Sensores de Humo propuestos.

Característica	FSA-410B	250-CO	SC10U-3B
Principio	Fotoeléctrico	Monóxido de Carbono	Ionización
Montaje	Techo	Pared	Techo
Alarma integrada	No	No	Si
Salida	Relevador	Relevador	Relevador
Alimentación	12 V _{DC}	12/24 V _{DC}	14 – 30 V _{DC}
Consumo	25 mA	150 mA	100 mA
Costo	\$ 40	\$ 100	\$ 63

Se eligió el sensor FSA-410B marca: **DSC** por las siguientes razones:

- Detección comprobada y certificada por UL, ULC y EU.
- Sensor de temperatura y alarma audible opcionales.
- Menor consumo de energía.
- Alimentación y salida adoptada por todos los sistemas de seguridad.
- Distribución y soporte técnico nacional brindado por **Seguridad C&B**.
- Excelente aceptación en el mercado por su calidad y bajo coste.



Figura 23. Detector de humo FSA-410B.

Sirena Local

La selección de este dispositivo se realizó basándose en las características constructivas del departamento, las cuales determinan el modelo de propagación acústico y por consiguiente los niveles de sonido y frecuencias necesarios para establecer una condición de alarma capaz de notificar a sus ocupantes.

A continuación se proponen los siguientes dispositivos de señalización audible:

Tabla 7: Principales características de las Alarmas Interiores propuestas.

Característica	SD15WULF	SD20W	SPC12RP
Tipo	Sirena	Sirena	Bocina
SPL	105dB	110dB	110dB
Potencia	15W	20W	15W
Alimentación	6-12 V _{DC}	6-12 V _{DC}	12 V _{DC}
Consumo	350 mA	700 mA	1.25 A
Costo	\$ 15	\$ 25	\$ 30

Se seleccionó la sirena SD15WULF marca: **DSC** por las siguientes razones:

- Nivel de sonido y frecuencia adecuado para interiores.
- Doble tono de señalización.
- Menor consumo de energía.
- Distribución y soporte técnico nacional brindado por **Seguridad C&B**.
- Diseño elegante y de bajo coste.



Figura 24. Sirena audible SD15WULF.

Sirena Remota

Debido a que la alarma remota se instalara en la pared externa de la caseta del personal de seguridad ubicada junto a la entrada principal de la UNI, es preciso utilizar dispositivos de señalización optimizados para ambientes exteriores.

De los dispositivos disponibles en el mercado se proponen los siguientes:

Tabla 8: Principales características de Alarmas para uso exterior propuestas.

Característica	PSR	CS405-7A-T	EG1R-HDVM
Tipo	Piezoeléctrica - Estroboscópica	Estroboscópica	Bocina con luz estroboscópica
SPL	110 dB	-	88.6 dB
Intermitencia	150/min	60/min	-
Alimentación	11-14 V _{DC}	20-24 V _{DC}	16-33 V _{DC}
Consumo	250 mA	96 mA	167mA
Costo	\$ 15	\$ 138	\$ 102

Se eligió la sirena audible con luz estroboscópica PSR marca: **DSC** porque:

- La tecnología Piezoeléctrica – Estroboscópica es capaz de establecer alarmas audiovisuales que se pueden percibir desde lejos debido al alto tono e intensidad acústica - luminosidad que pueden emitir.
- Menor consumo de energía.
- Distribución y soporte técnico nacional brindado por **Seguridad C&B**.
- Con gran aceptación en el mercado por ser de eficiente y de bajo coste.



Figura 25. Sirena piezoeléctrica con luz estroboscópica PSR.

3.2.2.2.2 Hardware de subsistemas de Control de Acceso y Alarmas

Circuito de control del SmartGLCD240x128Board

Los fabricantes del SmartGLCD diseñaron e implementaron este sistema en una placa de circuito que fue planificada cuidadosamente para optimizar sus recursos, la interconexión entre sus componentes y la disposición de puertos Entrada/Salida libre se encuentran determinados como se ilustra en la figura 26.

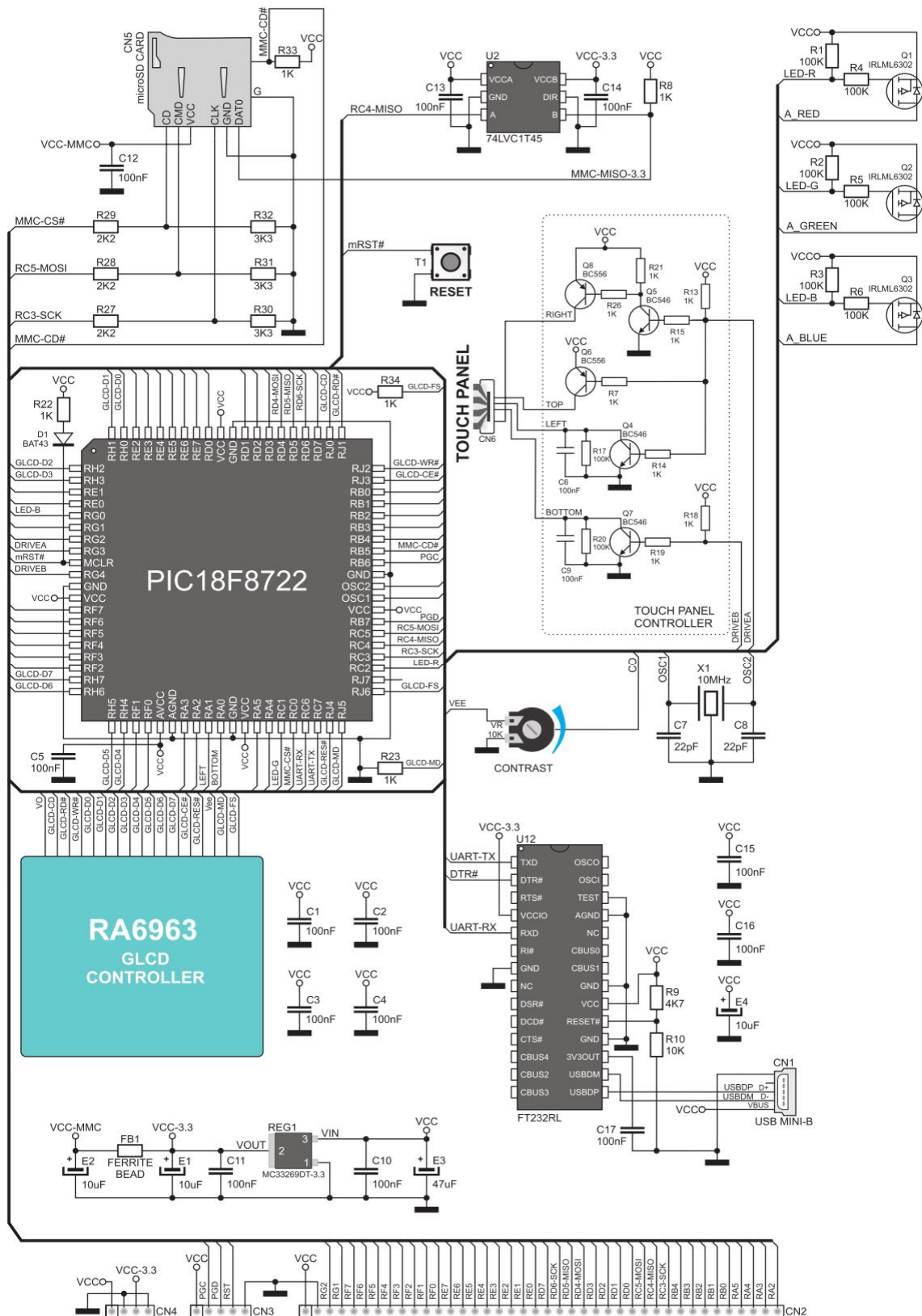


Figura 26. Diagrama de circuito del SmartGLCD240x128 Board.

Circuito para interactuar con dispositivos de entrada digitales

Los subsistemas de Control de Acceso y Alarma integran dispositivos de entrada que cumplen con tareas específicas de detección y control, estos dispositivos funcionan con un voltaje de alimentación de 12 V_{DC} , por lo tanto sus salidas no pueden contactarse directamente al MCU del SmartGLCD ($V_{\text{CC}} = 5\text{ V}_{\text{DC}}$).

Para monitorear el estado de estos dispositivos se diseñó una tarjeta de interfaz opto-acoplada que convierte niveles de voltajes de entrada de 12 V_{DC} en señales de lógica TTL (0 y 5 V_{DC}), las cuales pueden ser conectadas a las entradas del microcontrolador. Esta tarjeta a su vez es capaz de distribuir la alimentación en 12 V_{DC} a todos los dispositivos conectados en sus 8 canales, logrando así implementar un sistema de alimentación y monitoreo centralizado.

Conexión de los dispositivos de entrada

Los dispositivos de entrada se conectan a los bornes de tres pines etiquetados desde J1 hasta J8 (1 por canal), los pines 1 y 3 de cada borne proporcionan el voltaje de alimentación (12 V_{DC}) que requieren los detectores (ver figura 30). El pin 2 de cada borne se utiliza para monitorear el estado de los dispositivos.

Existen diferencias en la forma de conectar los detectores y los pulsadores utilizados, los detalles de conexión para cada caso se presentan a continuación:

Conexión de Detectores

Los detectores son subsistemas electrónicos que para su funcionamiento requieren energizarse con 12 V_{DC} , estos dispositivos utilizan un mecanismo de conmutación (relevador) que cambia de estado (cierra/abre sus contactos) cuando se detecta un cambio en la variable monitoreada.

La figura 27 muestra la conexión entre un detector y un canal de entrada de la tarjeta de interfaz, aquí se puede observar que los pines de alimentación (+ y -) del sensor se conectan a los pines 1 y 3 de la tarjeta (12 V_{DC}) respectivamente. Para monitorear el estado del detector se hace pasar la línea “+12V” por un

contacto del relevador y se retorna al pin 2 de la bornera, de esta manera cuando el sensor cambia de estado interrumpe/deja pasar el voltaje de retorno.

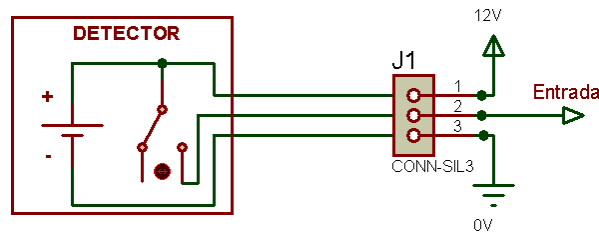


Figura 27. Conexión entre un detector y un canal de entrada.

Nota: La figura anterior muestra una conexión que usa el contacto normalmente abierto (NA) del relevador, sin embargo, también se pueden utilizar un contacto normalmente cerrado (NC) considerando que se invierte la lógica de detección.

Conexión de Pulsadores

Los pulsadores son dispositivos electromecánicos utilizados para solicitar una función. Los tipos de pulsadores que se utilizaron en este proyecto son: Un botón de salida (NC) y botón de reinicio (NA) cuya función es solicitar al MCU que abra la puerta y reinicie la clave de administrador respectivamente.

La figura 28 muestra la conexión entre un pulsador NC y un canal de entrada:

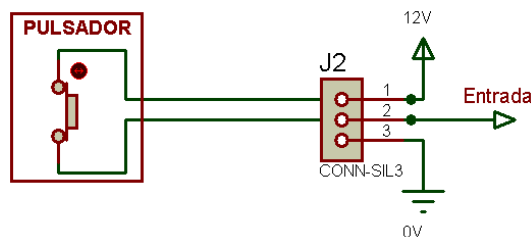


Figura 28. Conexión entre un pulsador y un canal de entrada.

Para el ejemplo de la figura anterior, bajo condiciones normales, el voltaje “+12V” siempre retorna al pin 2 de la tarjeta, sin embargo cuando una persona presiona el pulsador, este se abre e interrumpe el paso de los “+12V”, la tarjeta de interfaz detecta el cambio y lo refleja en la entrada del MCU, luego el micro interpreta la solicitud del pulsador y ejecuta la acción correspondiente. Los pulsadores NA realizan la misma función pero con estados lógicos invertidos.

Funcionamiento de la interfaz de entrada

Esta tarjeta esta compuesta por ocho canales ópticamente acoplados, los cuales se alimentan a través de dos fuentes (eléctricamente aisladas) de 12 V_{DC} y 5 V_{DC}, las cuales se conectan a través de los bornes J10 y J11 respectivamente (ver figura 30). Cada canal esta integrado por los siguientes componentes:

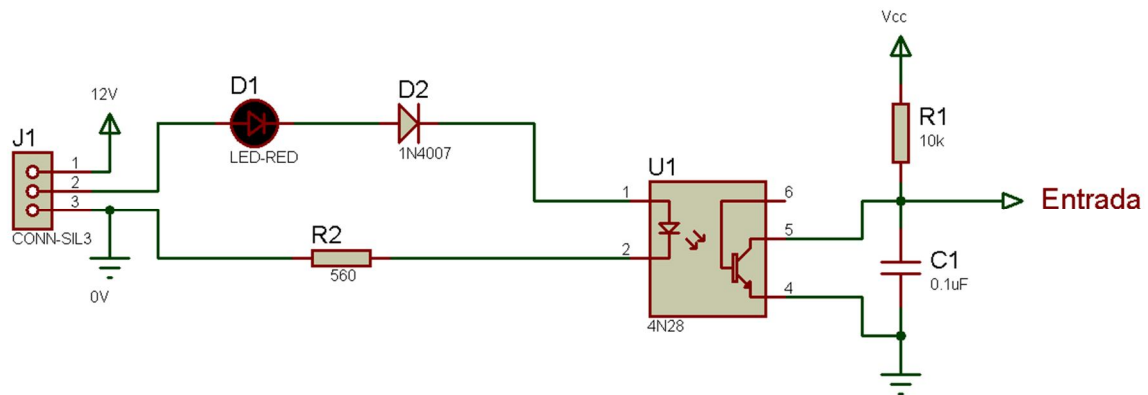


Figura 29. Canal de entrada de la tarjeta de interfaz.

Basándose en el circuito anterior, cuando un dispositivo de entrada retorna +12V al pin 2 (monitoreo), se genera una corriente de maya de la siguiente magnitud:

$$I_M = \frac{(12V - V(D1) - V(D2) - V(D_{OPTO}))}{R2} = \frac{(12V - 1.5V - 0.7V - 1.18V)}{560\Omega} = 15.39mA$$

Nota: Los voltajes de D1, D2 y D_{opto} son valores típicos de sus hojas de datos.

Según las especificaciones del 4N28 esta corriente es suficiente (5mA mínimo) para que el diodo LED del optoacoplador sature al fototransistor, el cual conecta a 0V (0 lógico) el pin que va a la entrada del MCU, al mismo tiempo el diodo LED (D1) se enciende para notificar que la entrada esta habilitada (12V en el pin2).

Cuando se interrumpe el retorno de +12V al pin 2, el diodo LED del optoacoplador no conduce y el fototransistor permanece en corte, debido a que la impedancia de entrada del PIC es alta, la corriente fluye hacia C1, el cual se carga rápidamente Vcc (5V) y luego se abre, de esta manera se logra establecer un 1 lógico a la entrada del microcontrolador. D2 se utiliza para evitar que voltajes de polaridad invertida (conectados por error) dañen al optoacoplador.

Circuito para interactuar con dispositivos de salida

El sistema de seguridad desarrollado utiliza varios dispositivos de salida que ayudan a cumplir la etapa final de la gestión de acceso y notificación de alarmas, estos dispositivos están clasificados en las siguientes categorías:

- Mecanismo de bloqueo (Cerradura electromagnética).
- Dispositivos de señalización (Alarma local y Zumbador).
- Transmisor de alarmas remotas (Modulo TX de RF).

Se diseño una tarjeta de interfaz de salida optoacoplada, la cual es capaz de controlar la operación de estos dispositivos utilizando las señales de control TTL que genera el microcontrolador del SmartGLCD (ver figura 34).

Esta tarjeta cuenta con seis canales de salida de tres tipos diferentes, cada uno se diseño especialmente para facilitar el control del dispositivo que tiene conectado. A continuación se presentan los tres tipos de canales implementados en conjunto con su fundamentación teórica:

Canales de salida a relevador

La tarjeta de interfaz cuenta con cuatro canales de salida a relevador, dos de ellos se utilizan para el control de la cerradura electromagnética y la alarma local, los otros dos canales están reservados para futuras ampliaciones.

Cada canal de salida a relevador esta integrado por los siguientes componentes:

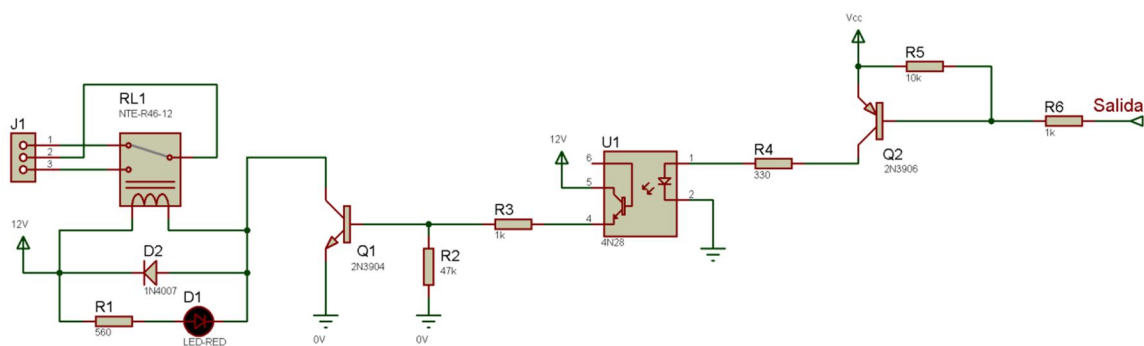


Figura 31. Canal de salida a relevador.

Funcionamiento de un canal de salida a relevador

Cuando el microcontrolador desconecta su salida (alta impedancia), la corriente que circula en R5 es nula debido a que no cierra un circuito, por lo tanto no hay caída de tensión en este resistor y el voltaje de base del transistor es Vcc, esto mantiene bloqueado al diodo de Emisor – Base Q2, de manera que este permanece apagado.

Sin embargo cuando la salida del microcontrolador pasa a 0V, el transistor 2N3906 se enciende, esto se debe a que R5 y R6 conducen (cierran un circuito) y esto provoca una caída de tensión en su voltaje de base, que se puede determinar de la siguiente manera:

$$V_B = V_E - V_{E-B} = V_{CC} - 0.7V = 5V - 0.7V = 4.3V$$

Según la hoja de datos del PIC18F8722, la corriente de entrada máxima (modo carga) que soporta cada pin del micro es de 25mA, para limitar esta corriente se calculo R6 de manera que permita una demanda de:

$$I_E = \frac{V_B}{R6} = \frac{4.3}{1K\Omega} = 4.3mA \quad \text{El cual es un valor de operacion seguro para el PIC}$$

Con Q2 encendido, Vcc pasa hasta el circuito serie comprendido por R4 y el diodo LED del optoacoplador, este LED se polariza en directa y conduce una corriente de la siguiente magnitud:

$$I_{OPTO} = \frac{V_{CC} - V_{CE}(Q2) - V(D_{OPTO})}{R4} = \frac{5V - 0.25V - 1.18V}{330\Omega} = 10.81mA$$

Esta corriente es suficiente para que el diodo LED sature al fototransistor del 4N28, el cual lleva 12V al circuito de polarización comprendido por R2, R3. Estas resistencias encienden a Q1 con un voltaje V_{BE} de la siguiente magnitud:

$$V_{B-E} = V_B - V_E = 0.7V + 0V = 0.7V$$

Q1 cierra el circuito que energiza con 12V la bobina del relevador y lo hace conmutar, a su vez enciende un LED que indica que esa salida esta activa (D1).

Cuando el relevador conmuta, provoca un cambio de estado en sus contactos (NC > abierto y NA > cerrado) por tanto se logra interrumpir o cerrar las líneas de alimentación de los dispositivos de salida conectados al relevador.

El resistor R1 se utiliza para limitar la corriente de D1 a un valor adecuado de:

$$I_{D1} = \frac{12V - V(D1) - V_{CE}(Q1)}{R1} = \frac{12V - 1.5V - 0.3V}{560\Omega} = 18.21mA$$

El diodo en paralelo con la bobina (D2) se utiliza como protección ante los picos de fuerza contraelectromotriz producidos por la carga inductiva de la bobina en el momento de conmutación.

Cuando la salida del microcontrolador es un alto (5V), los resistores R5 y R6 no conducen debido a que no hay diferencia de potencial entre ellos, por esta razón se mantienen 5V en la base de Q2 y este permanece apagado.

Con Q2 en corte el diodo LED del optoacoplador no satura al fototransistor y este a su vez no polariza a Q1, por lo tanto el relevador no se energiza y la salida permanece en las condiciones iniciales (NC > cerrado y NA > abierto).

Canal de salida de 12V con transistor MOSFET

La tarjeta de interfaz integra un canal de salida de 12V_{DC} (canal 5), este fue diseñado para alimentar un zumbador que agiliza el tiempo de acceso al local.

Se utilizo un transistor MOSFET (IRFP450) como elemento de salida debido a que se requiere mayor frecuencia de conmutación para indicar a los usuarios cuando esta finalizando el tiempo de ingreso y esta próximo a generarse una alarma local (por no cerrar la puerta).

Funcionamiento de un canal de salida de 12V con transistor MOSFET

El funcionamiento del circuito de polarización del LED del optoacoplador es similar al de los canales a relevador, con la diferencia que en este caso el diodo indicador de **“salida activa”** se conecta en serie con el LED interno del 4N28.

Para este canal (Ver figura 32) la corriente que pasa por el LED del optoacoplador y el LED indicador de salida es:

$$I_{OPTO} = \frac{V_{CC} - V_{CE}(Q10) - V(D9) - V_{OPTO}}{R27} = \frac{5V - 0.25V - 1.5V - 1.2V}{330\Omega} = 6.21mA$$

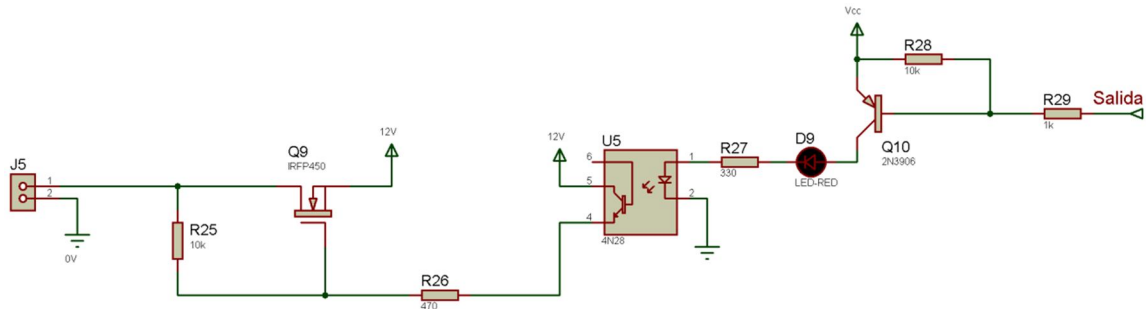


Figura 32. Canal de salida a transistor MOSFET.

Esta corriente satura al fototransistor del optoacoplador de manera similar al caso anterior, el cual polariza y enciende al transistor Q9, quien se encarga de mandar 12V a la salida de la bornera J5, donde se conecta el zumbador.

Los resistores R25 y R26 garantizan que el voltaje de polarización sea superior al mínimo ($V_{GS} = 2V$) para que el IRFP450 se sature, el cual, una vez encendido tiene una resistencia entre drenador y fuente muy baja ($R_{DS(ON)} = 0.4 \Omega$), debido a que la corriente consumida por el zumbador es de 15 mA, se puede asumir que todo el voltaje (12V) se le entrega a este dispositivo.

En conclusión cada vez que el microcontrolador manda 0V a este canal de salida, se mandan 12 V al zumbador, y cuando el PIC manda 5V, se desconecta la salida. La velocidad de conmutación del MOSFET permite enviar pulsos de salida de mayor frecuencia para generar tonos acústicos, los cuales se utilizan para agilizar el tiempo de ingreso al local.

Canal de salida de 5V con transistor BJT

El canal seis de la tarjeta provee una señal de salida TTL (no convierte niveles de voltaje) que se utiliza para la habilitación del transmisor de alarmas remotas.

Este canal utiliza un transistor BJT (TIP48) como elemento de salida para poder enviar 0V ó 5V a un puerto de entrada del transmisor de RF, el cual también interpreta estas señales como comandos para hacer una transmisión de estado.

Funcionamiento de un canal de salida de 5V con transistor BJT

Su funcionamiento es similar al de un canal de salida con transistor MOSFET, en la parte de polarización del optoacoplador no hay diferencia, sin embargo en la etapa de salida se puede observar que los resistores de polarización de Q11 tienen valores diferentes, esto se debe a que los transistores BJT tan solo requieren 0.7V entre Base y Emisor para encender. Otra diferencia que se encuentra en este canal de salida es que provee la alimentación ($5V_{DC}$) del transmisor de alarmas remotas a través del borne J6, tal y como se ilustra en la siguiente figura:

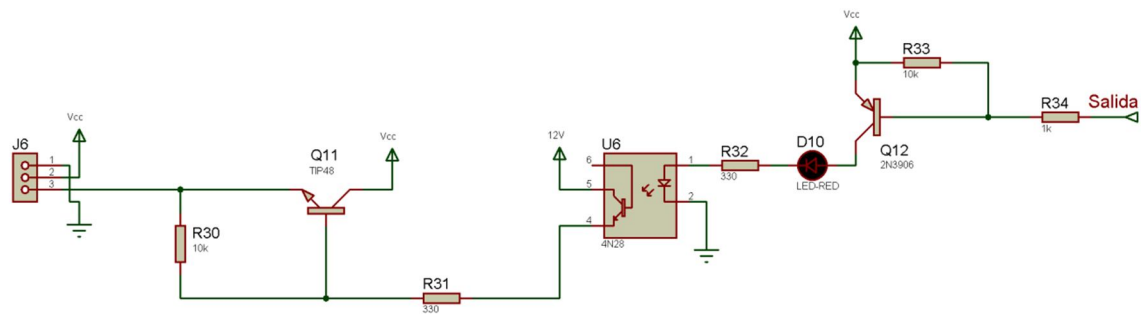


Figura 33. Canal de salida a transistor BJT.

