Universidad Autónoma de Querétaro

Facultad de Ingeniería

Ingeniería en Automatización

Sistema de seguridad para acceso a instalaciones basado en microcontroladores

Tesis

Que como parte de los requisitos para obtener el título de
Ingeniero en Automatización

Presenta:

Karen Andrea Ramírez Arriaga

Dirigido por:

Dr. Juan Manuel Ramos Arreguín

Dr. Juan Manuel Ramos Arreguín	
Presidente	Firma
Dr. Saúl Tovar Arriaga	
Secretario	Firma
Dr. Jesús Carlos Pedraza Ortega	
Vocal	Firma
Dr. Efrén Gorrostieta Hurtado	
Suplente	Firma

Centro Universitario Querétaro, Qro., México.
Agosto 2020

Dedicatorias

A mi abuelo Alfonso, que donde quiera que esté, estoy segura que se encuentra orgulloso de este gran logro.

A mi madre, por todo el apoyo que me brindó durante mis estudios y durante el desarrollo de mi proyecto de tesis. Gracias mamita por esforzarte para cumplir mi sueño.

Agradecimientos

Agradezco a mi familia, por apoyarme en mi carrera universitaria.

A mi director de tesis, el Dr. Juan Manuel Ramos Arreguín, por siempre poder confiar en él, durante el desarrollo de esta tesis y durante gran parte de la carrera. Gracias por guiarme con su experiencia.

A mis sinodales, el Dr. Carlos Pedraza, el Dr. Saúl Tovar y el Dr. Efrén Gorrostieta, por apoyarme en el proyecto de tesis y por siempre estar en la mejor disposición de dar observaciones a este trabajo.

A todos mis profesores, por transmitirme todos sus conocimientos.

Al Ing. José Luis Avendaño Juárez, por siempre apoyarme en los trámites de mi titulación y en todo lo relacionado con la coordinación de la licenciatura.

A mis amigos y compañeros que ante alguna duda estuvieron dispuestos a ayudarme.

RESUMEN

La seguridad es esencial cuando hablamos de edificios donde se encuentran materiales costosos, como centros de cómputo, máquinas y herramientas o equipos utilizados para la investigación. Con los años, los sistemas de control de acceso utilizados en estos espacios han ido cambiando, desde sistemas muy tradicionales que usan contraseña numérica, hasta sistemas de identificación biométrica. En este trabajo, se presenta un sistema de control de acceso basado en un microcontrolador *PIC*, también se realiza una comparación entre dos modelos de microcontroladores *PIC*, y se elige la mejor opción. Este sistema tiene dos formas de reconocimiento de usuarios, por huella digital o por contraseña numérica. El reconocimiento de huellas digitales se logra mediante un sensor óptico de huellas digitales, que tiene memoria flash interna en la que se almacenan las huellas digitales. El reconocimiento por clave numérica se realiza mediante un teclado matricial y el almacenamiento de las contraseñas se lleva a cabo en la memoria *EEPROM* interna del microcontrolador. El hardware incluye una etapa de potencia para el uso de una cerradura eléctrica. La interfaz de comunicación con el usuario es una pantalla *LCD*. Este prototipo se instalará en el Laboratorio de Mecatrónica de la Universidad Autónoma de Querétaro, específicamente en el área de maquinados, evitando así daños a los equipos.

Palabras clave: control de acceso, biometría, huella digital, microcontrolador, memoria *EEPROM*, pantalla *LCD*, contraseña numérica, teclado matricial.

ABSTRACT

Security is essential when we talk about buildings where expensive materials are found, such as computer centers, machines and tools or equipment used for research. Over the years, the access control systems used in these spaces have been changing, from very traditional systems that use a numerical password, to biometric identification systems. In this work, an access control system based on a *PIC* microcontroller is presented, a comparison is also made between two models of *PIC* microcontrollers, and the best option is chosen. This system has two forms of user recognition, by fingerprint or numerical password. Fingerprint recognition is accomplished using an optical fingerprint sensor, which has internal flash memory in which fingerprints are stored. The recognition by numerical password is carried out through a matrix keyboard and the storage of the passwords is made in the internal *EEPROM* memory of the microcontroller. The hardware includes a power stage for the use of an electric lock. The user communication interface is an *LCD* screen. This prototype will be installed in the Mechatronics Laboratory of the Autonomous University of Querétaro, specifically in the machining area, thus avoiding damage to the equipment.

Keywords: access control, biometrics, fingerprint, microcontroller, *EEPROM* memory, *LCD* display, numeric password, keypad.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ALGORITMOS

Capítulo 1. Introducción

1.1. Antecedentes

Las diferentes variantes en los sistemas de control de acceso han ido cambiando con el paso de los años, desde los tradicionales sistemas de seguridad basados en una clave numérica hasta sofisticados sistemas de identificación biométrica. Revisando diferentes investigaciones sobre prototipos de sistemas de control de acceso, se encuentra lo siguiente.

En 2013, *Vergara y Verónica*, desarrollan un proyecto que nace de la necesidad de brindar seguridad a los equipos del laboratorio de Telemática de la Universidad Politécnica Salesiana, con el objetivo de monitorear los equipos y tener un acceso controlado del personal autorizado. En este trabajo, se utiliza la tecnología de identificación por radiofrecuencia (*RFID*). El monitoreo y la administración de los accesos se logra mediante una interfaz gráfica en el software *LabVIEW (Vergara y Verónica, 2013).*

Un segundo trabajo, de *Chuqui (2013)*, en donde se involucra un sensor de huellas digitales, consiste en el desarrollo de un sistema de registro de horas de empleados, utilizando el reconocimiento de huella dactilar. La aplicación del sistema se realiza con ayuda del lenguaje de programación *C#* y para el almacenamiento de la información se utiliza la base de datos *SQL Server* 2008 *(Chuqui, 2013).*

Otro proyecto de *Oke, et al. (2009),* es un sistema cuya implementación se desarrolla en lenguaje de programación *Mikrobasic* con un microcontrolador *PIC*. El sistema consta de cuatro etapas: el lector de tarjetas, la etapa de potencia que se compone de un relé electromecánico para la puerta, la programación de un microcontrolador y la fuente de alimentación. El objetivo