En operación normal, cuando el microcontrolador establece 0V en la entrada de este canal, su salida envía 5V hacia el transmisor y cuando el micro establece 5V en la entrada, la salida se desconecta. En estado de alta impedancia del PIC la salida también permanece desconectada.

A continuación se presenta el diagrama de circuito completo de la tarjeta de interfaz de salida con sus seis canales, bornes de alimentación y sus pines de conexión al microcontrolador.

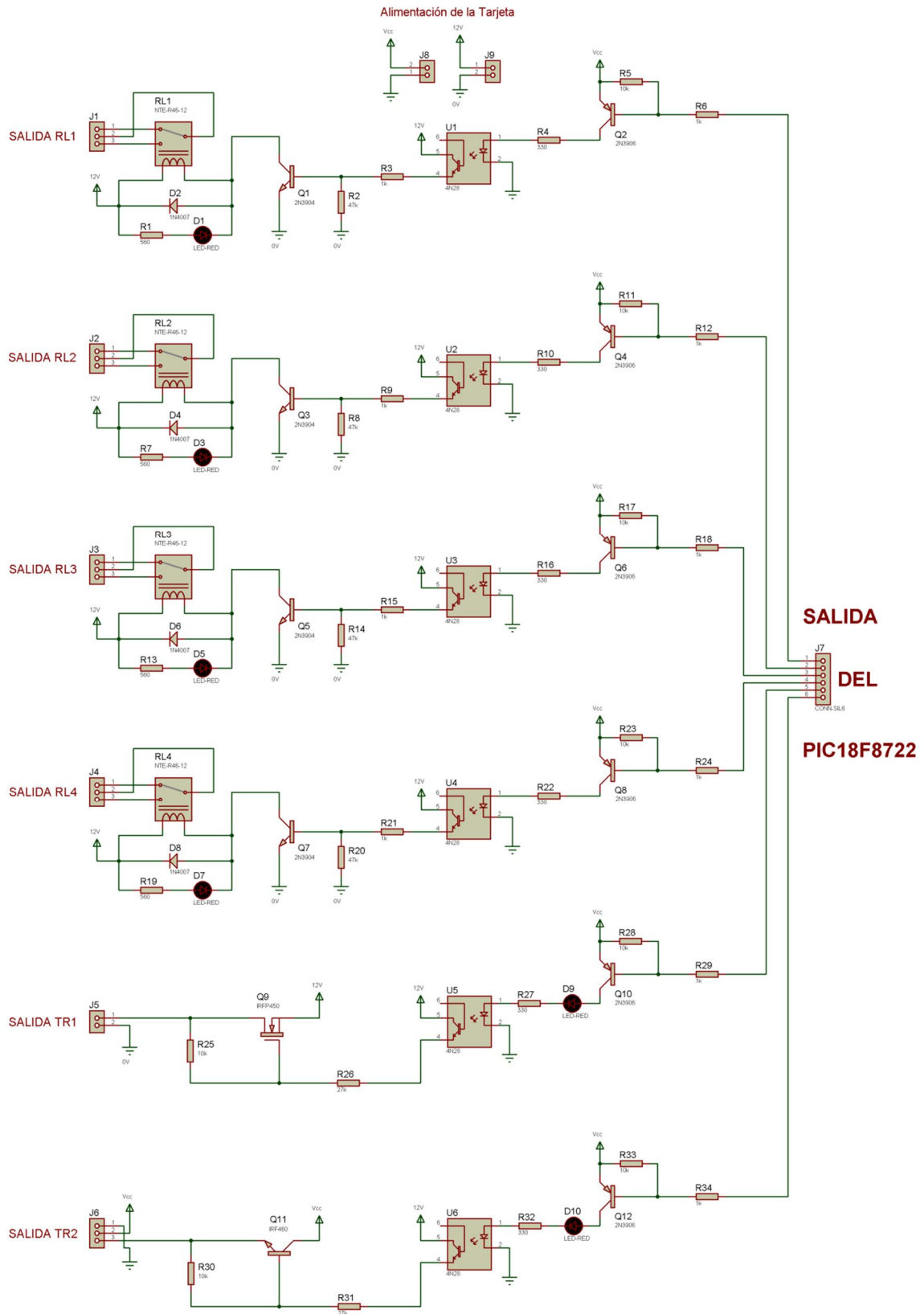


Figura 34. Diagrama de circuito de la interfaz de salida.

Circuito para interactuar con el RTC DS1307.

El DS1307 es un reloj calendario de bajo consumo que almacena la información del tiempo/fecha en formato BCD (Decimal codificado en binario), para su funcionamiento requiere interconectarse con algunos componentes externos y un dispositivo maestro que gestione la lectura y escritura de datos y comandos a través del protocolo serial I²C.

Para interactuar con el RTC se diseñó una tarjeta electrónica que integra al DS1307 con todos los componentes que este requiere para su funcionamiento, esta tarjeta se interconecta a los pines RG1 (SCL) y RG2 (SDA) del PIC18F8722, los cuales están configurados para operar como un puerto I²C implementado a nivel de software (Ver figura 35).

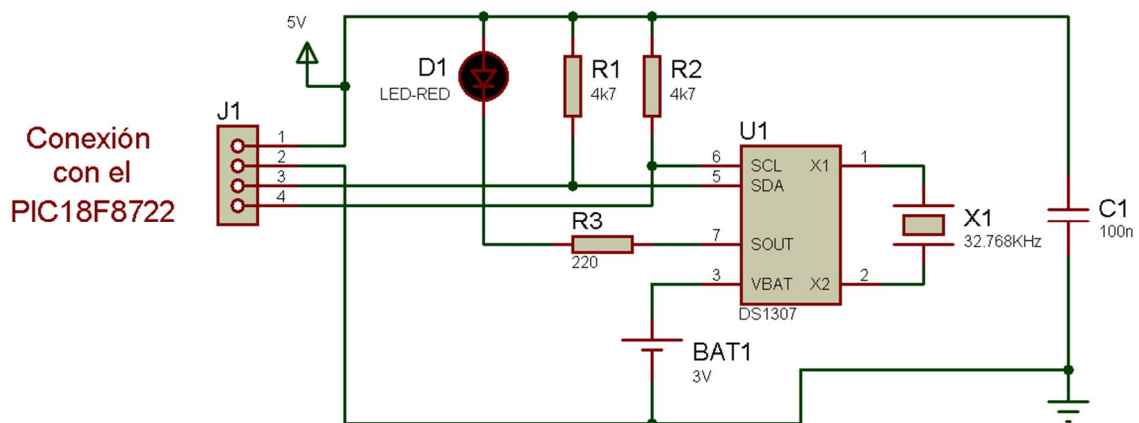


Figura 35. Diagrama de circuito de la tarjeta de control del DS1307.

Funcionamiento de la tarjeta del RTC DS1307

El componente principal del RTC es un preciso cristal de cuarzo que garantiza una frecuencia de operación de 32.768kHz (X1), este cristal debe tener una capacitancia de carga específica de $C_L = 12.5\text{pF}$.

El DS1307 requiere un sistema de alimentación de $5V_{DC}$, el cual llega a la tarjeta a través del conector J1, a su vez integra un sistema de alimentación de respaldo que consiste en una batería de 3V tipo moneda conectada al pin 3.

Internamente el DS1307 tiene toda la circuitería necesaria para detectar una falla en la alimentación principal y conmutar hacia el voltaje de respaldo, de igual manera retorna al voltaje principal cuando este se restablece.

Para implementar el bus de comunicación serial I²C entre el MCU y el DS1307 se requiere utilizar resistencias de **pullup** (R1 y R2) debido a que los pines SCL (Pin6) y SDA (Pin 5) son entradas de ***drenador abierto***. Estas resistencias se encargan de limitar la corriente de entrada hacia los pines de ambos dispositivos, de manera que se mantengan en valores de operación seguros para los mismos.

Para finalizar el Pin 7 del RTC se configura para que genere una señal cuadrada de 1Hz, la cual se utiliza para indicar el estado del reloj a través del diodo LED “D1” y la resistencia limitadora R3, de tal manera que el LED pasa 0.5 segundos encendido y 0.5 segundos apagado, determinando así cada segundo que pasa.

Durante operación normal, el DS1307 actualiza cada segundo sus siete primeros registros, los cuales están dedicados a brindar información de hora y fecha. El registro #8 (control) se utiliza para configurar parámetros de operación del RTC, tales como; bloqueo del Reloj, frecuencia de salida y habilitación de la misma.

Para leer la información de hora/fecha el MCU accede a los registros del DS1307 (utilizando I²C) en modo lectura, el cual le retorna los datos en formato BCD, de igual manera ingresa al registro de control y demás registros en modo escritura, para realizar configuraciones iniciales de la señal de salida, habilitación e inicialización del reloj.

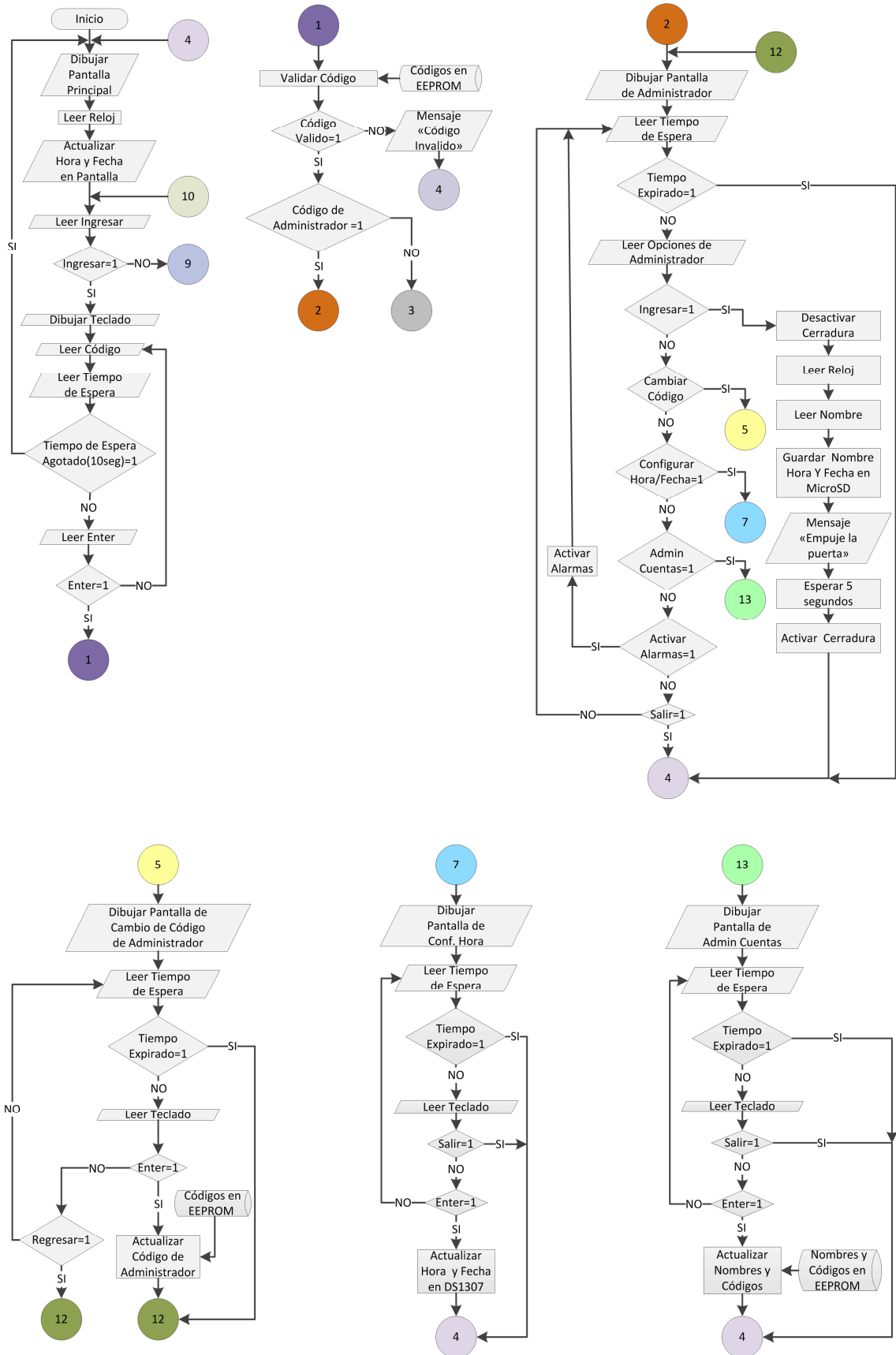
3.2.2.2.3 Algoritmo para los subsistemas de Control de Acceso y Alarma

Los autores proponen utilizar el algoritmo de control que se ilustra en la figura 36 para coordinar la ejecución de todas las tareas que contemplan los subsistemas de Control de Acceso y Alarma.

Este algoritmo fue traducido a código fuente en lenguaje de Basic y luego compilado en un archivo con formato .hex, el cual reside en la memoria de programa del PIC18F8722, desde donde se coordina toda la gestión de acceso y alarmas en conjunto con los demás componentes del sistema.

A continuación se enumeran las principales tareas que ejecuta el PIC18F8722, las cuales se encuentran contenidas en su algoritmo de control:

1. Inicializa todos los valores del RTC, Nombres y Claves de Acceso, etc.
2. Muestra información actualizada de hora/fecha en la pantalla.
3. Implementa una interfaz hombre-maquina en modo táctil.
4. Enciende/apaga y controla los colores de la luz de fondo de la pantalla.
5. Valida las claves de acceso ingresadas comparándolas con los usuarios autorizados de la tabla de acceso almacenada en su memoria.
6. Implementa dos tipos de cuentas con diferentes privilegios, Administrador:
Activar/desactivar las alarmas, configurar la hora/fecha, crear, modificar y eliminar cuentas de usuario, cambiar su contraseña e ingresar al local.
Usuario: Ingresar al local y cambiar su clave de acceso.
7. Libera la cerradura y coordina con precisión el tiempo de ingreso.
8. Evalúa la detección de intrusos, incendios y activa alarmas locales y remotas cuando es requerido.
9. Libera automáticamente la puerta en caso de incendios.
10. Arma/desarma el sistema automáticamente según horario establecido.
11. Almacena todos los eventos de acceso y alarmas en un registro diario que se guarda en una memoria MicroSD, este registro se crea en un archivo **.csv** (valor separado por coma) el cual es compatible con Microsoft Excel.



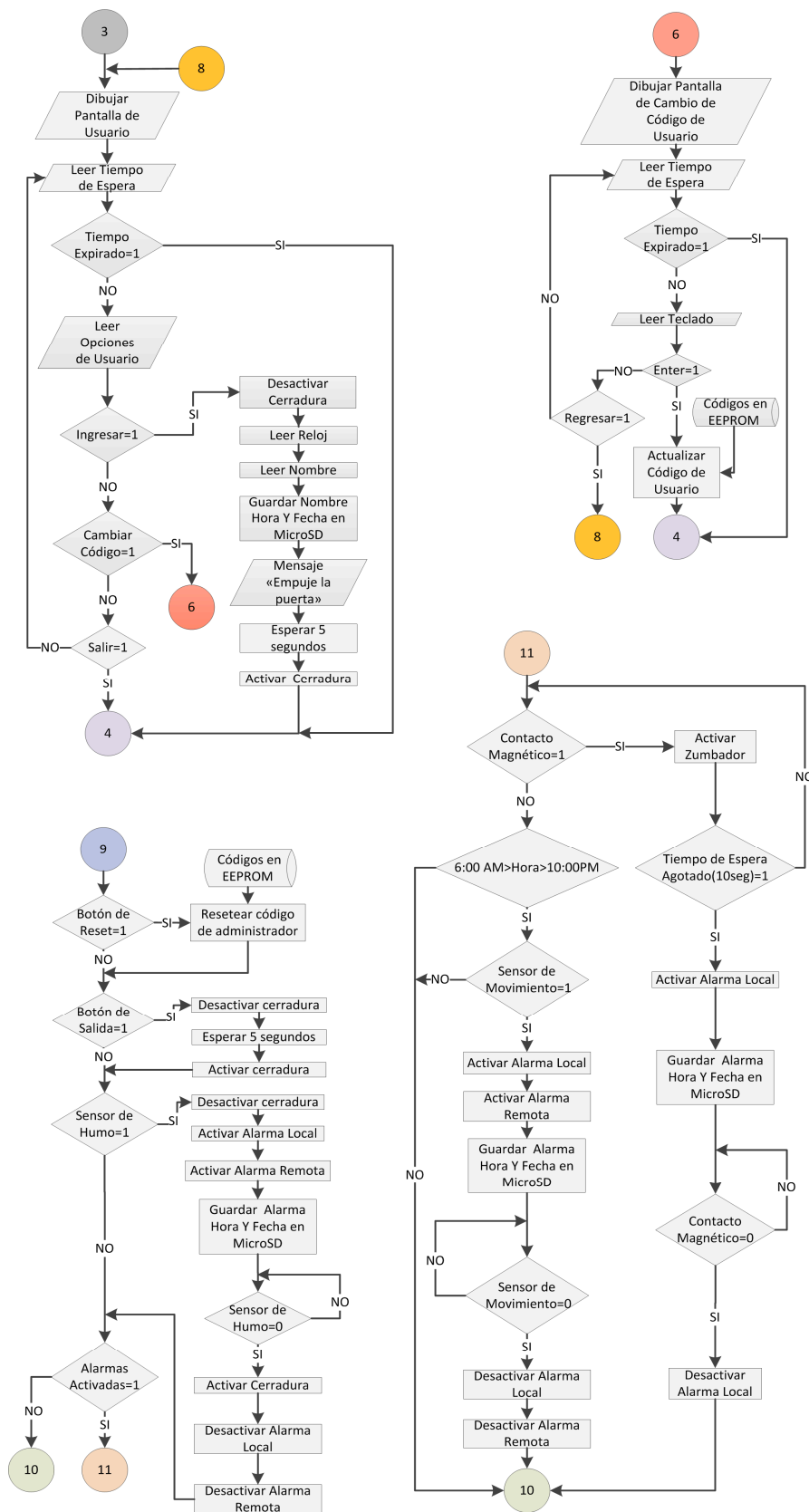


Figura 36. Algoritmo propuesto para Subsistemas de Control de Acceso y Alarma.

3.2.2.2.4 Alimentación de los Subsistemas de Control de Acceso y Alarma

La alimentación de los componentes que integran ambos subsistemas es proporcionada por dos fuentes de 5V y 12V, las cuales se utilizan de forma independiente para garantizar la distribución de energía de forma segura y eficiente. Estas fuentes se seleccionaron para suplir la demanda de corriente que consumen en conjunto todos los elementos de control de acceso y alarma, a continuación se presenta una tabla de consumo de corriente los dispositivos:

Tabla 9: Consumo de los componentes de Control de Acceso y Alarmas.

Modelo	Descripción	5V	12V	Observación
SmartGLCD	Pantalla Inteligente	500mA		Control
DS1307	Tarjeta del RTC	6.5mA		Control
ECL-ACC300	Cerradura Electromagnética		500mA	Fuerza
Piezo12	Zumbador Piezoeléctrico		15mA	Señalización
BV-300	Sensor de movimiento		60mA	3 Detectores
FSA-410B	Sensor de Humo		50mA	2 Detectores
SD15WULF	Sirena Local		350mA	Señalización
	Tarjeta de Interfaz de entrada (8 canales)		123.12 mA	15.39mA x canal
	Tarjeta de interfaz de salida (canales a relevador)	43.24mA		10.81mA en cada Opto
	Tarjeta de Interfaz de salida (canales a relevador)		192.84 mA	18.21mA (4) + 30mA (4)
	Tarjeta de interfaz de salida (canal a MOSFET)	6.21mA		In: LED del Opto
	Tarjeta de interfaz de salida (canal a BJT)	6.21mA		In: LED del Opto
Total		562.2mA	1.3 A	por fuente

Nota1: El consumo esta previsto para condiciones de máxima demanda.

Nota2: En las tarjetas de entrada se desprecia la corriente que fluye hacia el PIC debido a que este valor ya fue incluido en el nivel de consumo global de SmartGLCD. Además en los canales de salida a transistor se desprecia la corriente de polarización debido a que es muy baja e irrelevante para el cálculo.

Para suplir la demanda de corriente de todos los equipos instalados se requirió el uso de las siguientes fuentes de poder:

Tabla 10: Especificaciones técnicas de las fuentes de alimentación seleccionadas.

Característica	CFM40T-02	S-60-12
Voltaje de entrada	90 - 260 V _{AC}	100 - 220 V _{AC}
Voltaje de Salida	5 V _{DC}	12 V _{DC}
Corriente de Salida	2.5 A	5A
Potencia	40W	60W
Tipo de conversión	Conmutada	Conmutada

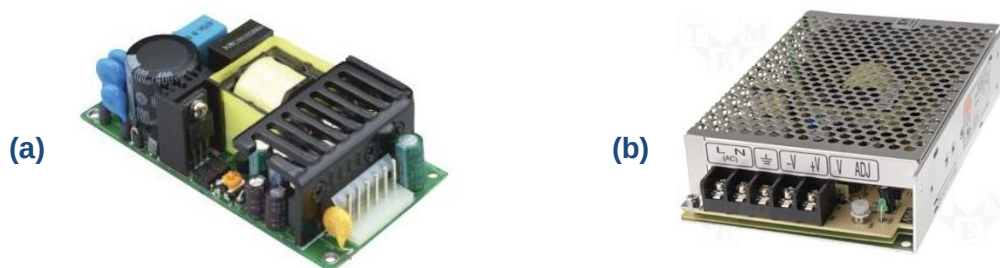


Figura 37. Fuentes de alimentación conmutadas a) CFM40T-02. b) S-60-12.

Estas fuentes entregan aproximadamente cuatro veces más de la potencia requerida en cada nivel de voltaje (5V y 12V), no obstante, se instalaron con el propósito de garantizar un amplio margen de servicio para futuras ampliaciones.

Sistema de Alimentación Ininterrumpida (UPS)

Para respaldar la alimentación de las fuentes de poder ante fallos de la energía comercial se instaló una UPS, su capacidad fue determinada en función de la máxima demanda de corriente alterna de cada fuente (valor especificado en sus hojas de datos como I_{IN}), este cálculo se especifica a continuación:

$$I_{UPS} = I_{IN(5V)} + I_{IN(12V)} = 1A_{(115V)} + 2A_{(115V)} = 3A$$

Se puede observar que estas fuentes demandan un máximo de 3A operando con 115 V_{AC}, por tanto la potencia de la UPS que se debe instalar debe ser de:

$$P_{UPS} = V_{SAL} * I_{SAL} = 115 V_{AC} * 3A = 345W$$

Por lo tanto se seleccionó una UPS marca: **FORZA**, modelo: **SL-761**, la cual es capaz de entregar hasta 375W operando en 115 V_{AC}. Durante las pruebas de autonomía se determinó que el UPS puede respaldar durante 4 horas el sistema.

3.2.2.3 Subsistema de Señalización Remota

El departamento de electrónica se encuentra ubicado en el tercer piso de la FEC, el cual, actualmente esta resguardado por el sistema de seguridad que ha sido implementado. En horario laboral, este departamento y sus entornos se encuentran ocupados por docentes y personal administrativo, sin embargo fuera de este horario no quedan ocupantes cerca de estas instalaciones, por esta razón se considero necesario implementar dos sistemas de señalización de alarmas: Señalización local y remota.

La señalización local se utiliza de 06:00.am a 10:00pm, su función es notificar a los ocupantes del entorno cuando se presenta alguna condición que infringe la seguridad del local, mientras que la señalización remota es un subsistema que se encarga de transferir un estado de alarma hasta la caseta del personal de seguridad, para obtener una respuesta física en momentos que no hay personas cerca del departamento. Este subsistema se activa diariamente de 10:00pm a 06:00am y tiempo completo en fines de semana, aunque durante el día también puede ser habilitado cuando se detecta humo en el local (incendio).

Componentes de hardware del subsistema de señalización remota:

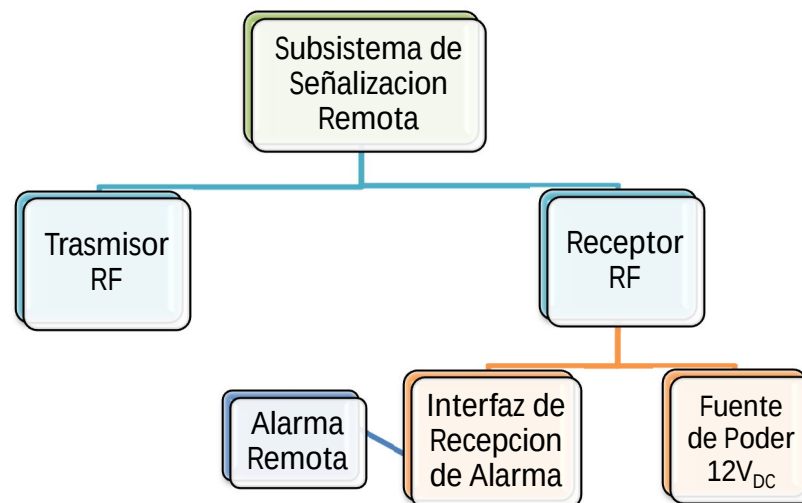


Figura 38. Diagrama en bloques del Subsistema de Señalización Remota.

3.2.2.3.1 Selección de principales componentes de Señalización Remota

Transmisor de RF

Para la selección del modulo transmisor se analizan las características de tres dispositivos capaces de establecer un enlace inalámbrico en radio frecuencia. Los criterios de clasificación se basan en determinar cual aporta más ventajas en la transmisión de un dato específico (alarma), el cual debe ser enviado a 20 metros por medio de un enlace con línea de vista hacia el receptor.

La siguiente tabla muestra los módulos propuestos para realizar esta función:

Tabla 11: Principales características de los módulos transmisores propuestos.

Modelo	rfPIC12F675F	TWS-BS-6	DR4100
Banda	UHF	UHF	UHF
Frecuencia	433.92 MHz	315 MHz	433.92
Modulación	ASK	ASK	ASK
Velocidad	40Kbps	8Kbps	115.2Kbps
Potencia	10dBm	14dBm	-
MCU	Si	No	No
E/S Externas	A/D	No	No
Programación	PICKit 1 Starter Kit	No	No
Conectividad	USB	No	Si
Alimentación	5 V _{DC}	1.5 - 12 V _{DC}	2.7 - 3.5 V _{DC}
Batería respaldo	Si	No	No
Costo	\$ 36	\$ 4.74	\$ 30

Se decidió utilizar el modulo rfPIC12F675F por las siguientes razones:

1. La banda de frecuencia de 433.92 MHz se puede operar sin costo alguno.
2. Atenuación irrelevante operando en ASK debido a la corta distancia que existen entre el transmisor y el receptor.
3. El MCU integrado permite implementar diversos algoritmos de cifrado, control y operación del transmisor.
4. Integra entradas y salidas externas ideales para telemetría y telecontrol.
5. Su alimentación esta completamente respaldada por una batería de 3.6V.
6. En la UNI se cuenta con un Kit de desarrollo para este dispositivo.

Receptor de RF

La elección del módulo de recepción se realizó con relativa facilidad, porque siempre se debe utilizar un receptor compatible con los parámetros de operación del transmisor. Por lo tanto, para el rfPIC12F675F seleccionado **Microchip** recomienda utilizar el módulo receptor: rfRXD0420.

A continuación se presentan sus características más relevantes:

Tabla 12: Principales características del módulo receptor rfRXD0420.

Modelo	rfRXD0420
Banda	UHF
Frecuencia	433.92 MHz
Modulación	ASK
Velocidad de señal	4800 Baud
Evaluación	PICKit 1 Starter Kit
Alimentación	5 V _{DC}
Costo	\$ 30

El Anexo B.1 se encuentra una explicación más detallada de los módulos de transmisión y recepción seleccionados, además de las ilustraciones gráficas e imágenes de los dispositivos.

Interfaz electrónica de recepción y activación de alarmas

Los módulos de transmisión y recepción seleccionados se interconectan a un interfaz externo que les proporciona los siguientes requerimientos:

1. Alimentación del módulo transmisor (5V_{DC}).
2. Señal de habilitación de alarma: Esta indica al rfPIC12F675F cuando debe transmitir una condición de alarma (se la proporciona el PIC18F8722 a través del canal #6 de la interfaz de salida).
3. Alimentación del receptor y decodificación de las señales recibidas.
4. Validación del dato recibido y activación de la alarma remota.

Para realizar las tareas 3 y 4 se diseñó una tarjeta electrónica que sirve de interfaz entre el módulo de recepción y la propia alarma remota.

Funcionamiento de la interfaz de recepción y activación de alarmas

La interfaz de recepción y activación de alarmas es una tarjeta electrónica que integra características similares a las interfaces de entrada y salida. En la figura 39 podemos observar que esta tarjeta cuenta con dos canales de salida a relevador similares a los estudiados en las paginas anteriores, con la única diferencia que a su salida (J1 y J2) establecen/cortan el voltaje de alimentación (12V) de la sirena remota (los anteriores solo conmutaban sus contactos).

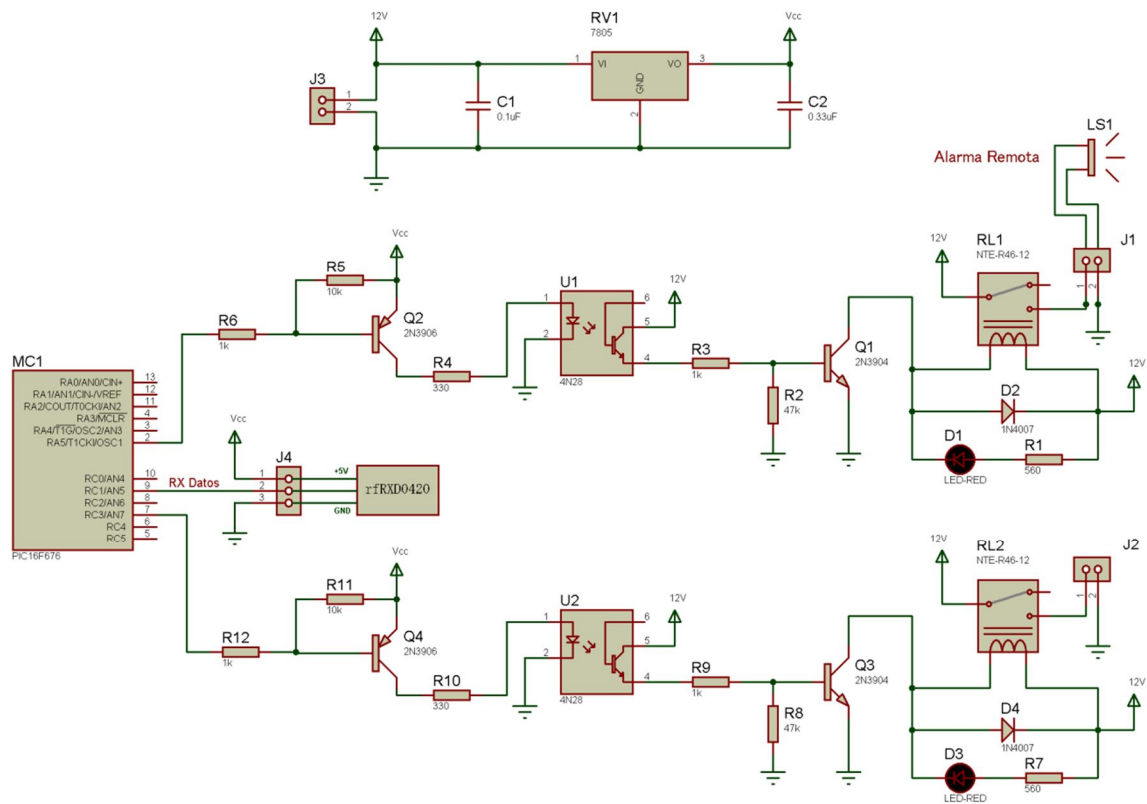


Figura 39. Diagrama de circuito de la interfaz de recepción de alarmas.

También se integra una bornera para la conexión con el receptor (J4), esta le proporciona la alimentación de 5V al rRXD0420, además de llevar los datos recibidos hasta el pin RC1 del PIC16F676. Este MCU esta programado para adquirir los datos recibidos, luego los compara con la rutina de encriptación configurada para determinar si la recepción corresponde a un dato de alarma real o se trata de ruido/interferencia.

Si el PIC determina como valido el dato recibido, este habilitara la alarma remota a través del canal de salida que esta conectado a su pin RA5.

El segundo canal de salida no tiene ninguna carga conectada, este se concibió como canal de reserva para tener flexibilidad ante futuras ampliaciones.

La alimentación principal de la tarjeta es de 12 V_{DC}, este voltaje proviene de una fuente de poder dedicada para los componentes del subsistema, sin embargo, para alimentar el microcontrolador y el receptor se requieren 5V_{DC}, los cuales se obtienen utilizando un regulador de voltaje LM7805 integrado en la tarjeta.

3.2.2.3.2 Alimentación del Subsistema de Señalización Remota

La alimentación de los componentes de señalización remota se basa en el siguiente censo de carga, que estima el consumo de corriente por componente:

Tabla 13: Consumo de componentes del subsistema de Señalización Remota.

Modelo	Descripción	5V	12V	Observación
PSR	Sirena piezoeléctrica con luz estroboscópica		250mA	Fuerza
rfRXD0420	Módulo de recepción	10mA		Control
PIC16F676	Microcontrolador PIC	200mA		Control
	Salidas a relevador	21.6mA		10.8mA en cada Opto
	Salidas a relevador		96.42mA	18.21mA (2) + 30mA (2)
	Total	231.6mA	346.4 mA	x fuente

Nota1: El consumo esta previsto para condiciones de máxima demanda.

Nota2: La carga total (578mA) se le puede atribuir a una sola fuente de 12V (aproximación) debido a que a partir de este voltaje el regulador 7805 proporciona los 5V (1.5A) a los dispositivos de control.

Se propone utilizar como sistema de alimentación una BCPS (Battery Charger and Power Supply), esta consiste en una fuente de voltaje que convierte de 120V_{AC} a 12V_{DC}, pero además cuenta con el respaldo de una batería de 7.2 AH para funcionar de forma ininterrumpida ante fallos de la energía comercial.

El modelo seleccionado ha sido la BCPS **ST-2406-2**, a continuación se muestran sus características técnicas junto a una ilustración de la fuente:

- Voltaje de entrada: 120V_{AC}, 60Hz
- Voltaje de salida: 12V_{DC}
- Corriente de salida: 1.5A Tip, 2A Max
- Potencia: 24W
- Carga batería: Si
- Costo \$30

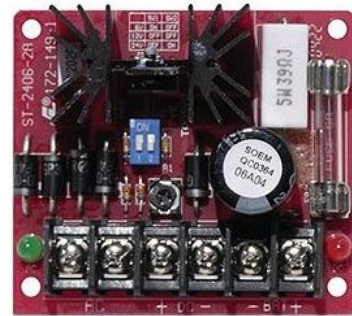


Figura 40. Fuente de alimentación con cargador de batería ST-2406-2.

Como se puede observar, esta fuente es capaz de suplir 1.5A a 12V de forma continua, lo cual es aproximadamente tres veces la corriente demandada por el subsistema, con un margen de crecimiento de la carga de hasta 1A.

Esta BCPS cuenta con circuitería de conmutación y carga para operar en modo batería, de manera que el acumulador siempre esta cargado y listo para respaldar durante aproximadamente 12 horas ($T_R = 7.2AH / 57mA = 12.45$ Hrs).

3.2.2.3.3 Algoritmo propuesto para el subsistema de Señalización Remota

El subsistema de señalización remota integra dos microcontroladores programables, uno en el transmisor (rfPIC12F675F) y otro en la tarjeta de interfaz del receptor (PIC16F676), estos dispositivos están programados para realizar las siguientes tareas:

rfPIC12F675F del modulo transmisor

1. Detectar la señal de activación de alarma (Pin GP4) del PIC18F8722.
2. Durante una transmisión enciende el LED "RFEN" (RF Enable > GP5).
3. Trasmite el dato de condición de alarma según el protocolo Keelog:
 - i. Preámbulo
 - ii. Encabezado
 - iii. Dato serial
 - iv. Bytes de función
 - v. Bytes de relleno
 - vi. Tiempo de guarda

PIC16F676 de la tarjeta de interfaz

- Adquiere los datos que provienen del receptor (Pin 18, Rx Data > RC1).
- Verifica que los datos lleguen correctamente según el protocolo Keelog.
- Si los datos pasan satisfactoriamente la verificación, activa la alarma remota por un periodo de tiempo específico a través del pin RA5.
- Desactiva la alarma remota y monitorea el canal de recepción.

La siguiente figura muestra los algoritmos propuestos para realizar estas tareas:

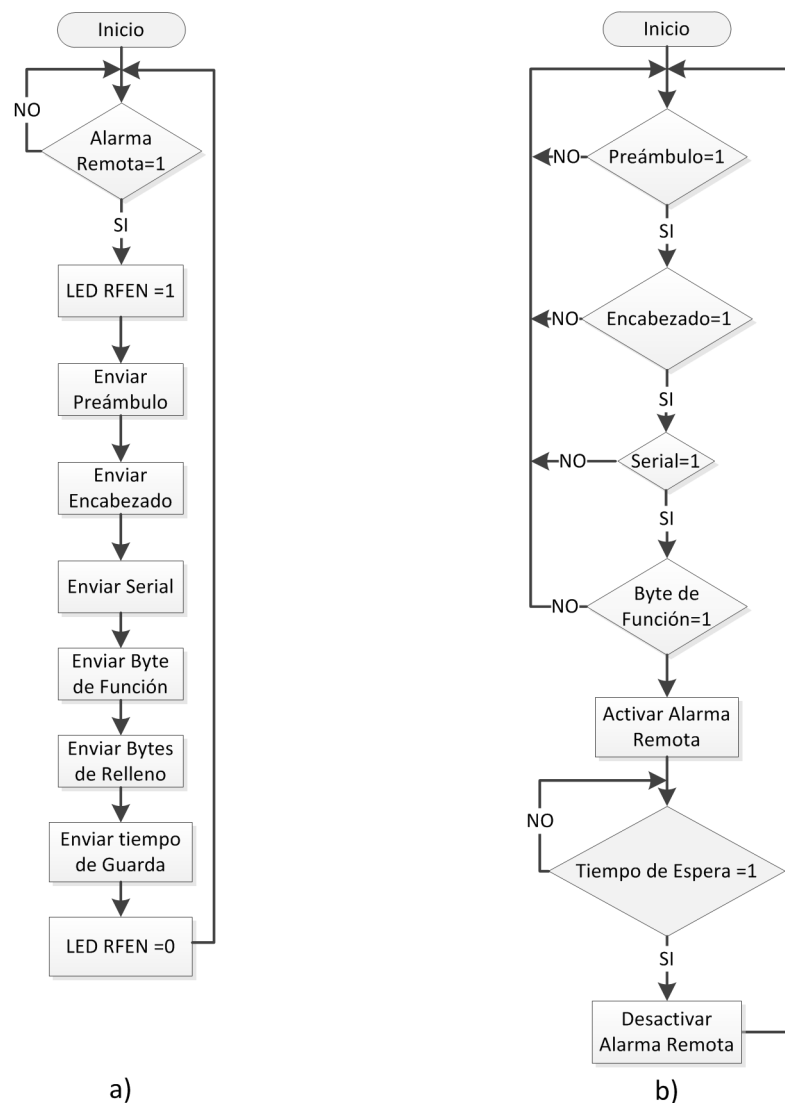


Figura 41. Algoritmo propuesto para el subsistema de señalización remota,
a) Programación del rPIC12F675F, b) Programación del PIC16F676.

3.3 IMPLEMENTACION DEL PROTOTIPO

El sistema de seguridad electrónica diseñado se implementó a nivel de prototipo utilizando los componentes que han sido descritos en las secciones anteriores. Durante la elaboración de este prototipo se llevaron a cabo varios procesos, dentro de los cuales se pueden mencionar; la programación de los microcontroladores, fabricación de las tarjetas electrónicas, instalación de los componentes del sistema en el local, pruebas y corrección de errores.

3.3.1 Programación de los MCUs

Los MCUs PIC18F8722, PIC12F675F y PIC16F676 fueron programados basándose en los algoritmos de control propuestos para cada uno de ellos, sin embargo, debido a la diferencia en la complejidad de sus tareas se decidió utilizar dos diferentes lenguajes de programación: Basic y Ensamblador. Estos lenguajes están implementados en varios software de aplicación, para este proyecto se utilizaron los programas MikroBASIC PRO for PIC y MPLAB debido a la cantidad de documentación y ejemplos que ofrecen sus desarrolladores.

A continuación se explica el desarrollo de los programas en cada lenguaje.

3.3.1.1 Compilador mikroBASIC PRO for PIC v4.6

MikroBASIC PRO es una herramienta de desarrollo para microcontroladores PIC que está diseñado para brindar al programador una forma fácil y rápida de crear aplicaciones en lenguaje de BASIC, sin sacrificar el desempeño del MCU. La figura 42 muestra una imagen del entorno de programación de mikroBASIC.

Una de las principales ventajas de utilizar mikroBASIC es que se disminuye drásticamente el tiempo de desarrollo, esto se debe a las rutinas, librerías y herramientas integradas en el software, lo cual reduce el tamaño del código y facilita el desarrollo de aplicaciones de mayor complejidad. A manera de ejemplo se puede citar el control de pantallas (7 Segmentos, LCD y GLCD), RTC, memorias (EEPROM, microSD), lectura de sensores, comunicación USB, USART, CAN, Ethernet, entre otras funcionalidades.

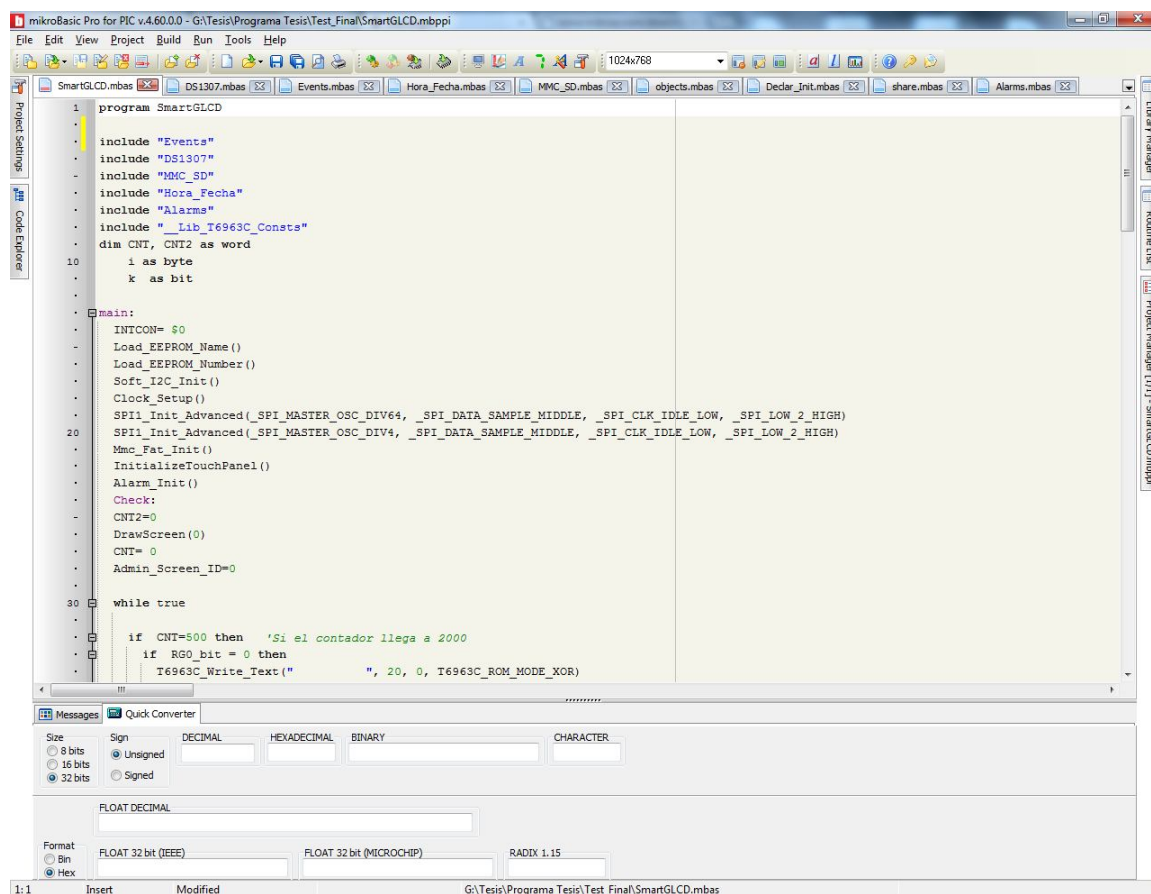


Figura 42. Entorno de programación de mikroBASIC PRO for PIC v4.6.

Librerías de mikroBASIC PRO

MikroBASIC contiene más de cuarenta librerías capaces de realizar varias rutinas específicas, estas pueden ser para interactuar con dispositivos de hardware o realizar cálculos matemáticos, a continuación se citan las librerías que contienen las rutinas utilizadas en el desarrollo del proyecto:

1. ADC Library
2. EEPROM Library
3. Multi Media Card library
4. Software I²C Library
5. SPI Library
6. Conversions Library
7. T6963C Graphic Lcd Library
8. Touch Panel Library
9. UART Library

Herramientas de mikroBASIC PRO

El menú de herramientas de MikroBASIC Pro contiene un conjunto de aplicaciones diseñadas para facilitar el uso del compilador, en la siguiente figura se muestran estas utilidades junto a su descripción:

Tools	Description
 mE Programmer F11	Run mikroElektronika Programmer.
 Package Manager	Run Package Manager.
 Active Comment Editor Ctrl+Alt+C	Show/Hide Active Comment Editor window.
 Ascii Chart	Run ASCII Chart
 EEPROM Editor	Run EEPROM Editor
 Export Code To HTML	Generate HTML code suitable for publishing source code on the web
 GLCD Bitmap Editor	Run Glcd bitmap editor
 HID Terminal	Run HID Terminal
 LCD Custom Character	Run Lcd custom character
 mikroBootloader	Run mikroBootloader
 Seven Segment Editor	Run Seven Segment Editor
 UDP Terminal	Run UDP communication terminal
 USART Terminal Ctrl+T	Run USART Terminal
 Options F12	Open Options window

Figura 43. Menú de herramientas de mikroBASIC PRO.

3.3.1.2 Desarrollo del programa de control del PIC18F8722

Este proceso inicia con una revisión de las tareas que se quieren ejecutar en el algoritmo de control, lo que permite al programador determinar los diversos aspectos involucrados (control analógico/digital, comunicaciones, adquisición, comparación y almacenamiento de datos, entre otros) a nivel de software.

En función de la cantidad y complejidad de los procesos se adopta un criterio de programación, para este proyecto se optó por la “Programación Modular”, que consiste organizar el código en varios módulos los cuales contienen sub-procesos y sub-funciones que son llamados desde el programa principal.

La figura 44 muestra cómo se implementó una estructura modular en el programa de control desarrollado para el PIC18F8722.



Figura 44. Estructura modular del programa del PIC18F8722.

En total se requirieron ocho módulos para realizar las tareas de control de acceso y alarmas, el código escrito en ellos contiene varias rutinas de las librerías antes mencionadas en combinación con el propio lenguaje de BASIC. El programa principal es quien coordina la ejecución de todas las tareas llamando a los procedimientos y funciones contenidos en los demás módulos con el fin de que realicen su contribución en el momento que sea requerido.

A continuación se presenta una breve descripción de las tareas que realiza cada uno de los módulos del programa, al mismo tiempo se detallan las librerías que se utilizaron para su desarrollo:

Declar_Init.mbas: Aquí se declaran las variables requeridas para el control de la pantalla táctil, de igual manera se configuran los pines del PIC dedicados al control del RA6963, Panel táctil y LEDs de la retroiluminación. Se hizo uso de las librerías “**T6963C Graphic Lcd Library, ADC Library y Touch Panel Library**” en la configuración y calibración de la pantalla táctil.

Objects.mbas: Para implementar la interfaz táctil se requiere de un conjunto de imágenes que se dibujan en pantalla, estas contienen información relevante que ayuda a los usuarios a interactuar con el sistema, por ejemplo tenemos:

- | | |
|------------------------------|---------------------------------|
| 1. Pantalla inicial | 5. Cambio de clave |
| 2. Teclados alfanuméricos | 6. Indicación de clave invalida |
| 3. Opciones de usuario | 7. Indicación de clave valida |
| 4. Opciones de administrador | 8. Configuración del RTC |

El modulo de objetos esta dedicado para almacenar estas imágenes en formato de mapa de bit, las cuales están asociadas a arreglos de datos tipo constante, a los que posteriormente se hace llamado durante la ejecución del programa.

DS1307.mbas: Este modulo se encarga de inicializar el DS1307, acá se configuran sus registros con una hora y fecha por defecto, además se incluye una rutina de adquisición y presentación de datos del RTC, la cual llama a procesos de lectura, conversión y formateo de datos del tiempo (creados en “**Share.mbas**”.) para luego mostrarlos en la pantalla grafica del SmartGLCD. El código hace uso de la librería “**Software I²C**” para la lectura/escritura de los registros del RTC. El Anexo C.1 explica el funcionamiento de este protocolo.

Share.mbas: El DS1307 almacena la información del tiempo en formato BCD, para hacer uso de estos datos, el PIC18F8722 lee sus registros y los convierte de BCD a valores decimales, luego los pone a disposición del programa principal para utilizarlos en las diversas tareas que se ejecutan. Un ejemplo claro es la presentación de la hora/fecha en pantalla principal, donde se requiere realizar otra conversión de datos tipo decimal a tipo cadena (caracteres ASCII), además de dar formato a estos registros para su correcta impresión.

Este modulo integra los procesos de lectura, conversión y formateo de datos de tiempo, los cuales pone a disposición de los demás módulos para que se ejecuten cuando se requiera. Las librerías utilizadas son **“Software I²C Library y Conversions Library”**.

Share.mbas también tiene procesos para leer la tabla de usuarios autorizados y sus claves de acceso desde la memoria EEPROM del PIC, luego la carga en arreglos de variables tipo RAM, para esto utiliza la **“EEPROM Library”**.

Hora_Fecha.mbas: Acá se encuentran tres procesos dedicados a implementar la interfaz de usuario para la configuración del RTC, inicialmente se lee e imprime la hora/fecha actual en la pantalla de configuración, al mismo tiempo se dibujan los botones de configuración que permiten modificar los datos, luego el programa entra en un ciclo de lectura del panel táctil para determinar y actualizar los datos que el usuario modifica, posteriormente cuando el usuario acepte una configuración de hora/fecha (presionando el botón guardar), entonces estos datos se guardan en RAM para que otro modulo los mande a escribir en el DS1307 y de esa manera hacer efectivos los cambios de hora/fecha.

En este modulo utilizo las librerías **“T6963C Graphic Lcd Library, ADC Library, Touch Panel Library, Conversions Library y Software I²C Library”**, además de algunas rutina desarrolladas en el modulo **“Share.mbas”**.

MMC_SD.mbas: Este modulo contiene los procesos encargados de crear el registro de eventos, acá se declaran los pines del MCU dedicados a soportar la comunicación SPI (consultar el Anexo C.2) entre la microSD y el PIC18F8722, además se declaran las variables que guardan temporalmente los datos transferidos a la microSD (nombres de usuarios, sensores, hora/fecha).

El primer proceso de este modulo crea diariamente un nuevo archivo en la microSD, este tiene extensión .csv, el cual es compatible con Microsoft Excel. El nombre de este archivo será la fecha del día en que esta siendo creado, lo cual se conoce leyendo los registros del RTC por medio de las rutinas creadas en **“Share.mbas”**.

Posteriormente los eventos se registran de forma indexada durante todo el día, hasta que el sistema determina que debe crear un nuevo archivo con fecha diferente (a las 00:00 horas). No existe forma de sobre-escribir los datos en un mismo archivo (si se extrae la memoria o se reinicia el PIC) debido a que el código detecta si el fichero ya existe y si fuese el caso, el cursor se salta a la última línea, de manera que los datos que habían sido registrados no se pierden.

Una particularidad de este módulo es su capacidad de dar formato “Fat16” a la microSD. Las librerías utilizadas son: **“Multi Media Card library y SPI library”**.

Alarms.mbas: Es aquí donde se realiza la inicialización y gestión de alarmas, por lo tanto, este módulo contiene la declaración de puertos de entrada/salida del PIC que se conectan a los sensores/pulsadores, dispositivos de bloqueo y señalización. Cada pin de entrada/salida tiene asignada una dirección, la cual sirve para determinar cual de los sensores/pulsadores se está habilitando.

El proceso de gestión de alarmas también tiene lugar en este módulo, en él se realiza el monitoreo de los sensores/pulsadores del sistema. Las acciones que toma este proceso dependen de tres factores: 1. *Estado del sistema (Armado, desarmado)*, 2. *Hora/fecha de la incidencia*, 3. *Tipo de evento*. Así por ejemplo, si el sistema está desarmado, no se atienden los eventos producidos por los detectores de intruso, solamente los del detector de incendio, por el contrario, con el sistema armado se da repuesta a todos los dispositivos de detección.

Los fines de semana y días laborales, desde las 10:00 pm hasta las 06:00 am, por cada detección se generaran alarmas locales y remotas, por el contrario durante el día solo se atiende a los detectores de incendio y los pulsadores/contactos del sistema de control de acceso.

Acá se hace uso de las rutinas creadas en los módulos **“MMC_SD.mbas y Share.mbas”**, para registrar los eventos de alarma que se presentan durante el monitoreo de los sensores del sistema. Las librerías utilizadas en el módulo son: **“T6963C Graphic Lcd Library” y “EEPROM Library”**.

Events.mbas: Eventos es el modulo dedicado a implementar las tareas de control de acceso del sistema, este incluye cuatro procedimientos y dos funciones que se describen a continuación:

El proceso Draw_Screen se encarga de dibujar en pantalla los gráficos almacenados en Objects.mbas, así el programa principal llama a este modulo y le envía un parámetro que determina la imagen que se requiere imprimir.

Las funciones Get_Option_AS y Get_Option_US leen las coordenadas del panel táctil y determinan cual es la opción de usuario/administrador que se desea elegir (presentes en la pantalla de usuario o administrador respectivamente).

Get_Key_AN_Keypad es la función que se encarga de adquirir las claves de acceso del teclado alfanumérico, además desde este modulo se puede resetear la clave de administrador (a solicitud del usuario), crear, modificar y eliminar cuentas de usuario.

Val_Code_S1 es la última función y se utiliza para verificar si el código digitado por el usuario se encuentra en la tabla de accesos permitidos del MCU.

Events.mbas hace uso de las rutinas creadas en los módulos Declare_Init, Objects, Alarms y Share. Las librerías utilizadas en el desarrollo del código son: **“T6963C Graphic Lcd Library”**, **“Touch Panel Library”** y **“EEPROM Library”**.

SmartGLCD.mbas: Es en esencia el programa principal del PIC, aquí se realiza la inicialización de todos los procesos y medios requeridos a lo largo del programa (Ej. Inicialización de la comunicación SPI, I²C, RTC, Panel Táctil y la gestión de alarmas), además se desactivan las interrupciones globales y se carga por primera vez la tabla de usuarios del sistema en la memoria RAM del PIC, luego se crea un ciclo en el que infinitamente se realiza la gestión de acceso y alarma.

En su código se integran llamadas a rutinas, procesos y funciones implementados en todos los módulos del programa, esto reduce considerablemente el tamaño del modulo principal.

3.3.1.3 Elaboración de la interfaz grafica con Visual GLCD

Visual GLCD es un software de desarrollo utilizado para crear sistemas basados en interfaz grafica, su librería integra varios tipos de controladores matriciales, lo que permite implementar aplicaciones en varios tipos de pantallas GLCD con Panel Táctil. Este software genera código fuente compatible con todos los compiladores de microelectrónica, lo que lo hace una útil herramienta para desarrollar aplicaciones graficas controladas por MCU.

En este proyecto se hizo uso de Visual GLCD para crear todas las pantallas de usuario de la interfaz de control de acceso y alarmas.

Procedimiento para crear las pantallas de usuario

- 1- Hacer un bosquejo de lo que se quiere expresar en papel.
- 2- Dibujarlo en lógica negativa con la ayuda del software PAINT.

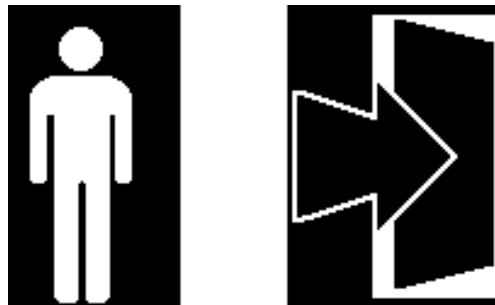


Figura 45. Gráficos en lógica negativa para Visual GLCD.

- 3- Guardar la imagen con formato de mapa de bit (BMP).

Imágenes .bmp son requeridas porque MikroBASIC solo permite interpretar gráficos de este formato, los cuales convierte en código de BASIC.

- 4- Configurar Visual GLCD para editar la imagen.

Esto se logra creando un nuevo archivo en Visual GLCD, luego en el menú de selección de hardware se elije al SmartGLCD, con esta información el software conoce la resolución, tipo de controlador, puertos requeridos, calibración el Panel Táctil, PIC utilizado y demás parámetros de operación.

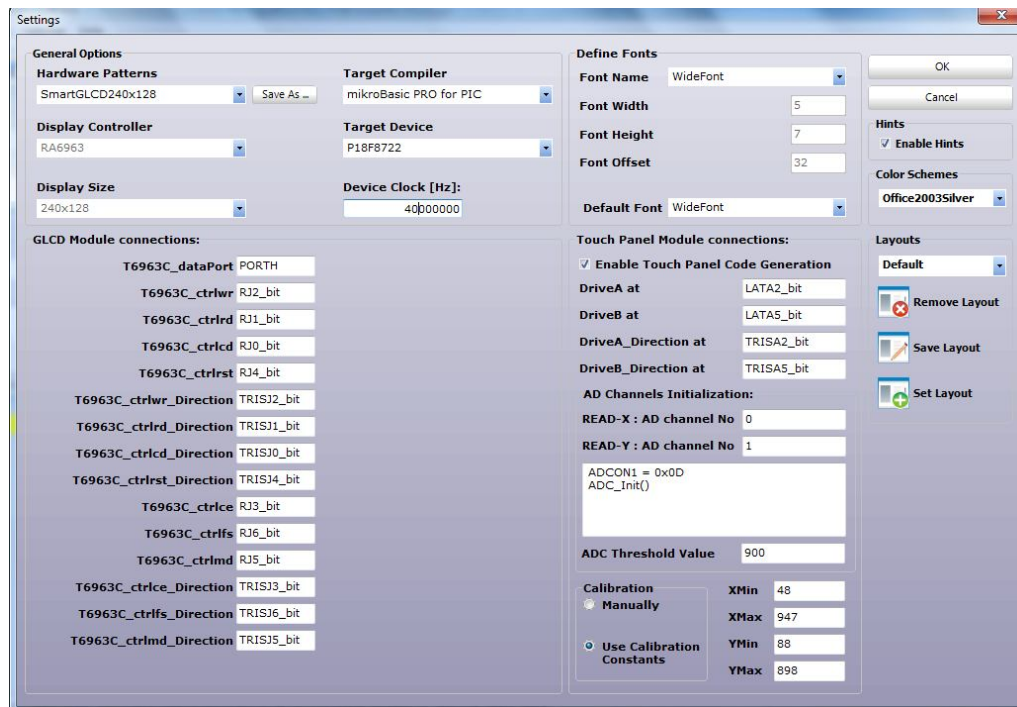


Figura 46. Menú de configuración de Visual GLCD.

Posteriormente se carga la imagen para verificar que se ajusta a las dimensiones de la pantalla, si no fuese así, el software permite editar la imagen, de manera que se puede modificar tamaño, agregar botones, efectos u otro tipo de atributos. Luego se copian las coordenadas que ocupa la imagen en la matriz del SmartGLCD (esto es útil a la hora de imprimir) y se procede a guardarla con formato .bmp.

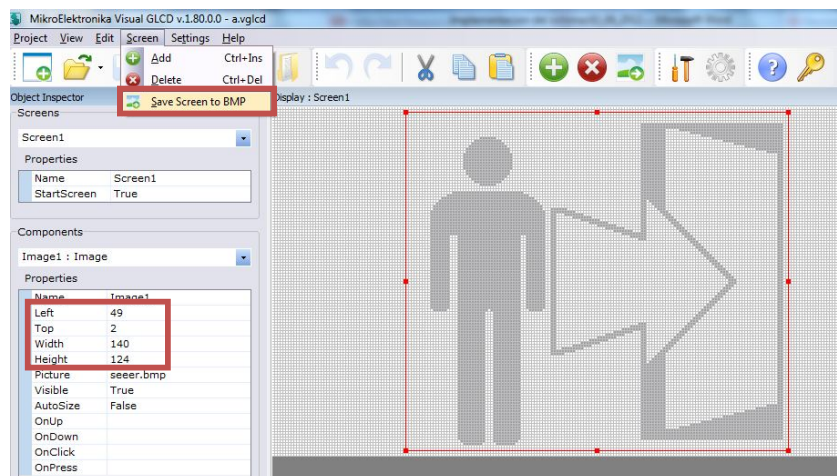


Figura 47. Coordenadas de la imagen editada.

Ejecutando la aplicación GLCD Bitmap Editor se configura el tipo de controlador (T6963C), resolución de la pantalla y compilador utilizado, luego se carga la imagen guardada para que la aplicación genere una constante tipo arreglo que contiene el código de la imagen en lenguaje de BASIC.



Después de realizar la copia del código en el modulo Objects.mbas finalmente se manda a llamar la imagen utilizando el comando **T6963C_PartialImage(constante).**

A red rectangular emergency exit sign. At the top, the text "EMPUJE LA PUERTA" is written in white capital letters. Below the text is a white graphic of a stylized human figure standing next to a door, with a large white arrow pointing to the right, indicating the direction to push the door open.

87

3.3.1.4 PROTEUS 7.10

PROTEUS es una SUITE de programas para diseño y simulación de circuitos electrónicos, este consta de tres aplicaciones principales:

ISIS (Intelligent Schematic Input System): Es el programa que se utiliza para diseñar el esquema eléctrico del circuito que se desea realizar.

VSM (Virtual System Modeling): Es un modulo asociado a ISIS que permite simular los circuitos en tiempo real (incluyendo MCU y MPU).

ARES (Advance Routing Modeling): Es el software que se utiliza en el diseño PCB, permite la edición, elaboración de pistas y ubicación de los componentes en forma manual y automática (exportando el esquema desde ISIS).

3.3.1.4.1 Simulación y depuración de errores con ISIS (MMC, RTC, GLCD)

Durante el proceso de programación, el software ISIS fue una excelente herramienta de evaluación, debido a que permitió simular los diferentes dispositivos y componentes integrados en el sistema, de manera que sin necesidad de exponer el hardware adquirido, se realizó la verificación y corrección de errores del programa, emulando de forma virtual su comportamiento, además se elaboraron los diagramas de circuito, para posteriormente fabricarlos de forma artesanal.

La siguiente imagen ha sido extraída de una simulación realizada con ISIS, en ella se muestran algunos resultados obtenidos de la programación del PIC18F8722 para el control de la pantalla grafica y el DS1307. Además de estos dispositivos, ISIS permitió emular el comportamiento las memorias de almacenamiento (microSD y EEPROM interna) y periféricos de entrada/salida que forman parte del sistema de seguridad.

SISTEMA DE SEGURIDAD ELECTRONICA

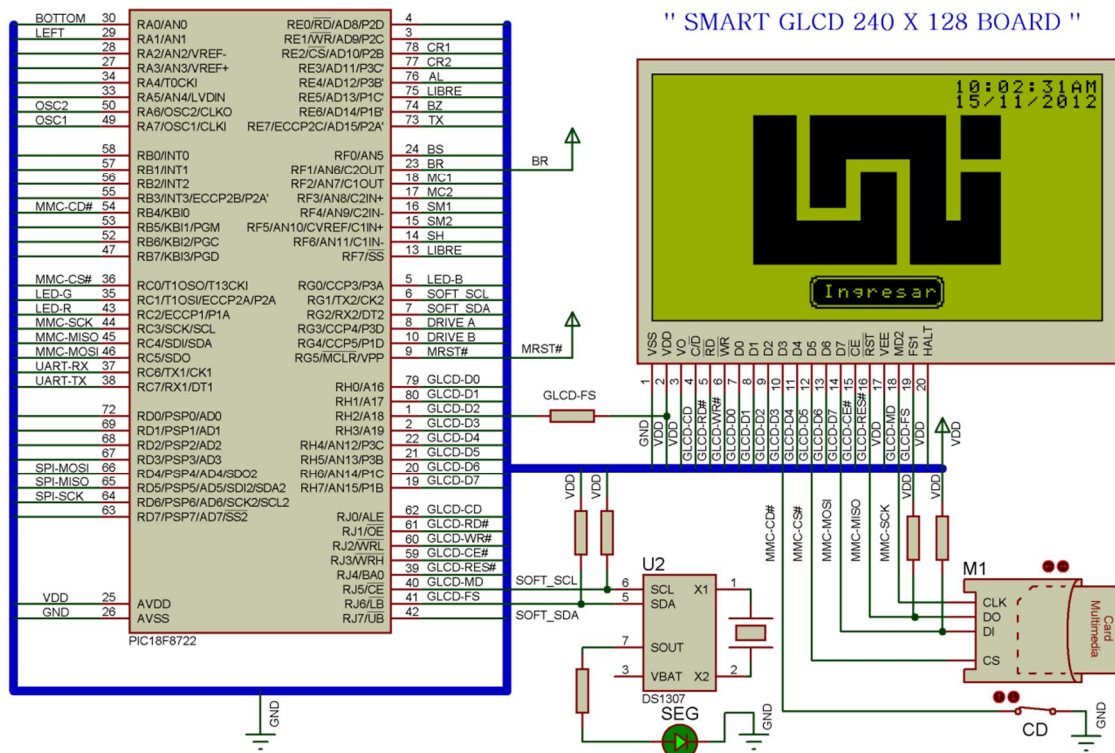


Figura 50. Simulación del SmartGLCD240x128Board.

3.3.1.5 Resultados de la programación del SmartGLCD

Al finalizar la etapa de programación se logro integrar todas las tareas propuestas en la memoria del PIC, a continuación se muestran algunos de los resultados obtenidos de la implementación práctica de este prototipo:

Pantalla principal: Es la pantalla de inicio de la interfaz de usuario, muestra la hora/fecha, el logo de la UNI y un botón de función: *'Ingresar'*, al presionarse este botón, se inicia el proceso de autenticación. La luz de la pantalla se desactiva después de 5 segundos de ocio y se activa al presionar la pantalla.



Figura 51. Pantalla de inicio.

Pantalla de Autenticación: Por medio de un teclado Querty (Keypad) cada usuario digita su código de acceso, este se compara con la tabla del personal autorizado que esta en la EEPROM del PIC y luego se valida como: usuario, administrador o intruso, ejecutando una acción diferente para cada caso.



Figura 52. Teclado alfanumérico.

Pantalla de código inválido: Si un usuario digita mal su clave, el microcontrolador determinara que no esta autorizado y por lo tanto mantendrá bloqueada la cerradura, además se imprime un mensaje en pantalla indicándole que el código de acceso es incorrecto.



Figura 53. Código invalido.

Pantalla de usuario: Si el código se valida como autorizado, el sistema muestra el nombre de usuario a quien pertenece la cuenta y le brinda tres opciones: Ingresar al local, cambiar su código de usuario y salir del sistema.



Figura 54. Pantalla de usuario.

La opción '**cambiar código**' lee y guarda una nueva clave de acceso para la cuenta, esta función mostrara un teclado alfanumérico (ver figura 52) y un mensaje solicitando el nuevo código. '**Salir**' es un salto a la pantalla principal.

Opción ingresar: Al presionar el botón Ingresar ubicado en las opciones de usuario/administrador, el sistema libera la cerradura, temporiza el ingreso al local (5 segundos), guarda el nombre del usuario con la hora y fecha de ingreso en el registro de eventos (en un archivo de Excel) y vuelve a la pantalla de inicio.



Figura 55. Pantalla de ingreso.

Pantalla de administrador: Se presenta cuando se determina que el código pertenece al administrador del sistema, desde acá se realizan las mismas funciones de un usuario común, más la posibilidad de configurar el RTC, activar/desactivar las alarmas, crear, modificar y eliminar cuentas de usuario.



Figura 56. Pantalla de administrador.

Configuración de hora y fecha: Al ejecutar esta función, el MCU lee y muestra los valores del RTC (ver figura 57), luego el administrador cambia estos datos (utilizando las flechas) hasta establecer la hora/fecha requerida y confirma la escritura de estos utilizando el botón GyR (Guardar y Regresar).



Figura 57. Configuración del RTC.

Los dos puntos se ubican sobre el valor que esta siendo modificado, la flecha de retorno se utiliza para descartar los cambios realizados y salir del modo configuración.

Gestión de cuentas: Para agregar un nuevo usuario el administrador se ubica en una posición de memoria disponible donde se alojaran los datos de la cuenta, esto se realiza navegando con las flechas ↑ ↓ del teclado. Para digitar el nombre de usuario se hace uso de los caracteres alfanuméricos y luego se reinicia la clave (Re).



Figura 58. Gestión de cuentas.

El código por defecto después de un reinicio es: “000000”, de manera que el nuevo usuario debe cambiar su código al ingresar por primera vez. Las cuentas creadas pueden ser modificadas o eliminadas por el administrador, para lograrlo basta con realizar cambios o borrar por completo los datos de una cuenta.

Activación de Alarmas: El administrador también puede activar/desactivar el sistema de alarmas, con el sistema armado, la luz de fondo permanece en rojo, esto indica que esta activo el monitoreo de los detectores de intruso, por el contrario, este permanece en amarillo cuando se ha desarmado el sistema.



Figura 59. Sistema armado.

Registro de eventos

Una de las tareas críticas que se plantearon en el algoritmo propuesto fue implementar un registro de los eventos que se presentan en el sistema.

Esta tarea se cumplió satisfactoriamente gracias a dos factores importantes:

1. El SmartGLCD integra un lector de microSD, por lo tanto no fue necesario adquirir, ni acoplar un lector de tarjetas externo.

2. MikroBASIC PRO incluye un paquete de librerías para trabajar con memorias SD, además de rutinas para manipular archivos utilizando FAT16 (File Allocation Table 16). Esto permitió implementar el registro de eventos utilizando ficheros de tipo .CSV (Comma Separated Value), los cuales generan tablas de datos compatibles con Microsoft Excel, tal y como se ilustra el siguiente ejemplo.



	A	B	C	D
1	REGISTRO DE ACCESOS Y ALARMAS DEL DEPARTAMENTO DE ELECTRONICA			
2				
3	FECHA	HORA	NOMBRE	ALARMA
4	15/11/2012	08:20:52PM	MILTON_ZELEDON__	
5	15/11/2012	09:20:52PM		HUMO EN LA SALA
6	15/11/2012	10:20:52PM	FRANCISCO_LOPEZ_	
7	15/11/2012	11:20:52PM		MOVIMIENTO SALA1
8	15/11/2012	12:20:52PM		PUERTA 1 ABIERTA
9	15/11/2012	08:20:52PM	MILTON_ZELEDON__	
10	15/11/2012	09:20:52PM		HUMO EN LA SALA
11	15/11/2012	10:20:52PM	FRANCISCO_LOPEZ_	
12	15/11/2012	11:20:52PM		MOVIMIENTO SALA1
13	15/11/2012	12:20:52PM		PUERTA 1 ABIERTA
14				

Figura 60. Registro de eventos compatible con Microsoft Excel.

Programación de los MCU del Subsistema de Señalización Remota

Los rPIC12F675F y PIC6F676 integrados en el transmisor y tarjeta de recepción se programaron para transmitir y validar una condición de alarma (dato) bajo el protocolo de comunicación Keelog (codificación de línea).

La programación de estos dispositivos se realizó en el software MPLAB de Microchip, este permite desarrollar aplicaciones para PIC en lenguaje ensamblador. Los programas desarrollados están compuestos por un solo módulo principal debido a que no son demasiado extensos.

Para simular la lógica de operación de este subsistema se utilizó ISIS de Proteus, el cual permitió verificar la correcta implementación del protocolo.

3.3.2 Diseño y Fabricación del Hardware requerido

Para implementar este prototipo fue necesario elaborar los circuitos impresos de las Tarjetas de Control del Reloj, Interfaz de Entrada, Interfaz de Salida e Interfaz de Recepción de Alarmas. En el Anexo D.1 se documenta el proceso. Como resultado se obtuvo los PCB ilustrados a continuación:

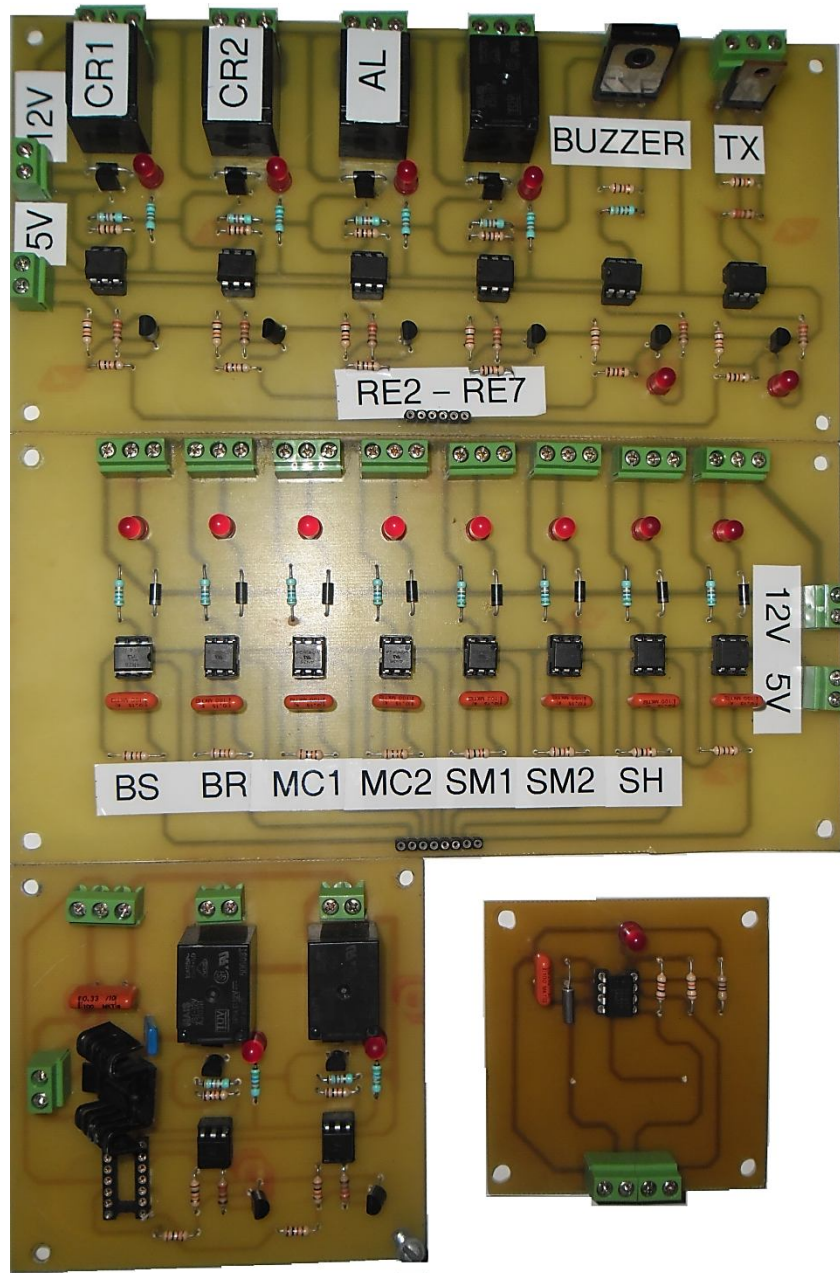


Figura 61. Tarjetas electrónicas fabricadas.

3.3.3 Instalación y montaje del sistema

A continuación se presentan los aspectos más relevantes de la instalación del Sistema de Seguridad en el Departamento de Electrónica:

1. La pantalla táctil se instaló en la pared ubicada a la derecha de la entrada principal, a una altura de 1.4 mts sobre el nivel de piso terminado. A lo interno de esta pared se encuentra empotrado el Panel de Control, el cual aloja al SmartGLCD, las Tarjetas Electrónicas de Interfaz y PCB del Reloj.
2. En la parte superior de la puerta izquierda (vista desde afuera) se instaló la cerradura electromagnética de 600 Lbs, el cableado y montaje de este dispositivo quedó a lo interno del local para impedir que sea deshabilitada.
3. A la derecha de la puerta de ingreso (internamente) se encuentra el botón de salida, esta ubicado a 1.1 metros de altura. Además se instalaron dos botones de salida en paralelo que permiten liberar la puerta desde el cubículo del Jefe del Departamento y el del Administrador del Sistema.
4. Se instalaron tres sensores de movimiento ubicados estratégicamente para interceptar intrusos desplazándose a través de sus zonas de detección, el fabricante recomienda esta posición para mejorar la sensibilidad.
5. El detector de humo se instaló en el centro del cielo falso del departamento, según las especificaciones técnicas del fabricante, su radio de detección es adecuado para brindar protección a todo el departamento.
6. Las fuentes de alimentación y UPS no están al alcance de los usuarios, el propósito es que no sean fácilmente quebrantadas por intrusos.
7. El Transmisor de RF se encuentra instalado en la azotea del edificio de la FIQ, el cual establece un enlace con línea de vista hacia el receptor, ubicado en la pared exterior sur de la caseta del personal de seguridad.
8. En la caseta de guardianía se instaló el panel que contiene la Interfaz de Recepción y Activación de Alarmas, junto a su fuente de poder. En la pared exterior este de esta misma caseta se instaló la Alarma Remota.

En las siguientes figuras se ilustra la instalación física del sistema:

3.4 PRUEBAS DE FUNCIONAMIENTO Y CORRECCION DE ERRORES

Durante esta fase se realizaron las pruebas de operación al sistema, con el objetivo de certificar su correcto funcionamiento, además de identificar oportunidades de mejoras. A continuación se exponen los problemas corregidos.

- **El RTC no arranca o se queda congelado**

Este problema era provocado por falta conexión a tierra (GND), para superarlo se alimentó las fuentes desde una red eléctrica con sistema de puesta a tierra.

- **El RTC se descontrola y la MMC no guarda correctamente**

Ante un evento de acceso/alarma el sistema guardaba un registro (hora/fecha, nombre o alarma) en la microSD con los datos de tiempo y caracteres erróneos, el error era provocado por un conflicto en el uso de las librerías SPI y Software I²C (microSD y RTC), debido a que utilizan el mismo temporizado para su señal de reloj. El problema se resolvió inicializando cada protocolo antes de utilizarse.

- **Se presentan falsas alarmas locales**

La sirena audible se activaba sin que hubiese condición de alarma alguna. Esta anomalía era producida por el mal contacto entre los opto-acopladores y sus sockets, para corregirlo se cambiaron las bases de estos dispositivos.

Periodo de pruebas

Luego de corregir los errores de funcionamiento, el sistema se sometió a 15 días de pruebas, con el objetivo de que los usuarios (docentes) pudieran proponer mejoras al sistema, las cuales fueron implementadas en la siguiente secuencia:

- **Mejoras a la interfaz de usuario**

Inicialmente se propuso un teclado numérico para solicitar la clave de acceso. Sin embargo se determinó que esta forma de autenticación no tenía un buen nivel de seguridad, por lo tanto se desarrolló un algoritmo de gestión de acceso que solicitaba un nombre de usuario y su código en un teclado alfanumérico.



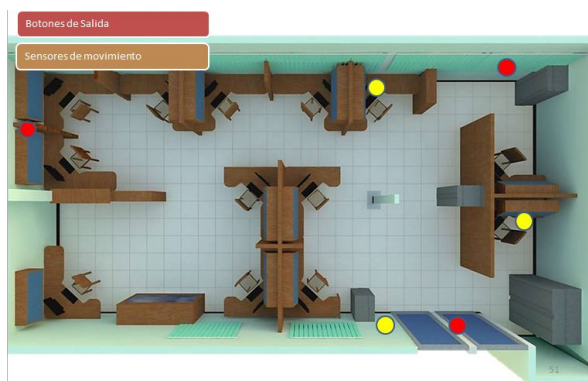
Figura 63. Pantallas de autenticación anteriormente propuestas utilizando:
a) Teclado numérico, b) Teclado alfanumérico.

Esta propuesta aportaba mayor seguridad al proceso de autenticación, por lo tanto, se sometió a pruebas durante una semana. La experiencia de los usuarios reveló que el procedimiento era muy largo y recomendaron solicitar únicamente la clave de acceso, la cual se vincularía automáticamente con el nombre del usuario a quien le pertenece, además propuso que se implementara un teclado tipo Qwerty y que se suprimiera del mismo la tecla de **Enter** (↵).

Tomando en cuenta la recomendación de los usuarios finales se desarrolló el modo de autenticación final implementado en la pantalla de la figura 52.

• Detectores de movimiento

Inicialmente se instaló un sensor de movimiento en la entrada, pero se verificó que no cubría toda el área del departamento, por lo tanto, se instalaron dos unidades más, ubicados estratégicamente para maximizar la sensibilidad de detección.



Detectores (rojo). Botones (amarillo)

Botones de Salida

Además de botón de salida que está junto a la puerta, se instalaron dos más, uno en el escritorio del Jefe de Departamento y otro en el del Administrador del Sistema, para brindar acceso a personas que lleguen de visita al departamento.

3.4.1 Resultados

El resultado de este proyecto fue un Sistema de Control de Acceso y Alarma Contra Intrusos instalado y probado y optimizado en el Departamento de Electrónica. A continuación se listan las características del prototipo elaborado:

- Como cerebro del sistema se utiliza un SmartGLCD, el cual contiene todos los componentes de software y hardware necesarios para realizar las tareas de: Gestión de Acceso, Gestión de Alarmas y Registro de Eventos.
- Se implementa una interfaz táctil para realizar los procesos de autenticación y administración del sistema de forma rápida y eficiente.
- El sistema de gestión (algoritmo) reconoce dos tipos de cuentas:
 - Cuenta de Administrador: Tiene control completo para ingresar, cambiar su código, configurar la hora/fecha, administrar cuentas de usuario y habilitar alarmas.
 - Cuenta de usuario: Solamente puede ingresar y cambiar su código.
- Cuando un usuario ingresa al local, se libera la puerta y se registra su información junto a la hora/fecha de entrada.
- Durante un evento de acceso se activa un zumbador que emite un tono audible cuando se agota el tiempo de ingreso y la puerta aun esta abierta.
- Tres sensores de movimiento instalados en posiciones estratégicas permiten garantizar un alto nivel de detección dentro del área resguardada.
- Un sensor de humo ubicado en el centro del salón detecta indicios de incendio, ante tal evento, el sistema libera la puerta y genera alarmas.
- Con la detección de intrusos/incendios habilitada el sistema se arma y desarma automáticamente siguiendo una calendarización predefinida.
- Se envían alarmas remotas a la caseta de los CPF utilizando transmisores y receptores de RF, las cuales utilizan PIC como dispositivos de control.
- El sistema crea diariamente un fichero .CVS (compatible con Microsoft Excel) en el cual se almacenan todos los eventos de acceso y alarmas.
- El suministro eléctrico cuenta con el respaldo de una UPS de 750 VA capaz de garantizar una autonomía de 4 horas durante operación normal.

3.4.2 Costos del prototipo

A continuación se presentan los costos de los dispositivos y materiales utilizados en la implementación del prototipo, estos precios disminuyen cuando se realizan compras por cantidades mayores. No obstante, existen factores no cuantificados en la tabla 14, que impactan directamente en el costo real del prototipo, tales como: costo de desarrollo, herramientas de diseño, e instalación, entre otras.

Tabla 14: Costos de implementación del prototipo.

Modelo	Descripción	Cant	C/U U\$\$	Total U\$\$
SmartGLC D 240 x128	Pantalla Táctil inteligente, incluye: MCU, Lector de Memoria microSD, puerto USB y LEDs de retroiluminación.	1	120	120
---	Memoria microSD de 2GB.	1	9	9
Tarjeta 1	Interfaz electrónica de entrada.	1	30	30
Tarjeta 2	Interfaz electrónica de salida.	1	40	40
Tarjeta 3	Interfaz de recepción y activación de alarma.	1	30	30
Tarjeta 4	Circuito para interactuar con el RTC DS1307.	1	12	12
ECL-ACC300	Cerradura Electromagnética de 600 Libras.	1	90	90
---	Pulsadores para solicitar salida.	3	3	9
---	Contactos magnéticos para puerta.	2	1.5	3
BV-300	Sensor de movimiento PIR.	3	18	54
FSA-410B	Sensor de humo fotoeléctrico.	1	40	40
SD15WULF	Sirena audible de uso interior, 15W.	1	15	15
SPL	Sirena piezoeléctrica de uso exterior, con luz estroboscópica.	1	15	15
rfPIC12F675	Transmisor RF, ASK, 433.92 MHz.	1	36	36
rfRXD0420	Receptor RF, ASK, 433.92 MHz.	1	30	30
CFM40T-02	Fuente de alimentación 5V, 40W.	1	40	40
S-60-12	Fuente de alimentación 12V, 60W.	1	50	50
ST-2406-2	Fuente de alimentación 12V, 24W, con adaptador y batería incluido.	1	56	56
SL-761	UPS 120V, 375W, 750VA.	1	70	70
Legrand	Cajas plásticas con protección IP55 para montaje de paneles de control, fuentes, transmisor y receptor.	5	---	95
---	Rollo de cable # 22AWG de 4 hilos.	1	25	25
---	Ducto conduit con sus accesorios.	25	1	22
---	Gastos varios de instalación.	1	9	9
	TOTAL DE GASTOS EN DOLARES		U\$\$	900

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En base a los objetivos que fueron propuestos durante la fase inicial de este proyecto y los resultados obtenidos se llego a las siguientes conclusiones:

- El sistema de seguridad electrónica desarrollado integra medios de software y hardware que ejecutan tareas para mejorar la seguridad del departamento. Por tanto, después de realizar pruebas de campo al sistema instalado, se logro comprobar su valioso aporte a la detección de intrusos/incendios así como el control del personal que ingresa al local.
- El Sistema de Control de Acceso y Alarmas desarrollado responde a los requerimientos del departamento y sus usuarios, de manera que integra las características y funcionalidades descritas en los objetivos propuestos.
- La lógica de control del sistema principal y demás subsistemas se logro implementar utilizando tecnología de microcontroladores PIC, lo cual proporcione gran flexibilidad para programar las tareas y acciones de control así como para interactuar con otros dispositivos de hardware del sistema.
- El mecanismo de autenticación y monitoreo de alarmas implementado tiene bajos costos operativos. Por ejemplo, en el sistema se puede agregar o eliminar usuarios utilizando la gestión de cuentas, lo cual no tiene ninguna implicación económica, de igual forma se podría incrementar el número de detectores o sustituir sensores averiados sin cambiar el hardware utilizado.
- Este trabajo monográfico permitió a los autores desarrollar competencias en el diseño e implementación de: Sistemas de seguridad electrónica, sistemas basados en microcontroladores PIC, Tarjetas de circuito impreso, transmisión/recepción de datos a través de RF, además de adquirir nuevas habilidades en simulación, programación de PIC e instalaciones eléctricas.
- El contenido teórico-practico del presente trabajo monográfico puede ser de utilidad para estudiantes de ingeniería que deseen investigar y ampliar sus conocimientos en diseño de sistemas basados en microcontroladores PIC.

Recomendaciones

A continuación se presentan algunas recomendaciones orientadas a mejorar las prestaciones del prototipo desarrollado:

- Instalar detectores de intrusos e incendios en las áreas adjuntas al departamento, integrarlos a la gestión de alarmas del sistema desarrollado.
- Agregar al sistema capacidad de control sobre los dispositivos de climatización (aires) e iluminación, para reducir el consumo de energía e incrementar a vida útil de los equipos. “Esto se puede lograr apagándolos automáticamente cuando no haya ocupantes en el departamento”.
- Adicionar al SmartGLCD software y hardware de comunicación Ethernet, para desarrollar una aplicación web que permita el monitoreo, control, configuración y almacenamiento de los registros del sistema desde internet.
- Instalar una cámara IP conectada a internet para visualizar y confirmar de forma remota los eventos que determina el sistema de seguridad.
- Agregar al sistema un modem SMS compatible con microcontroladores PIC, realizar la programación requerida para habilitar funciones de monitoreo y control a través de mensajes de texto, directamente desde un celular.
- Desarrollar un sistema de seguridad centralizado basado en PC, capaz de monitorear y controlar sistemas autónomos (replicas del prototipo desarrollado) instalados en los laboratorios y oficinas de la FEC, de manera que se pueda resguardar y disminuir el consumo energético en estas áreas.
- Realizar un estudio de mercado para averiguar si existe demanda de parte de la población para el sistema desarrollado, cuales son las expectativas de compra y que monto esta dispuesto a pagar un cliente promedio, para luego determinar la rentabilidad de producir este sistema en mayores volúmenes.

BIBLIOGRAFIA

Robert L. Pearson, Electronic Security Systems; Elsevier, Burlington, USA, 2007.

Philip Walker, Electronic Security Systems; Newnes, London, England, 1998.

Bill Phillips, Master Locksmithing; McGraw-Hill, e-book, USA, 2008.

Gerard Honey, Intruder Alarms, Newnes, Burlington, USA, 2003.

Access Control, 2012. Obtenido de: http://en.wikipedia.org/wiki/Access_control

Card Reader, 2011. Obtenido de: http://en.wikipedia.org/wiki/Card_reader

SmartGLCD 240x128 User Manual; Mikroelectronica, UK, 2011.

Dogan Ibrahim, Using Touch Screen LCDs In Embedded Applications; Electronics World, Near East University, Cyprus, 2010.

RA6963 Dot Matrix LCD Controller Spacification V1.3; RAIO Tecnology Inc, Taiwan, 2008.

Dusan Mihailovic, De acuerdo ahora necesitas una Pantalla Tactil; Mikroelectronica, UK.

Enrique Palacios, Microcontrolador PIC16F84 “Desarrollo de Proyectos”; Alfaomega, Madrid, España, 2004.

Dogan Ibrahim, Advance PIC Microcontroller Projects in C; Newnes, Burlington, USA, 2008.

Juan Clavijo, Diseño y Simulación de Sistemas Microcontrolados en Lenguaje C; Colombia, 2011.

ANEXOS

ANEXO A: FUNCIONAMIENTO DE LOS DISPOSITIVOS INTEGRADOS EN SMARTGLCD 240x128 BOARD

A.1. Funcionamiento de una pantalla de cristal líquido (LCD).

Un LCD es una pantalla delgada y plana formada por una matriz de píxeles en color o monocromos delante de una fuente de luz.

Cada pixel está formado de una capa de moléculas de cristal líquido alineadas entre dos electrodos transparentes, dos filtros de polarización y los ejes de transmisión tal y como se ilustra en la figura 64.

Las moléculas de cristal son tratadas con campos eléctricos a través de los electrodos para bloquear o permitir el paso de la luz a la superficie reflectante, la cual devuelve la luz al espectador. Los filtros de polarización horizontal y vertical se encargan de dejar pasar el color de luz deseado.

Para controlar la activación de los píxeles toda pantalla cuenta con un controlador matricial que es capaz de aplicar voltaje (campo eléctrico) de forma organizada a cada pixel para poder representar caracteres o imágenes.

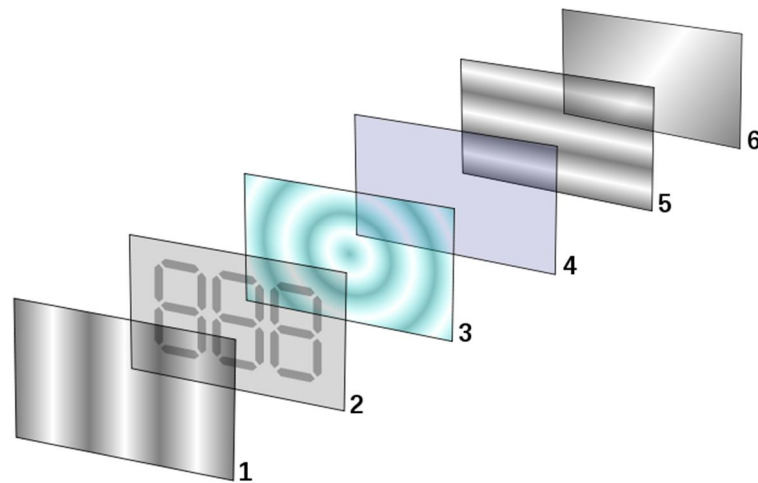


Figura 64. 1:Filtro vertical, 2: Electrodos (sus formas determinan los píxeles que se mostrarán), 3: Cristales líquidos, 4: Electrodo común, 5: Filtro horizontal, 6: Superficie reflectante (no incluida cuando la pantalla incluye retroiluminación).

A.2. Controlador RA6963.

El RA6963 fue desarrollado por **RAIO Technology Inc** y es completamente compatible con el tradicional controlador **T6963C** de **Toshiba**.

Está diseñado para controlar varios formatos de pantallas que se ajustan a sus especificaciones e integra un bus de datos paralelo de 8 bits y líneas de control para lectura y escritura a través de un MPU/MCU.

Las principales características de este controlador son:

- Soporta formatos de pantallas de:
Columnas: 32, 40, 64, 80.
Filas: 2, 4, 6, 8, 10, 12, 14, 16, 20, 24, 28, 32.
- Interfaz de 8 bits para procesadores 8080.
- Generador de caracteres de 256 palabras.
- Memoria ROM de caracteres ASCII, Japonés y numéricos.
- Soporta modo texto, modo gráfico y una combinación de ambos.
- Tamaño de la fuente Vertical: 8 y horizontal entre 5, 6, 7 y 8 pixeles.
- Soporta fuente **negrita** y efecto de inversión de los datos de la pantalla.

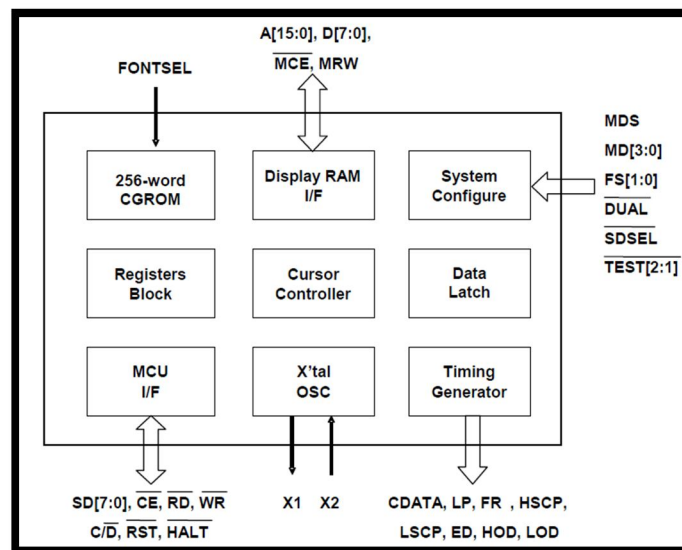


Figura 65. Diagrama en bloques del RA6963.

Los registros más relevantes del RA6963 son los de interfaz con el MCU y configuración del sistema. La siguiente tabla describe estos pines y su función.

Tabla 15: Descripción de los pines del RA6963.

Nombre	E/S	Descripción															
SD[7...0]	E/S	Bus de datos: Bus para transferencias de datos entre el MCU y RA6963.															
RD	E	Control de lectura: Señal de lectura de datos. Cuando está en bajo, el MCU lee los datos del RA6963.															
WR	E	Control de escritura: Señal de escritura de datos. Cuando está en bajo, el MCU escribe datos en el RA6963.															
C/D	E	Selector de comando/dato: Señal para indicar al RA6363 si se le enviara un dato o un comando desde el MCU. <table><tr><td>C/D</td><td>WR = Low</td><td>RD = Low</td></tr><tr><td>1</td><td>Escritura comando</td><td>Lectura de estado</td></tr><tr><td>0</td><td>Escritura de dato</td><td>Lectura de dato</td></tr></table>	C/D	WR = Low	RD = Low	1	Escritura comando	Lectura de estado	0	Escritura de dato	Lectura de dato						
C/D	WR = Low	RD = Low															
1	Escritura comando	Lectura de estado															
0	Escritura de dato	Lectura de dato															
CE	E	Chip Habilitado: Habilitación del RA6963, cuando el MCU se comunica con el RA6963 CE = Low.															
FS[1:0]	E	Selección de fuente: <table><tr><td>FS0</td><td>H</td><td>I</td><td>H</td><td>L</td></tr><tr><td>FS1</td><td>H</td><td>H</td><td>L</td><td>L</td></tr><tr><td>Fuente</td><td>5x8</td><td>6x8</td><td>7x8</td><td>8x8</td></tr></table>	FS0	H	I	H	L	FS1	H	H	L	L	Fuente	5x8	6x8	7x8	8x8
FS0	H	I	H	L													
FS1	H	H	L	L													
Fuente	5x8	6x8	7x8	8x8													
MD	E	Selección del tamaño del GLCD															
RST	E	Señal de reinicio: RST = Bajo > RA6963 se reiniciara. RST = Alto > Modo normal.															
VCC	P	Alimentación, 5V _{DC}															
GND	P	Tierra, 0V _{DC}															

A.3. Funcionamiento de un panel táctil resistivo.

Un panel táctil resistivo está compuesto por tres capas alineadas de forma horizontal como se ilustra en la figura 66.

- La capa inferior es un vidrio cubierto con una solución resistiva de óxido de indio y estaño (ITO).
- La capa superior es una lámina de plástico flexible de tereftalato de polietileno (PET) cubierta con una solución resistiva de ITO.
- Las capas conductoras están separadas por un espaciador de micropunto para evitar contacto entre las dos capas hasta que se presione el panel.

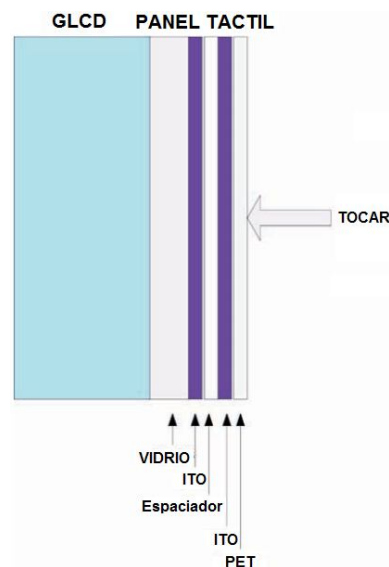


Figura 66. Panel táctil resistivo.

Los lados opuestos de las láminas del panel disponen de contactos para acceder a una faja de cuatro hilos de cables flexibles que se utilizan para suministrarle y leer un voltaje (usualmente de 0 - 5V_{DC}) del panel.

El procedimiento para determinar las coordenadas del punto (x,y) donde se presionó el panel se puede dividir en dos pasos:

Determinación de coordenada X: Se conecta el contacto izquierdo de la superficie X a 0V y el derecho a Vcc, de esta manera se obtiene un divisor de tensión, donde el valor del voltaje de salida se puede leer desde el contacto inferior de la superficie Y y es proporcional a la distancia en el eje horizontal. Este voltaje se digitaliza con un ADC para procesarlo y obtener la coordenada X.

Determinación de coordenada Y: Se conecta el contacto inferior de la superficie Y a 0V y el superior a Vcc. El principio es el mismo y en este caso la lectura de la tensión se tomara del contacto izquierdo de la superficie X.

Las siguientes figuras muestran en detalle la estructura de un panel táctil resistivo y la relación del voltaje con las coordenadas del punto presionado.

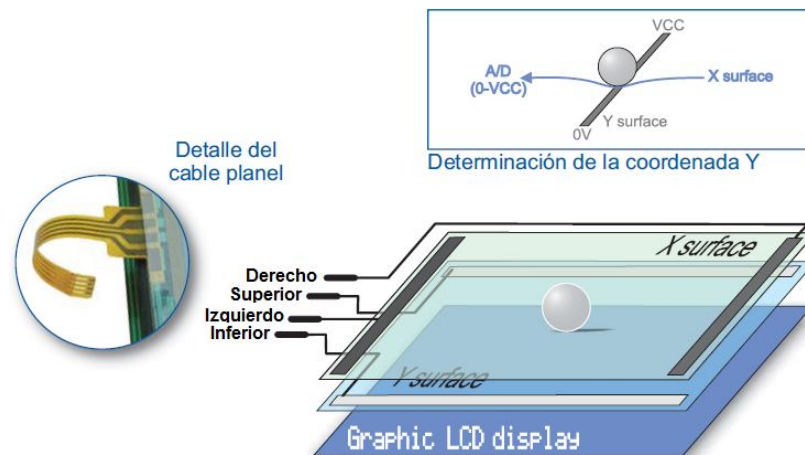


Figura 67. Estructura de un panel táctil resistivo.

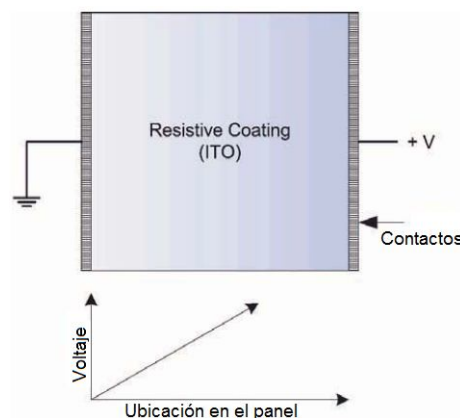


Figura 68. Gradiente de voltaje de una capa resistiva.

A.4. Funcionamiento del controlador de panel táctil resistivo.

El controlador de panel táctil del SmartGLCD está conectado a través de cuatro hilos al PIC18F8722 así como se ilustra en la figura 69, su función es acoplar los contactos de la Superficie X y la Superficie Y a los voltajes de V_{CC} y 0V una a la vez para que el MCU pueda realizar la adquisición.

Los pines RG3 (DRIVEA) y RG4 (DRIVEB) del PIC se configuran como salidas digitales, el programa de control de MCU los pondrá en 5V o 0V en función de la superficie que se desee habilitar, mientras que los pines RA0 (BOTTOM) y RA1 (LEFT) se configuran como entradas analógicas para digitalizar la lectura de voltaje del panel.

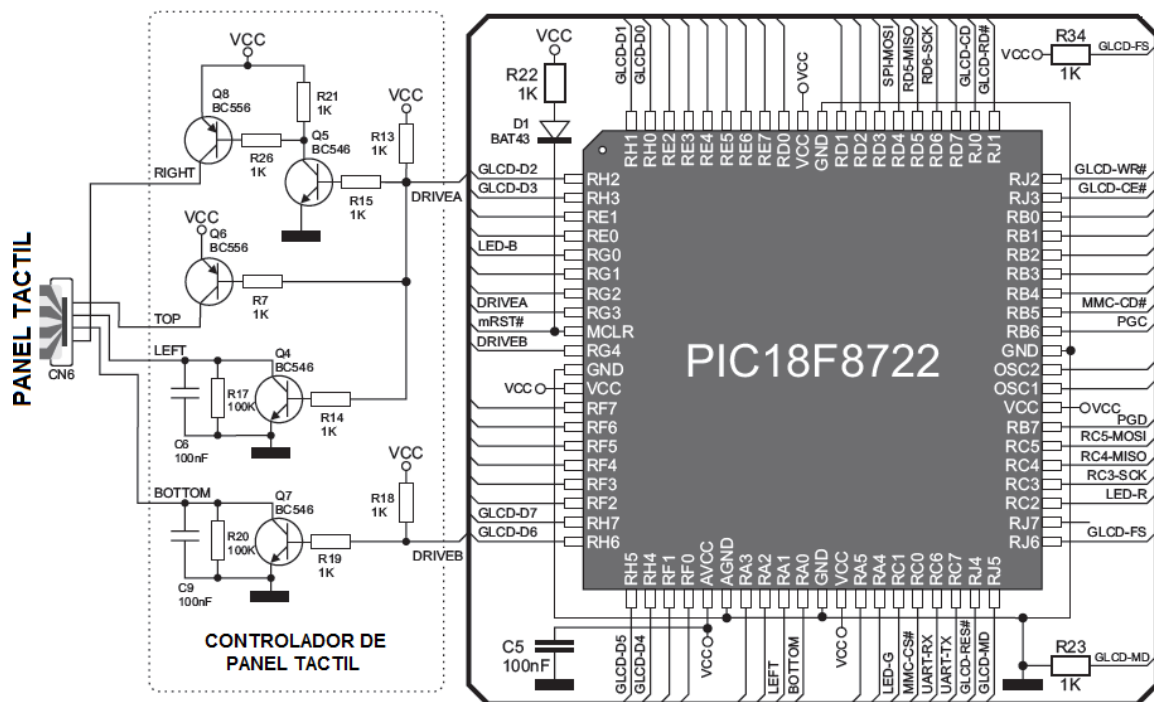


Figura 69. Controlador de panel táctil resistivo.

En la tabla 16 se muestran los voltajes de salida que se obtienen en los contactos del panel (TOP, BOTTOM, LEFT, RIGHT) producto de la combinación de los pines de salida del PIC en los pines DRIVEA y DRIVEB. A continuación se presenta el análisis del circuito que sustenta estos resultados.

DRIVEA = 0, DRIVEB = 1

1. Si DRIVEA=0, el transistor Q6=ON debido a $V_B < V_E$ (pnp), con Q6 habilitado el contacto superior (TOP) de la superficie Y del panel se conecta a Vcc.
2. Si DRIVEB=1, el transistor Q7=ON debido a $V_B > V_E$ (npn), con Q7 habilitado el contacto inferior (BOTTOM) de la superficie Y del panel se conecta a 0V.
3. Si DRIVEA=0, el transistor Q5=OFF debido a $V_B = 0$ (npn) y Q8 =OFF por no haber caída de voltaje en R21 y R26 (pnp), con Q8 deshabilitado el contacto derecho (RIGHT) de la superficie X del panel no se conecta a Vcc.
4. Si DRIVEA=0, el transistor Q4=OFF debido a $V_B = 0$ (npn), con Q4 deshabilitado el contacto izquierdo (LEFT) de la Superficie X del panel no se conecta a 0V.

Como resultado el PIC configura el panel para leer las coordenadas de la Superficie Y (TOP=Vcc, BOTTOM=0V). La lectura de voltaje proporcional a la Coordenada Y se toma del contacto LEFT.

DRIVEA = 1, DRIVEB = 0

Si DRIVEA=1, el transistor Q6=OFF debido a $V_B = V_E$ (pnp), con Q6 deshabilitado el contacto superior (TOP) de la superficie Y del panel no se conecta a Vcc.

Si DRIVEB=0, el transistor Q7=OFF debido a $V_B = V_E$ (npn), con Q7 deshabilitado el contacto inferior (BOTTOM) de la superficie Y del panel no se conecta a 0V.

Si DRIVEA=1, el transistor Q5=ON debido a $V_B > V_E$ (npn) y Q8 =ON debido a $V_B < V_E$ (pnp), con Q8 habilitado el contacto derecho (RIGHT) de la superficie X del panel se conecta a Vcc.

Si DRIVEA=1, el transistor Q4=ON debido a $V_B > V_E$ (npn), con Q4 habilitado el contacto izquierdo (LEFT) de la superficie X del panel se conecta a 0V.

El PIC configura el panel para leer las coordenadas de la Superficie X (RIGHT=Vcc, LEFT=0V). La lectura de voltaje proporcional a la Coordenada X se toma del contacto BOTTOM.

Para determinar con precisión las coordenadas del punto que se presionó en el panel, el PIC a través de los pines DRIVEA y DRIVEB configura la superficie que se va a leer, cuando la superficie está conectada a los voltajes adecuados a través de sus contactos, el voltaje de salida proporcional a la posición de la coordenada que se quiere determinar estará disponible en los pines RA0 (BOTTOM) y RA1 (LEFT), estos están configurados como entradas analógicas que utilizan el ADC integrado en el PIC para digitalizar y procesar matemáticamente el valor de voltaje que determina con precisión el punto que se presionó.

Solo se explican dos de los cuatros resultados obtenidos en la tabla, debido a que el primer y último resultado son condiciones no deseadas que el algoritmo de control del PIC debe evitar durante el proceso de lectura.

Tabla 16. Voltajes de salida del controlador de panel táctil resistivo.

DRIVEA	DRIVEB	TOP	BOTTOM	RIGHT	LEFT	Observaciones
0V	0V	Vcc	-	-	-	No deseada
0V	Vcc	Vcc	0V	-	Y Coord	Determinación de coordenadas en Y
Vcc	0V	-	X Coord	Vcc	0V	Determinación de coordenadas en X
Vcc	Vcc	-	0V	Vcc	0V	No deseada

A.5. Definición de conceptos acerca de los PIC18.

Memoria de programa: Esta memoria almacena el programa que controla el MCU, en los PIC18F se implementan en Flash ROM (Read Only Memory), lo que permite al usuario reprogramar el micro miles de veces.

Memoria de datos: Almacena datos temporales durante la ejecución del programa de un micro, esta memoria es de tipo volátil y se implementa en RAM.

Memoria EEPROM: Es un tipo de memoria no volátil que puede ser borrada y reprogramada eléctricamente utilizando un programador adecuado. Algunos PIC integran una memoria EEPROM que puede ser borrada y reprogramar a través de un software de aplicación.

Convertidor Analógico Digital (ADC): Se utiliza para convertir señales analógicas tales como voltaje en formatos digitales. En general los PIC18F tiene un ADC integrado que permite implementar varios canales analógicos para leer señales externas y luego procesarlas de manera adecuada.

MSSP (Master Synchronous Serial Port): Este es un módulo de comunicación serie que soporta los protocolos SPI (Interfaz serie de periféricos) e I²C (interconexión integrada). Bajo estos dos protocolos se pueden realizar comunicaciones entre MCU-MCU y MCU-Periféricos, tales como memorias microSD, EEPROM, RTC, sensores de temperatura, entre otros.

EUSART (Enhance Universal Synchronous Asynchronous Receiver Transmitter): Es un módulo que proporciona comunicación serial a nivel básico, fue creado para soportar las comunicaciones entre terminales tontas y un ordenador central. Cuando el USART se implementa a voltajes superiores para transmisión a distancia es conocido como **RS232**, generalmente los microcontroladores lo utilizan para comunicarse con las computadoras.

Entrada para reinicio: Esta se utilizan para reiniciar el MCU externamente, durante este proceso el microcontrolador pone sus registros en un valor conocido e inicializa nuevamente la ejecución del programa de control.

A.6. Tarjetas de memoria SD.

Las tarjetas de memoria SD son dispositivos de almacenamiento masivo diseñadas para cumplir con los requerimientos de capacidad, seguridad, tamaño y desempeño impuestos por modernos aparatos portátiles y multimedia tales como: reproductores de audio, video, cámaras, celulares, GPS, entre otros.

La principal innovación tecnológica de SD se basa en las opciones de cifrado de contenido que permiten proteger sus datos a través de autenticación y lectura de claves, por esta razón Secure Digital no permite controladores de código abierto, su licencia y documentación está disponible solo para los miembros (desarrolladores de tecnología) de la Secure Digital Card Association.

Dentro de las memorias SD más utilizadas tenemos:

- SDXC (Secure Digital Extended Capacity) con capacidad entre 32GB a 2TB.
- SDHC (Secure Digital High Capacity) con capacidad entre 2GB a 32GB.
- SD (Secure Digital) con capacidad máxima de 2GB.

Las memorias SD están disponibles en tres formatos diferentes, SD, miniSD y microSD. La siguiente figura muestra las dimensiones de sus presentaciones.

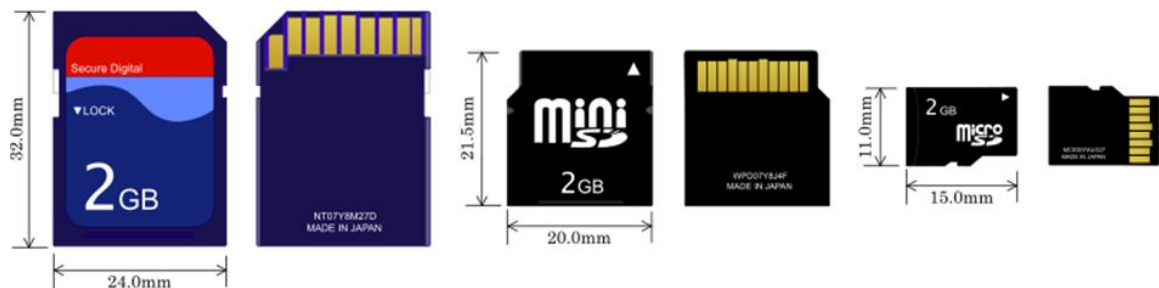


Figura 70. Dimensiones de memorias SD, miniSD y microSD.

Se pueden crear aplicaciones con memorias SD ignorando las opciones de cifrado de contenido, para lograrlo se utiliza el modo SPI/MMC el cual se basa en la compatibilidad entre las memorias SD y MMC (Multimedia Card). Existen compiladores como **Mikrobasic** que integran librerías de configuración de memorias MMC compatibles con SD y SDHC para microcontroladores PIC.

ANEXO B: FUNCIONAMIENTO DE LOS DISPOSITIVOS DE RADIOFRECUENCIA

B.1. Módulos de transmisión y recepción RF

Introducción a la banda ISM

ISM (Industrial Scientific and Medical) es una banda de frecuencia para aplicaciones industriales, médicas y científicas definidas por la **ITU** (International Telecommunication Union) en el artículo 5 de las regulaciones de radio. Esta banda 433.05-434.79 MHz se opera con una frecuencia central de 433.92 MHz.

El uso de la banda ISM es abierto a todo usuario sin utilizar licencia, siempre y cuando se respeten las regulaciones que limitan los niveles de potencia. Este hecho fuerza a que las comunicaciones en ISM toleren cierta cantidad de errores, además de requerir mecanismos de protección contra interferencias.

Módulo de transmisión rfPIC12F675

El rfPIC12f675 es un transmisor de bajo costo y alto desempeño diseñado por microchip utilizando el **rfPIC12F675F** para **433.92 MHz** y el **rfPIC12F675K** para **315 MHz**, opera bajo el esquema de modulación ASK con potenciales aplicaciones en sistemas de corto alcance tales como:

1. Control a distancia inalámbrico
2. Entrada remota sin llave
3. Sistemas de seguridad
4. Telemetría de bajo consumo

Los componentes que integra el rfPIC12F675 son enumerados e ilustrados a continuación:

- rfPIC12F675F (En este trabajo se utilizó la banda ISM “433.92 MHz”)
- 2 pulsadores conectados a GP3 y GP4
- 2 potenciómetros conectados a GP0 y GP1
- LED para indicar que la transmisión RF está habilitada, conectado a GP5
- Datos ASK disponibles en GP2
- Antena

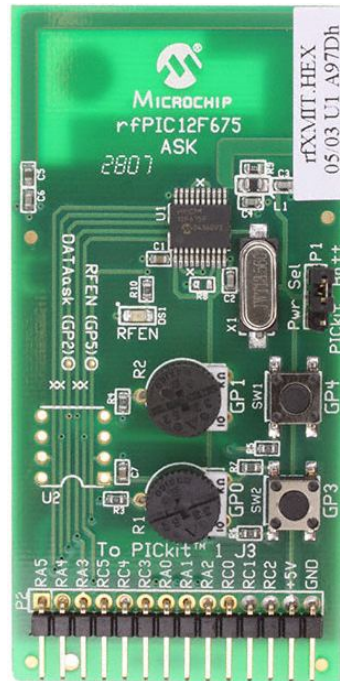


Figura 71. Modulo transmisor rfPIC12F675.

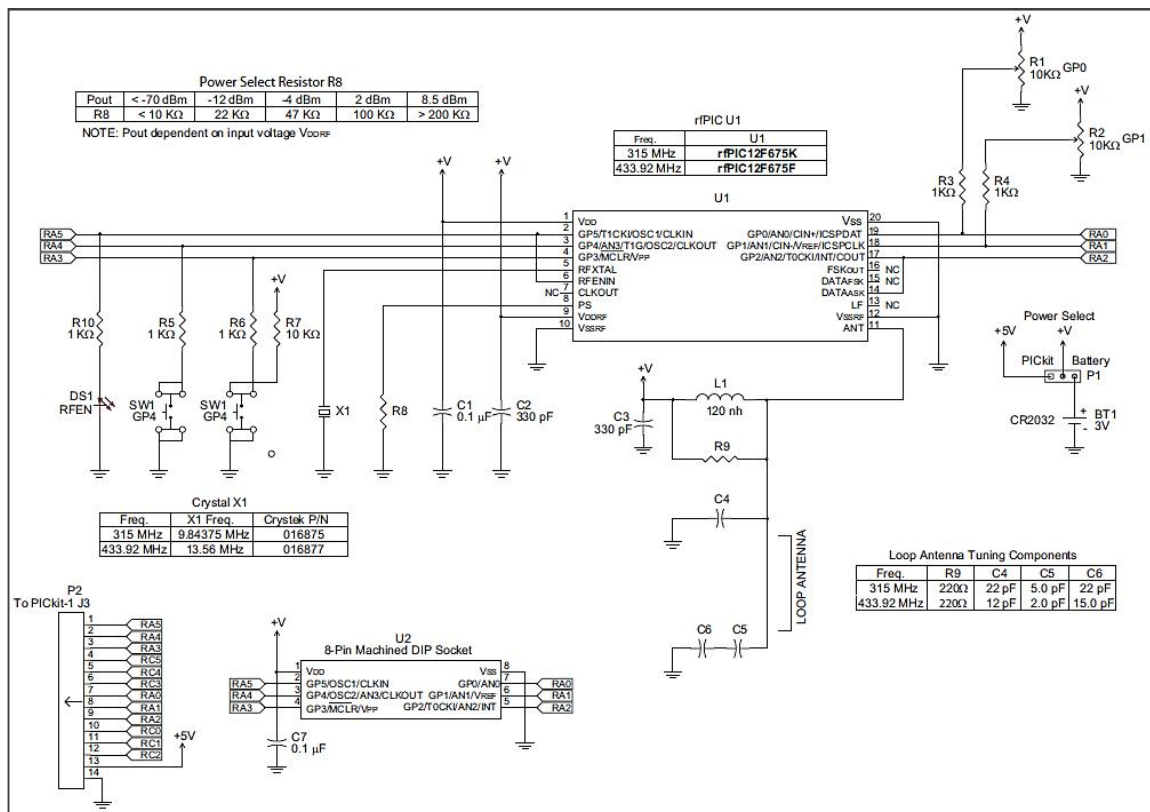


Figura 72. Diagrama de circuito del rfPIC12F675.

Funcionamiento del transmisor rfPIC12F675

Internamente el transmisor rfPIC12f675 esta compuesto por un oscilador a cristal, un PLL (lazo enllavado por fase), un amplificador de potencia (PA) con salida de colector abierto y un medio de control lógico (ver figura 73).

Un oscilador Colpitts genera la frecuencia de referencia establecida por el cristal. Al mismo tiempo el VCO convierte el voltaje en el pin LF a frecuencia, la cual se divide por 32 y se compara con la referencia del cristal, si la frecuencia o la fase no son iguales el circuito de carga corregirá el voltaje en el pin LF.

La salida del VCO también pasa por el amplificador de potencia (PA), cuya salida unipolar va hacia la antena.

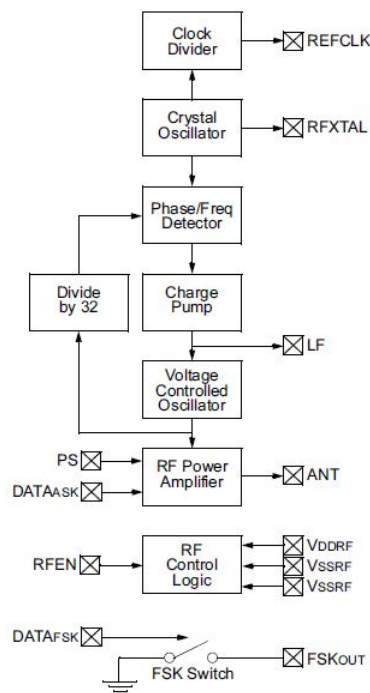


Figura 73. Diagrama en bloques del transmisor rf12F675.

Codificación PWM con Modulación ASK (Amplitud Shift Keying)

La modulación ASK consiste en generar una señal de diferente amplitud en función del dato a transmitir. El rfPIC12f675 utiliza esta modulación en conjunto con la codificación PWM (Modulación por Ancho de Pulso).

La codificación PWM divide el intervalo de tiempo que dura la transmisión de un dato (0,1) en tres intervalos, esto se realiza con el propósito de crear un código de transmisión más robusto para cada dato. Por ejemplo para transmitir un “1”, el PWM genera un alto durante 1/3 del periodo de transmisión y el resto del tiempo permanece en bajo, para transmitir un “0” se mantiene en alto 2/3 del periodo de transmisión y el resto en bajo (ver figura 74). La señal PWM la genera el programa de aplicación cargado en el `rfpic12f675`.

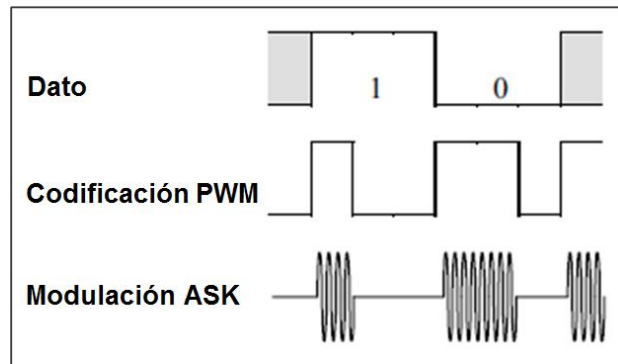


Figura 74. Codificación PWM con modulación ASK.

Protocolo Keelog

La codificación de línea utilizada es el protocolo Keelog simplificado cuyo formato de transmisión se ilustra en la siguiente figura.

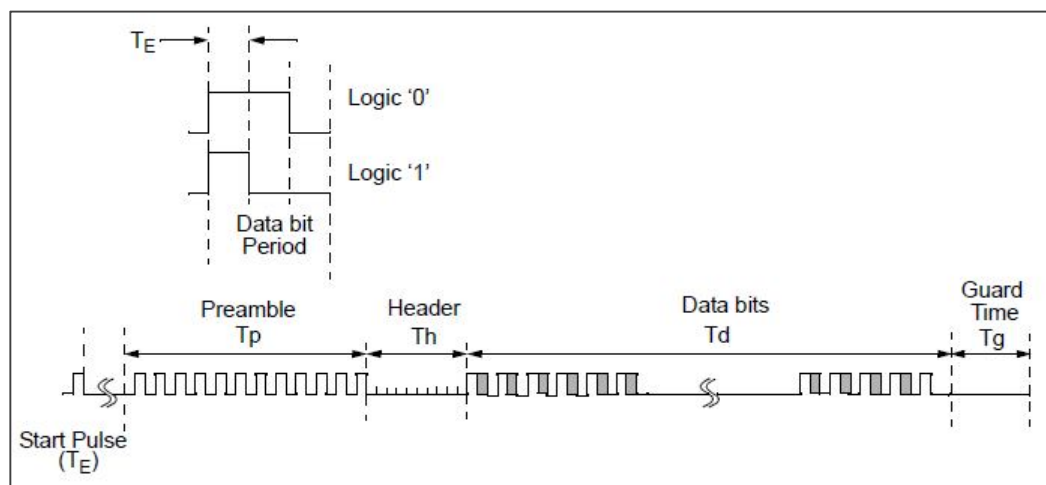


Figura 75. Formato de transmisión del protocolo Keelog.

La trama inicia con un preámbulo que consiste en una serie de pulsos repetitivos cada uno con un periodo fundamental de $T_e=400\mu s$, luego le sigue el encabezado “un pulso en bajo con una longitud de $10 \cdot T_e$ ”. Después se envían 66 bits de datos seguido del tiempo de guarda, el cual es un espacio de tiempo antes de que se inicie otra transmisión.

Organización de la palabra de código

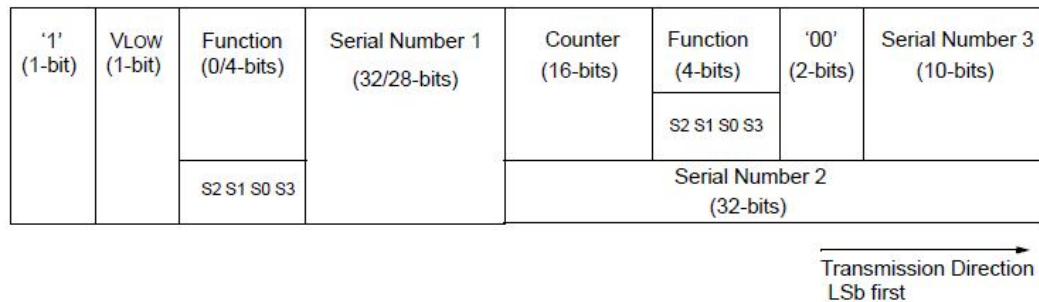


Figura 76. Organización de la palabra de código.

En la implementación realizada en este trabajo monográfico solo se utilizan los primeros dos bytes, el primer byte es el numero serial y el segundo es el byte de función. El receptor identifica el número serial del transmisor y procede a ejecutar la acción dictada por el byte de función, luego el receptor ignora los demás bytes y procede a identificar el tiempo de guarda.

Módulo receptor rfRXD0420

El rfRXD0420 es un receptor RF de bajo costo y alto desempeño diseñado para aplicaciones de corto alcance en ASK. El receptor es compatible con los rfPIC, por lo tanto puede operar a 315 MHz o 433.92 MHz, para seleccionar la frecuencia de operación se debe instalar una antena de longitud adecuada.

Para construir la antena se utiliza cable calibre 24 AWG (ver figura 77), su longitud se determina utilizando la siguiente formula:

$$Longitud. antena(pulgadas) = \frac{2952.8}{f(MHz)} \quad \text{Para } f = 315.00 \text{ MHz} > 9 \frac{3}{8}''$$

$$\text{Para } f = 433.92 \text{ MHz} > 6 \frac{3}{4}''$$

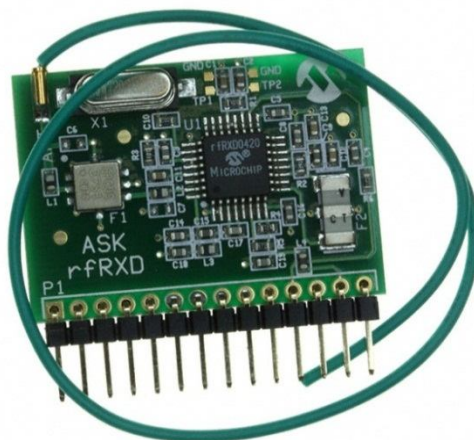


Figura 77. Módulo receptor rfRXD0420.

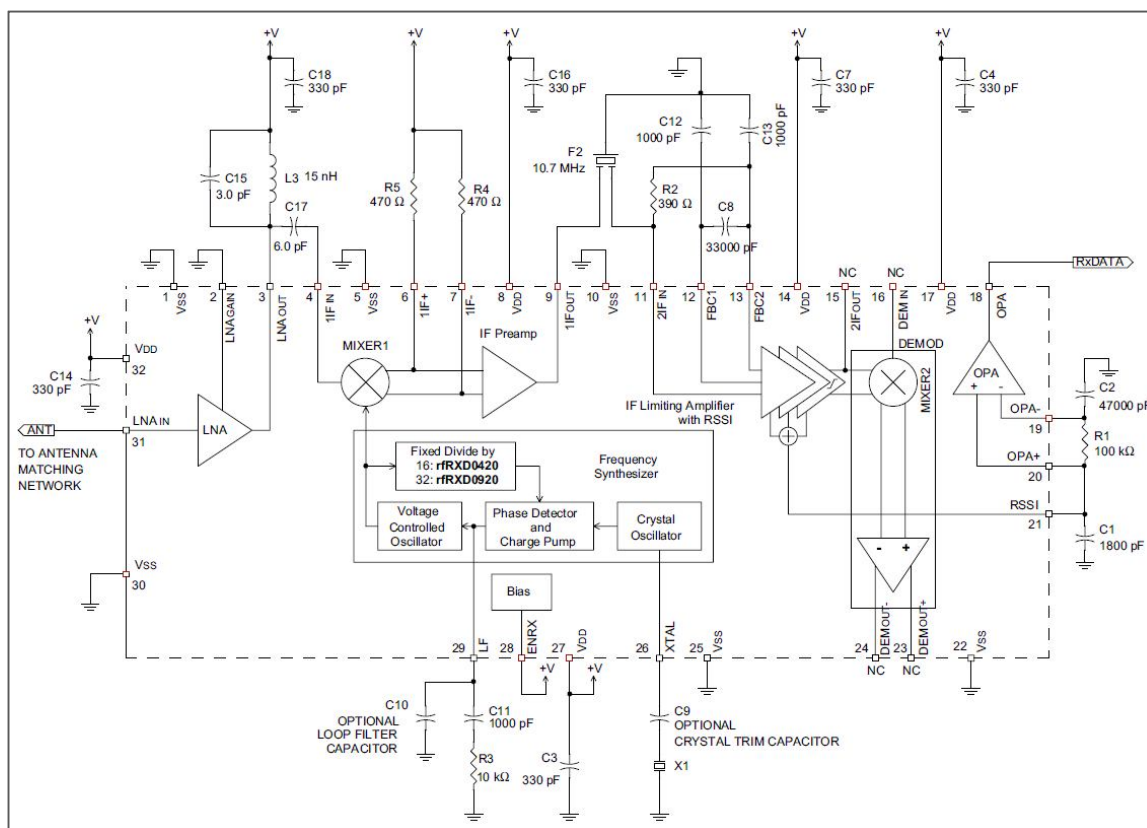


Figura 78. Diagrama de circuito del rfRXD0420.

Funcionamiento del receptor rfRXD0420

El rfRXD0420 tiene un circuito conocido como **BIAS** que se encarga de habilitar o deshabilitar el receptor. Para su funcionamiento este utiliza el pin ENRX, el cual debe estar en “1” (V+) para que el transmisor permanezca encendido.

Con el receptor habilitado, la señal que recibe la antena pasa por un **filtro de onda superficial (SAW)** para evitar que la frecuencia imagen ($F_{rf-imagen}$) y otras señales no deseadas entren en el receptor, este filtro también mejora la razón señal a ruido (SNR) del receptor.

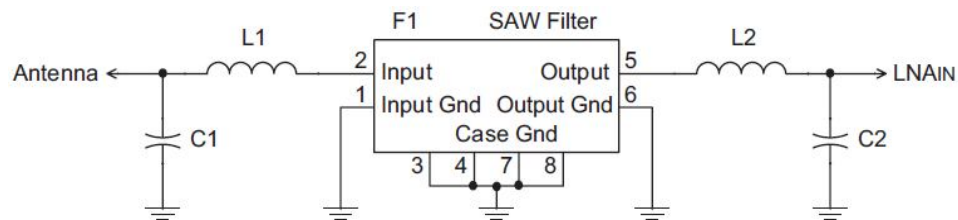


Figura 79. Filtro de onda superficial (SAW Filter).

Seguido del filtro de onda, la señal entra al receptor y pasa por un **amplificador de bajo ruido (LNA)** y alta ganancia ($LNA_{GAIN} = 0V$) con el objetivo de eliminar señales espurias y mejorar la sensibilidad del receptor.

Los componentes capacitivos e inductivos que se encuentran entre LNA_{OUT} y $1IF_{IN}$ proporcionan un filtro pasabanda a la frecuencia recibida (F_{RF}), la cual posteriormente entran al **mezclador (MIXER1)**, en el mezclador la señal RF se baja a una frecuencia intermedia (IF), seguidamente pasa por un **preamplificador de IF**. La salida del preamplificador $1IF_{OUT}$ se pasa por un filtro cerámico de frecuencia intermedia de 10.7MHz que define la selectividad de señal adyacente.

En la etapa final del receptor se encuentra un **amplificador limitador con RSSI**, el propósito de este amplificador es mantener la magnitud de la señal constante para su demodulación y general el Indicador de fuerza de señal recibida (RSSI).

La señal RSSI (en banda base) es proporcional al logaritmo de la señal de entrada de RF en $2F_{IN}$. Esta señal pasa un filtro paso bajas y luego se compara con un voltaje de referencia dinámico (creado por R1 y C2) para determinar si la señal recibida representa un dígito binario “1” o “0”.

Proceso de decisión

En el proceso de filtrado se eliminan altas frecuencias y ruido para ayudar al proceso de decisión. El τ (tau) del filtro RC depende del periodo de la señal y del instante en que la decisión será tomada por el MCU externo al receptor.

La mejor sensibilidad con una razonable distorsión de pulsos ocurre cuando la constante de tiempo es de una a dos veces el periodo de la señal. Si la decisión ocurre en el centro del periodo de la señal entonces la constante de tiempo τ debe de ser menor o igual que la mitad del periodo de la señal (ver figura 80).

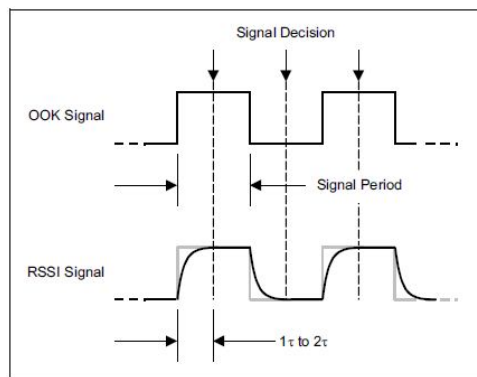


Figura 80. Señal RSSI.

En la siguiente figura el trazo superior es la salida del opamp (pin18) que va hacia un MCU externo (Dato), los otros dos trazos inferiores son la señal RSSI (señal bajo decisión) y la referencia de voltaje del opamp (en el medio de la señal RSSI, la cual proporciona una comparación óptima de los datos entrantes).

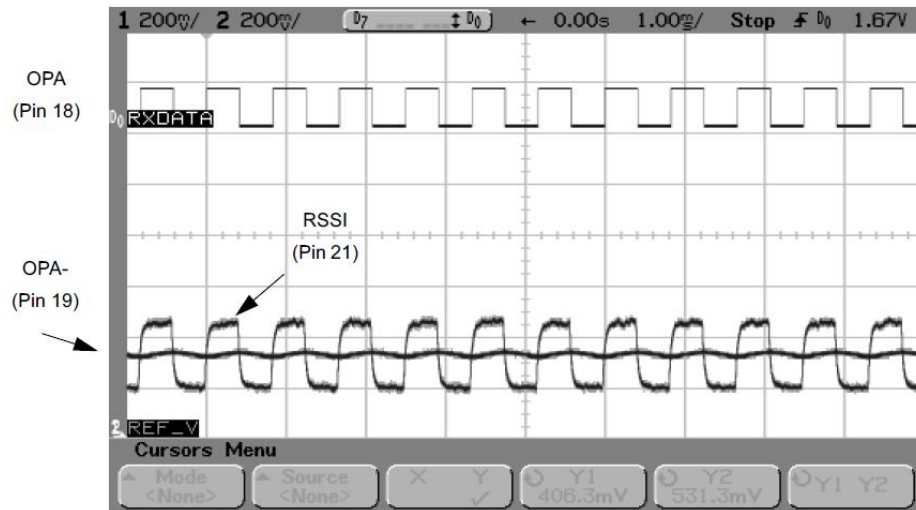


Figura 81. Comparación entre el voltaje de referencia y RSSI.

PICKIT Flash Starter Kit 1

PICKIT Flash Starter Kit 1 es un equipo de desarrollo y demostración para el modulo transmisor rfPIC12F675 y el modulo receptor rfRX0420.

Programación del Modulo Transmisor rfPIC12F675

El modulo transmisor rfPIC12F675 puede ser programado por el PICKIT Flash Starter Kit 1, para esto se debe realizar los siguientes pasos:

1. Colocar el jumper en la posición 1 y 2 para seleccionar la alimentación por los pines 13 y 14, de este modo la alimentación será proporcionada por el PICKIT Flash Starter Kit 1.
2. Remover cuidadosamente el PIC16F676 de su socket.
3. Insertar el modulo transmisor rfPIC12F675 en el puerto de expansión J3.
4. El PIC12F675 contenido en el módulo transmisor será programado, la figura 82 ilustra este procedimiento.

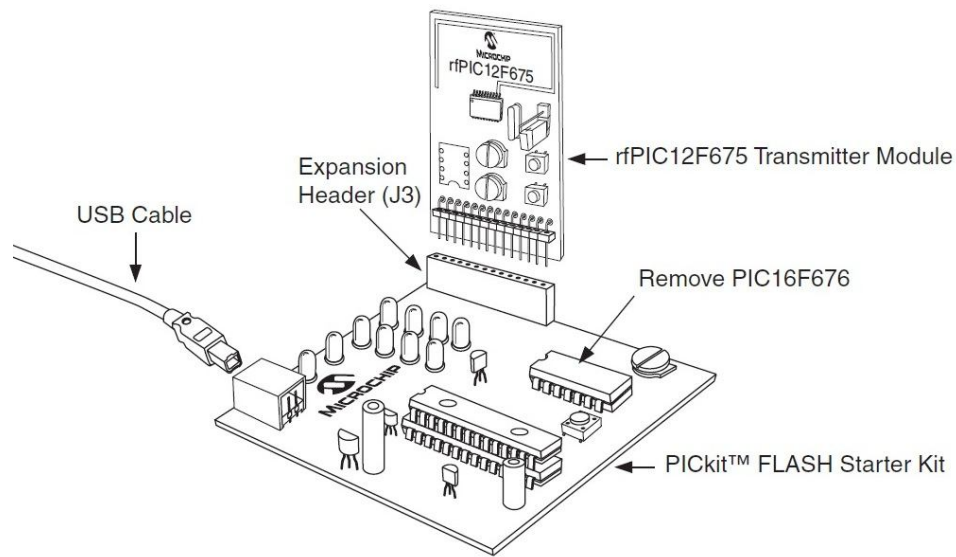


Figura 82. Procedimiento de programación del transmisor.

Trasmisión del estatus de Alarma

Cuando el MCU del panel de control genere una señal de alarma, esta habilitará la transmisión de un número de 2Bytes pre programado en el rfPIC12F675, este número también se encuentra cargado en la memoria de programa del PIC16F676.

En la aplicación desarrollada para este trabajo monográfico el PIC16F676 se programa para decodificar el flujo de datos a la salida del rfRXD0420 (Pin18).

Si la señal es recibida y decodificada satisfactoriamente el PIC16F676 se encarga de activar un relevador que energiza la sirena audible instalada en la caseta del CPF de la UNI.

ANEXO C: PROTOCOLOS DE COMUNICACIÓN

C.1. Protocolo de comunicación Software I²C

Software I²C es un protocolo de comunicación serial que es independiente del hardware y que puede ser implementado en cualquier MCU (microcontrolador). Utiliza dos líneas para comunicarse: SDA (línea de datos serial) usada para transmisión de datos y SCL (reloj serial) para señalización. Estas líneas son de “*drenador abierto*”, por lo tanto, se requieren resistencias de pull-up en cada una. Para implementar I²C por software se requiere utilizar los temporizadores del MCU, esto implica desactivar el servicio de interrupciones de microcontrolador para evitar que el micro le preste atención las banderas de los timer.

El siguiente esquema muestra la arquitectura y conexionado de un bus I²C:

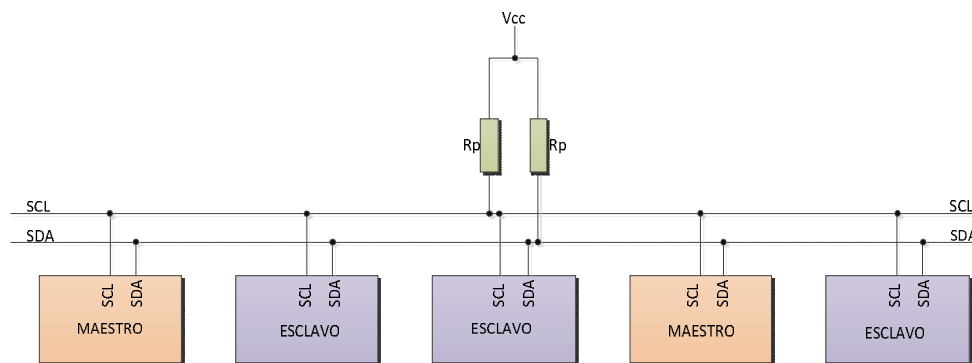


Figura 83. Bus I²C.

Los dispositivos conectados a este bus mantienen un protocolo de comunicación de tipo maestro/esclavo, el maestro es quien inicia y termina la transferencia de información además de controlar la señal del reloj (generalmente es un MCU) y el esclavo es direccionado/subordinado al maestro (generalmente un periférico).

La línea SDA es bidireccional, es decir tanto el maestro como los esclavos puede actuar como transmisores o receptores de datos, dependiendo de la función del dispositivo.

Transferencia de un bit: Para transferir un bit por la línea SDA, se debe generar un pulso de reloj por la línea SCL, los bits de datos transferidos por SDA

deben de mantenerse estables mientras la línea SCL este a nivel alto, de manera que el estado de SDA solo puede cambiar cuando SCL está a nivel bajo.

La siguiente figura ilustra esta lógica:

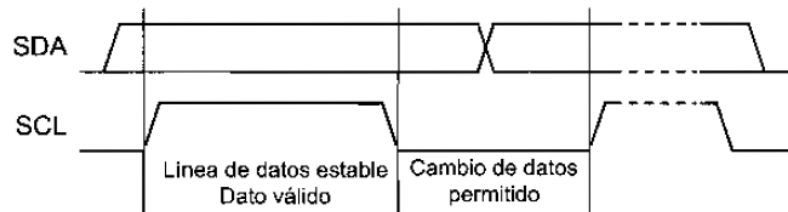


Figura 84. Lógica de transmisión de datos en un bus I2C.

Condiciones de Start y Stop

Para que la transferencia de información pueda ser iniciada el bus no debe estar ocupado, para indicar esta condición, ambas líneas deben de estar en alto, una vez verificado esto, el transmisor procederá a enviar un bit cada pulso de reloj.

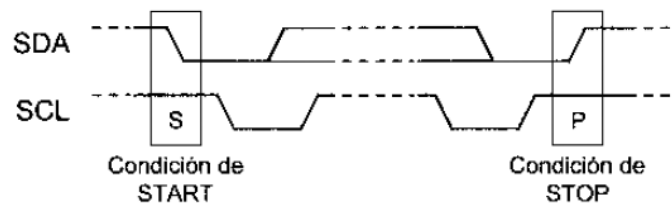


Figura 85. Señalización Start y Stop de un bus I²C.

Las condiciones Start y Stop son siempre generadas por el microcontrolador maestro. El bus I2C se considera ocupado después de la condición de Start y libre después la condición Stop.

Formato de una Transferencia de datos

Cada dato enviado por la línea SDA debe tener 1 byte. El número de bytes que se puede enviar no tiene restricción. El byte de datos se transfiere empezando por el bit 7 que es el más significativo, una vez que ya se ha transmitido el byte,

el receptor deberá mandar un bit de acuse de recibo en el noveno pulso del reloj. El receptor ejecuta este acuse poniendo la señal SDA a un nivel bajo.

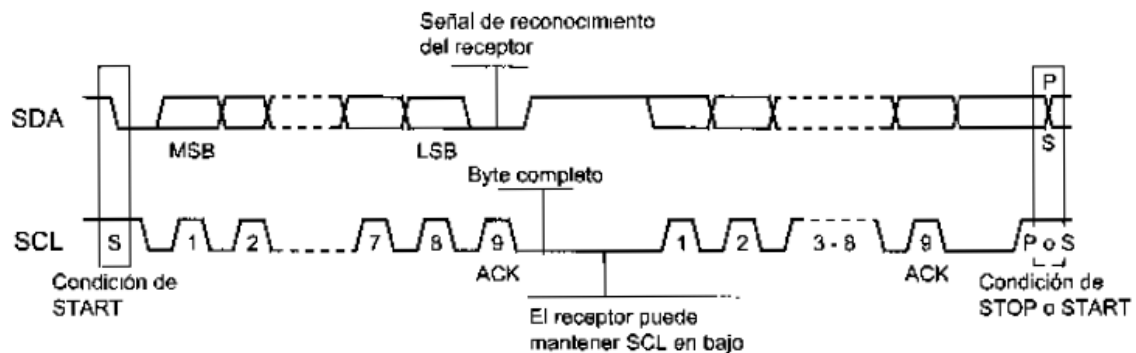


Figura 86. Esquema de transmisión de datos del protocolo I²C.

Formato de una transferencia de datos

Los siguientes pasos son necesarios para enviar o recibir información:

1. Un bit de Start.
2. Siete bits de direccionamiento de un esclavo.
3. Un bit de lectura/escritura que define si el esclavo es transmisor o receptor.
4. Un bit de acuse de recibo.
5. Un mensaje de 1 byte.
6. Un bit de Stop.

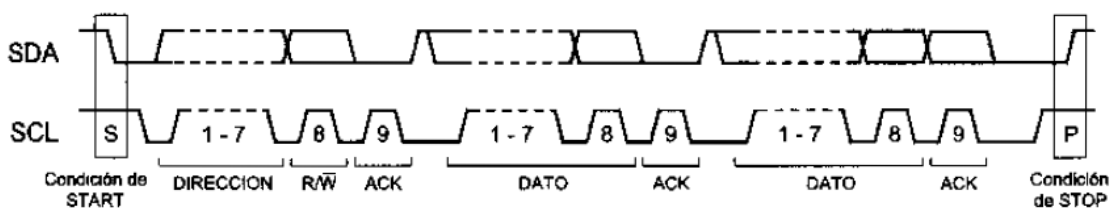


Figura 87. Formato de Trasmisión/Recepción entre Maestro - Esclavo.

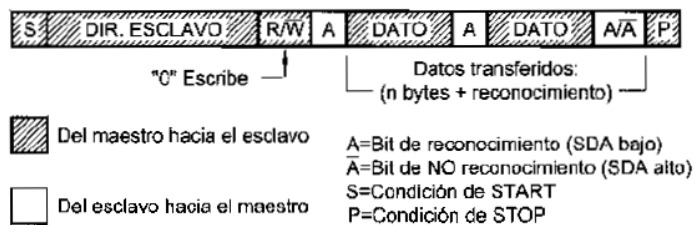
Como puede haber varios esclavos conectados al bus, el maestro debe indicar mediante una dirección de esclavo a cuál de ellos va destinada la información. Cada esclavo tiene una dirección de identificación, todos ellos escuchan continuamente la línea para determinar a quien se dirige el maestro.

Cada dispositivo comprueba los 7 primeros bits de la dirección con la suya y si esta coincide, este será un esclavo-receptor o esclavo-emisor dependiendo del bit R/W que envía el Maestro (R/W=0 > Receptor y R/W=1 > Emisor).

Tipos de Formatos de transferencia

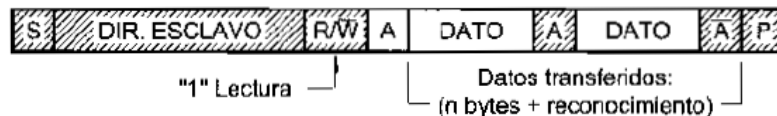
Maestro-emisor transmite al esclavo receptor:

Si el bit R/W=0 que indica escritura la secuencia seria:



Maestro-receptor lee de un esclavo emisor

Si el bit R/W=1 que indica lectura la secuencia seria:



Formato combinado:

Una transferencia de datos siempre termina con una condición de stop generada por el maestro, sin embargo, si un maestro todavía requiere comunicarse por el bus puede generar repetidamente condiciones de Start y direccionar a otro esclavo, sin necesidad de generar la condición de Stop. Durante un cambio de flujo de datos dentro de una transferencia, la condición de Start y la Dirección del esclavo se repiten, pero con el bit R/W invertido.

Velocidades

El protocolo I²C se puede implementar básicamente en tres velocidades; Standard mode: 100Kbits/s, Fast mode: 400Kbits/s y High-speed mode: 400Kbits/s.

C.2. Protocolo de comunicación SPI

El Puerto Serial Síncrono Maestro (MSSP por sus siglas en inglés) proporciona 2 tipos de comunicación: SPI e I²C. Estos protocolos son usados por los MCU para interactuar con periféricos que soportan esta forma de comunicación.

El protocolo SPI es un estándar de comunicaciones, usado principalmente para la transferencia de información entre circuitos integrados.

Este protocolo es simple, rápido, usa direccionamiento por hardware y comunicación síncrona, por lo tanto, una señal de reloj gobierna la transmisión/recepción de datos. Los bits de datos son almacenados en el registro de desplazamiento del SPI, los cuales son transferidos uno a uno en cada ciclo de reloj (ver figura 88), se puede alcanzar velocidades de hasta 5 MHz si el reloj del MCU es 20MHz.



Figura 88. Lógica de transmisión de datos en un Bus SPI.

Funcionamiento

Uno de los MCU debe actuar como maestro generando la señal de reloj, los demás deben comportarse como esclavos, usando el reloj del maestro tanto para enviar como para recibir información.

Las señales necesarias para establecer una comunicación SPI son:

- Reloj serial (SCK)
- Dato serial de entrada (SDI)
- Dato serial de salida (SDO)
- Seleccionador de esclavo (SS)

El siguiente grafico muestra un esquema de una conexión típica entre un MCU maestro y un esclavo transmisor y otro receptor:

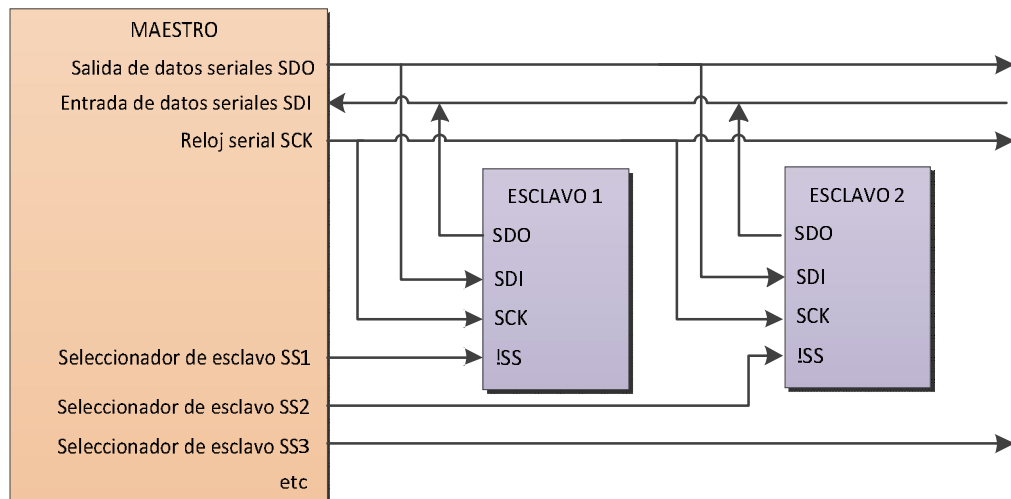


Figura 89. Bus SPI.

A continuación se presenta un grafico muestra un diagrama en bloques del módulo MSSP en modo SPI.

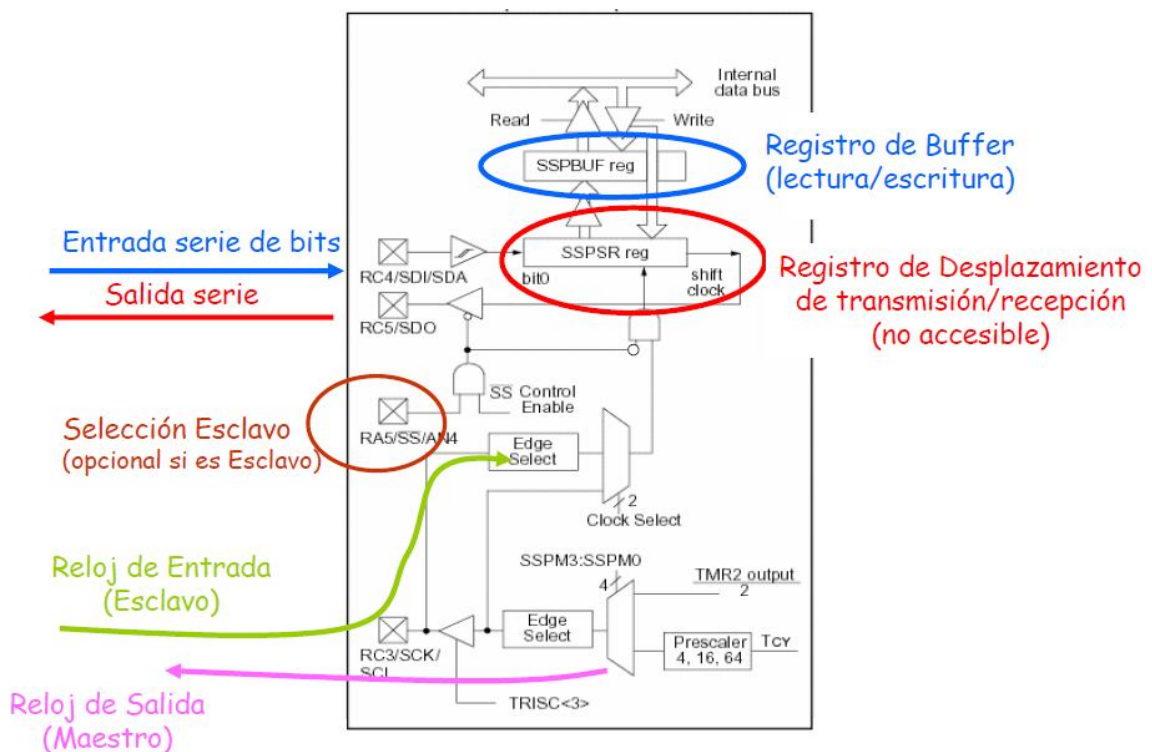


Figura 90. Diagrama en bloques del Puerto Serial Sincrono Maestro (SPI).

ANEXO D: DISEÑO Y FABRICACION DES TARJETAS DE CIRCUITO IMPRESO

D.1. Diseño de las Tarjetas de Circuito Impreso (PCB)

Para realizar los cuatro diseños se utilizó el software ARES de Proteus, el cual integra varias funciones y herramientas que facilitan esta labor.

Generalmente un diseño en Ares comienza con la selección de los componentes del circuito, sin embargo, este software también ofrece la opción de importar un NetList desde ISIS (ver figura 91), lo que resulta verdaderamente satisfactorio, debido a que se transfiere la lista de componentes utilizados, encapsulados, plantillas de montaje y hasta la información de interconexión entre componentes.

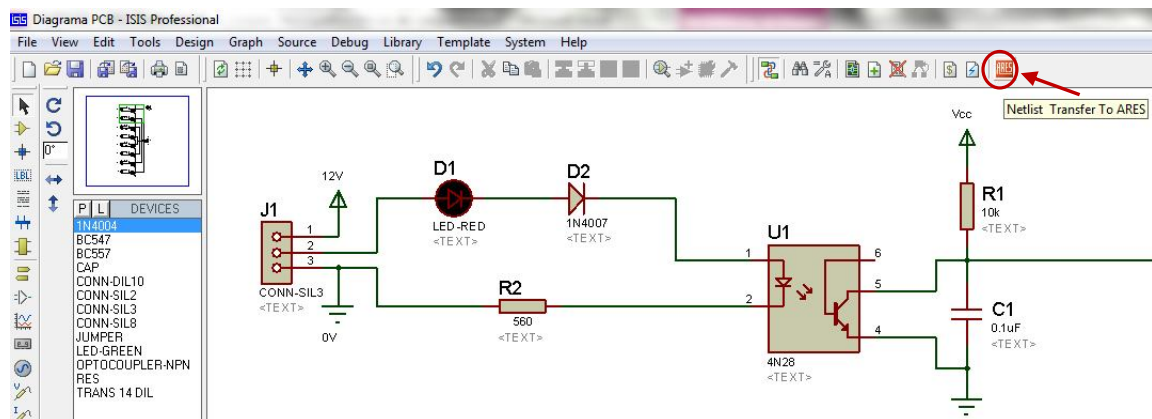


Figura 91. Procedimiento para transferir el Netlist de ISIS a ARES.

Cuando el Netlist se ha cargado satisfactoriamente en ARES, se procede a configurar la geometría y dimensiones de la placa que se utilizara, seguido de la ubicación e interconexión (ruteo) entre los componentes. ARES permite realizar estas funciones de forma automática (utilizando el NetList), sin embargo para este proyecto se realizó el proceso de forma manual, para garantizar estética, uniformidad y sobre todo la funcionalidad de los PCBs.

Las siguientes imágenes fueron capturadas de la pantalla de edición de ARES, en ella se encuentra terminado el diseño de las cuatro tarjetas involucradas.

El ancho de las pistas depende de la corriente máxima en cada circuito y la densidad de cobre (*Onzas/pie²*) de la tarjeta virgen utilizada en la fabricación.

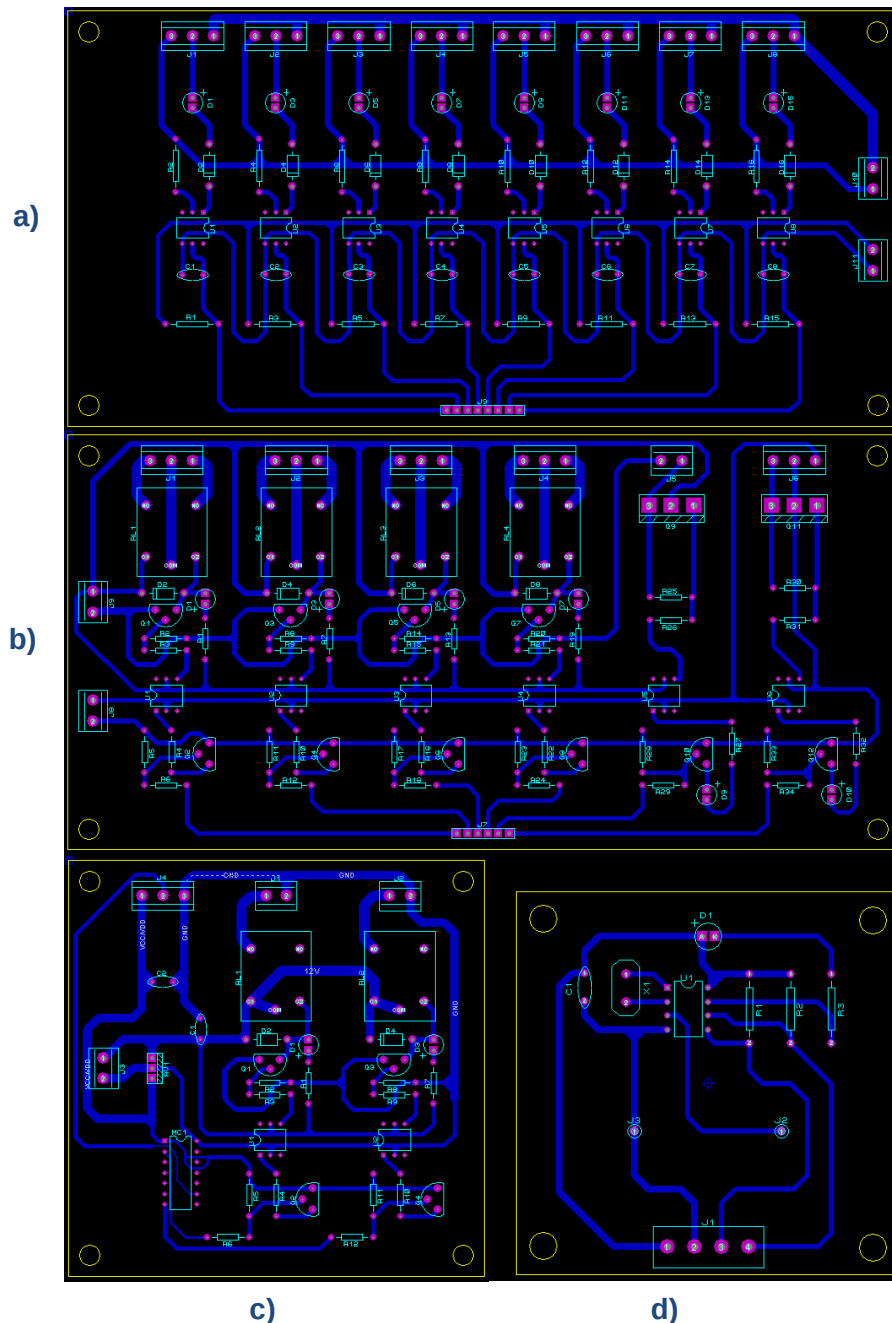


Figura 92. Diseños de los PCB. a) Interfaz de Entrada, b) Interfaz de Salida, c) Interfaz de Recepción de Alarma, d) Tarjeta de Control de Reloj.

Depuración de Errores de diseño

ARES integra herramientas para evaluar los diseños elaborados, que incluyen funciones para verificar la conectividad (según Netlist), detectar errores de separación entre pistas, falta de encapsulado y además tiene capacidad de crear

una representación 3D de la PCB, lo que permite al usuario comprobar sus resultados antes de ser fabricados. A continuación se ilustra este concepto.

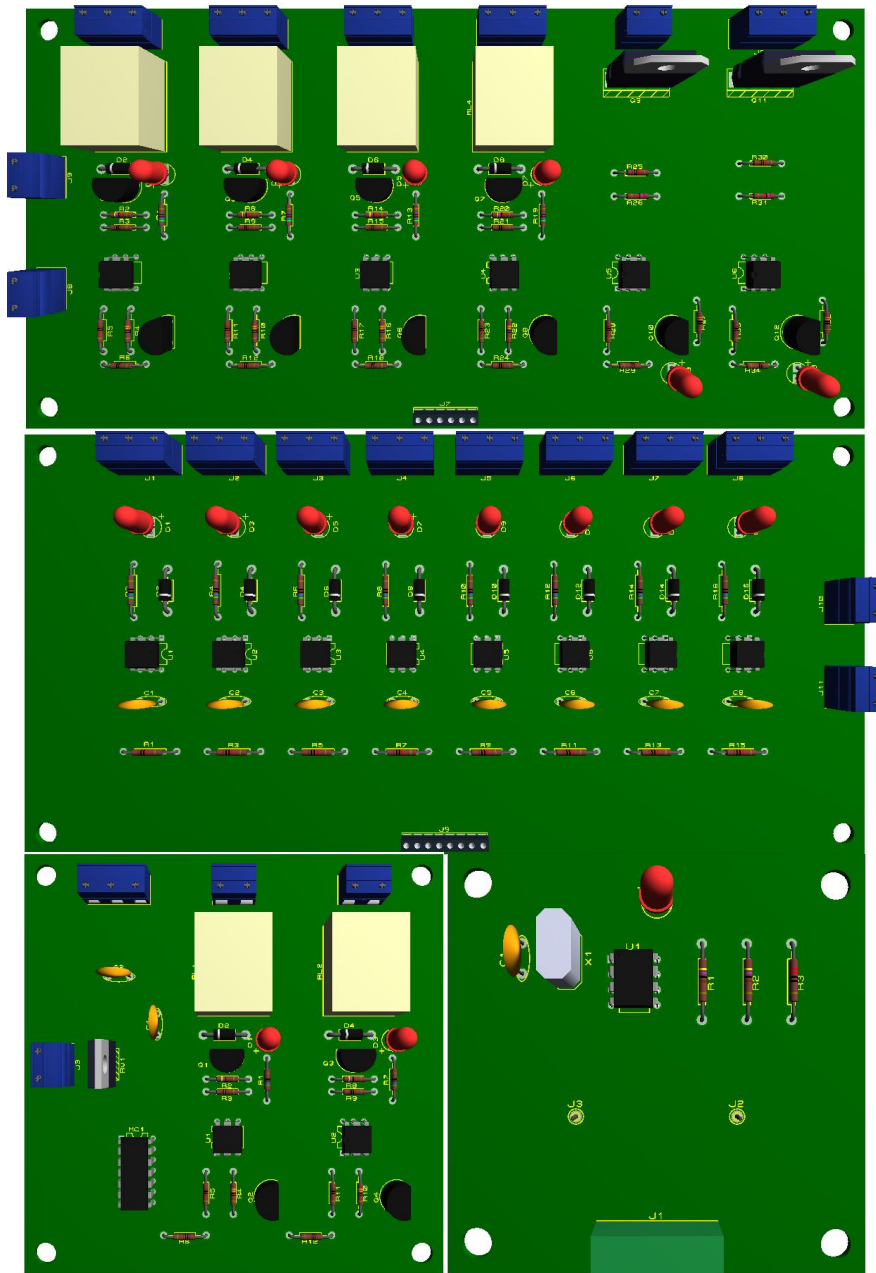


Figura 93. Representación 3D de los diseños de la Figura 92.

Elaboración de las Placas de Circuito Impreso

El proceso de fabricación de las PCB se realizó utilizando el Método de Insolación, este consiste en revelar el circuito impreso utilizando material fotosensible (película autoadhesiva sensible a la luz UV), una cámara de exposición Ultra Violeta y una solución reveladora.

Este proceso se puede sintetizar en los siguientes pasos:

1- Impresión del PCB en filminas

Se configura el diseño de ARES y se imprime en una lámina de filmina utilizando lógica negativa. Una sola impresión no fue suficiente para obtener un revelado de calidad, por lo tanto se tuvo que imprimir cinco filminas y colocarlas unas sobre otras para bloquear completamente los rayos UV, el resultado es una lámina como la siguiente.

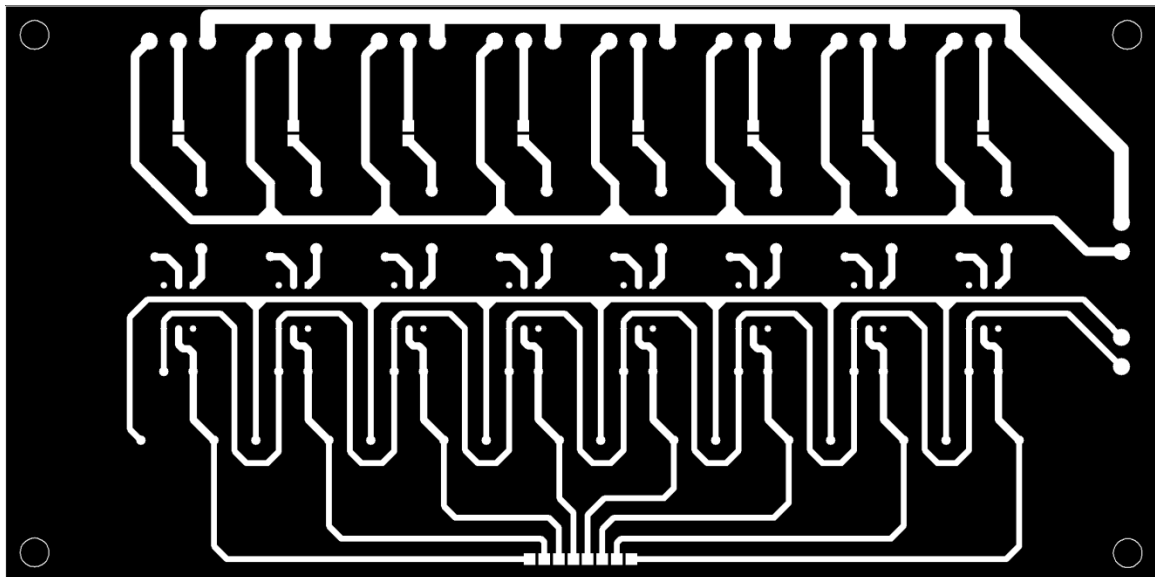


Figura 94. Impresión en filmina de un circuito impreso (revelado invertido).

2- Exposición a Luz Ultra Violeta

Se coloca la película fotosensible y la filmina impresa sobre la tarjeta de cobre virgen, se debe sujetar con cinta adhesiva antes de introducirla a la Insoladora.



Figura 95. Tarjeta de cobre preparada para su exposición a los Rayos UV.

Se programa la máquina para un tiempo de exposición de 10 minutos y una vez concluidos se introduce la tarjeta en el ácido revelador, cuya mezcla con agua es de 1:10. Con una brocha suave se quita el resto de película no expuesta y luego se introduce en agua para limpiar la tarjeta del ácido revelador.



a)



b)

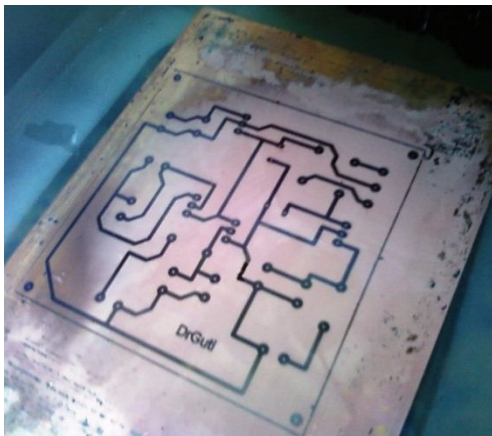
Figura 96. a) Tiempo de exposición de 600 segundos, b) Tarjeta en proceso de revelado después de la insolación.

3- Supresión del exceso de cobre y perforación de la tarjeta

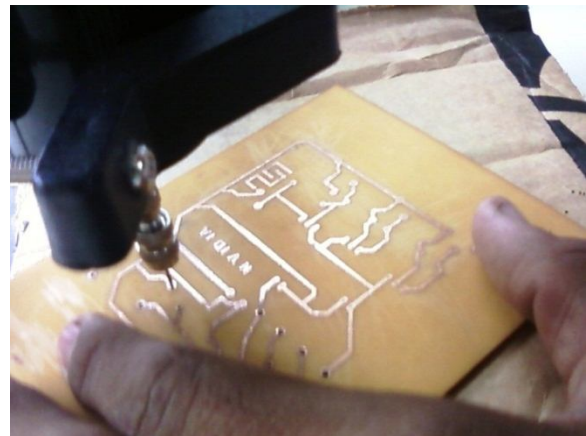
El siguiente paso es introducir la tarjeta en el percloruro férrico, una solución acida que remueve el cobre donde no está protegido por la película fotosensible.

Durante la exposición UV esta película se vuelve más resistente y permite neutralizar por completo los efectos del percloruro férrico, de esta manera quedan impresos en cobre las pistas y nodos de la nueva tarjeta.

Posteriormente se realizo la perforación de los agujeros en donde se montan los componentes electrónicos de la tarjeta (taladro PCB), la siguiente figura muestra dos imágenes que ilustras estos procesos.



a)



b)

Figura 97. a) Tarjeta inmersa en Percloruro Férrico, b) Proceso de perforación de puntos de montaje (Broca de 0.75mm).

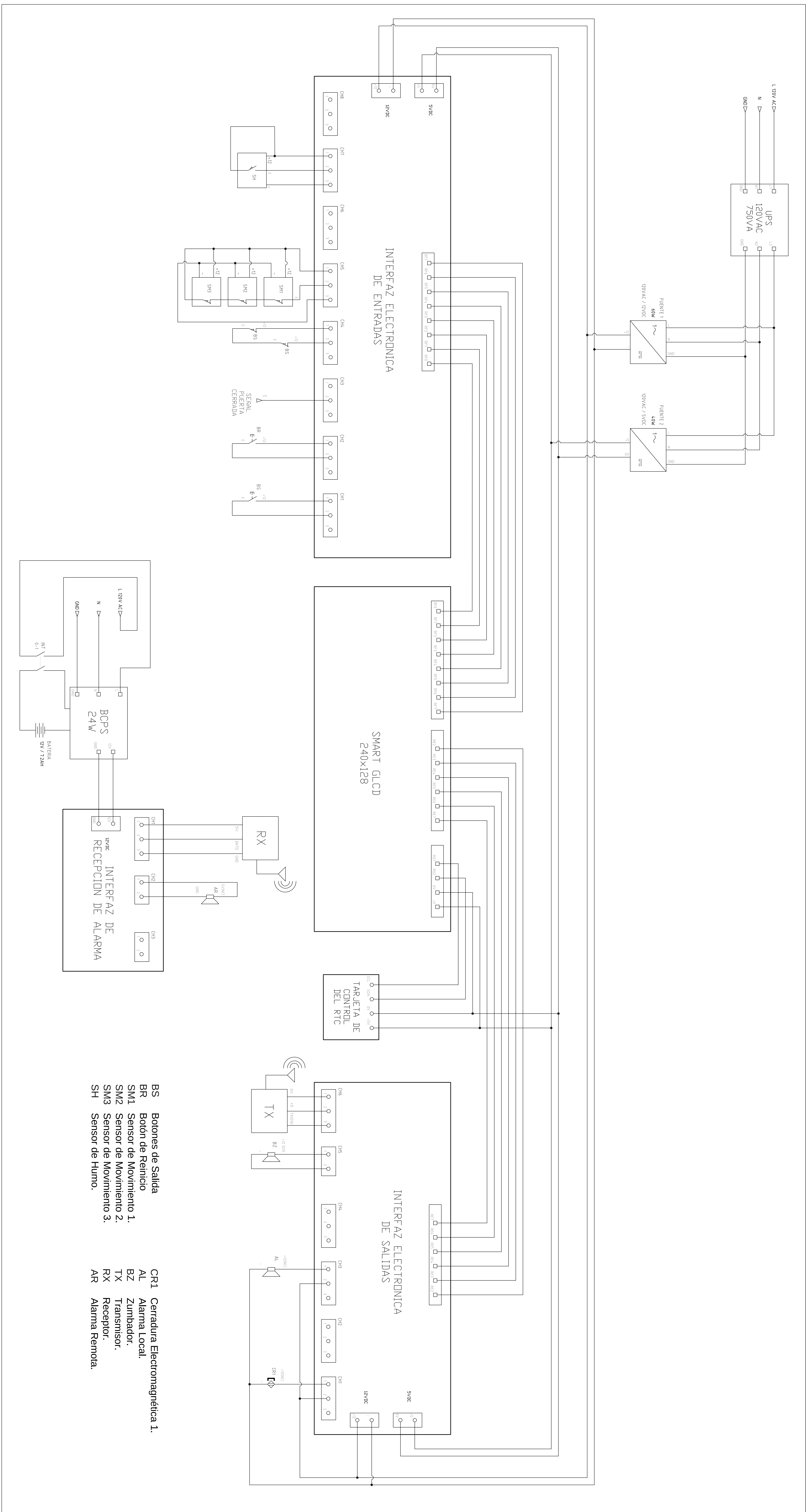
4- Montaje de componentes.

Esta última etapa consiste en interconectar todos los componentes que integran la tarjeta, cada punto de soldadura debe garantizar la mejor conductividad entre el pin de un componente y la pista de cobre del PCB.

Una vez que se han montado los componentes se procede a realizar una inspección visual, su propósito es verificar el correcto ensamblaje de los componentes, según el diagrama eléctrico de la tarjeta.

Posteriormente se procede con las pruebas de funcionamiento, acá se energizó por primera vez la tarjeta electrónica, estas pruebas se realizaron en un ambiente controlado (laboratorio) para garantizar la seguridad del personal y evitar daños mayores a los componentes bajo prueba (con fuentes limitadoras).

ANEXO E: DIAGRAMA ELECTRICO DEL SISTEMA



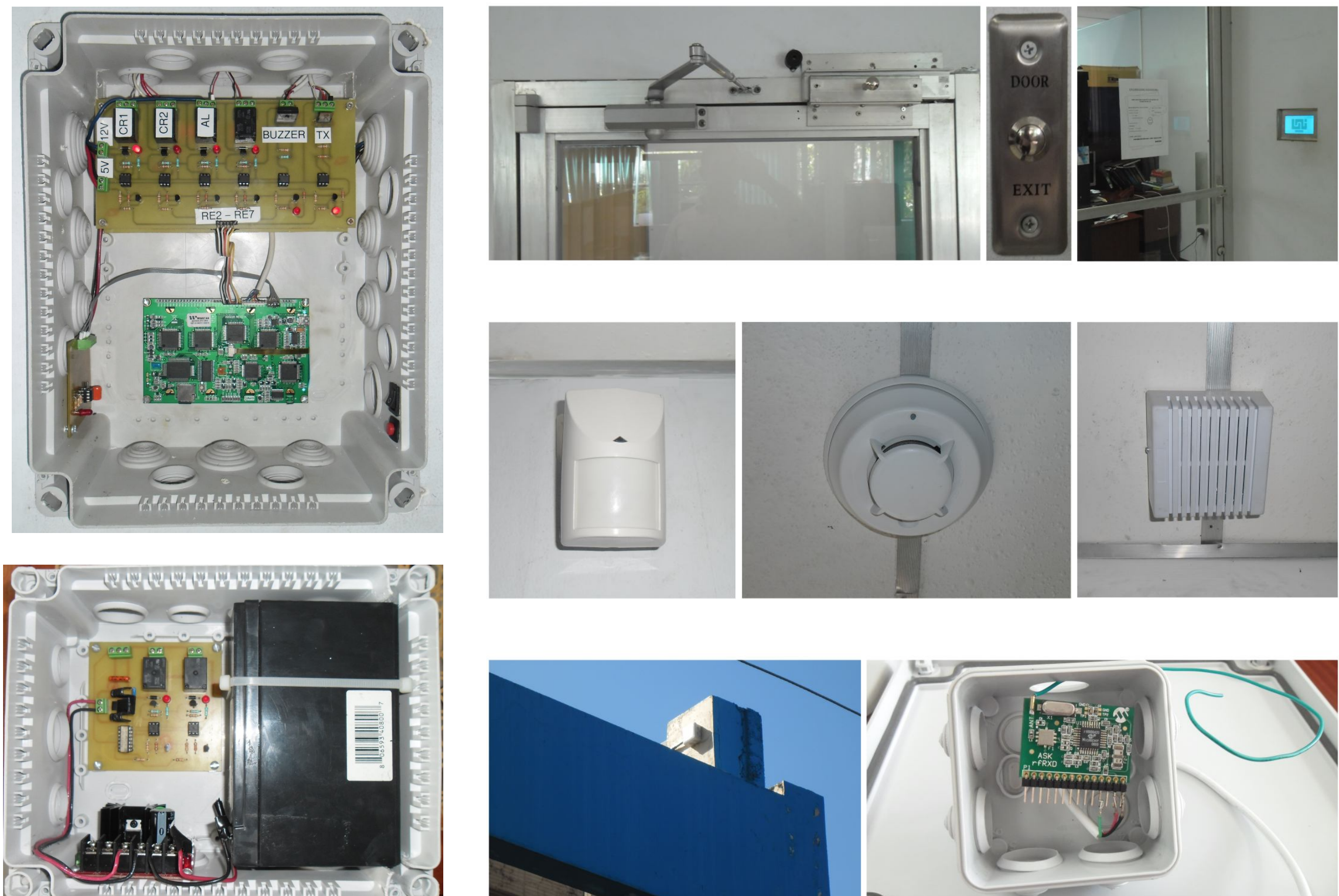


Figura 62. Ubicación de los componentes del sistema de seguridad.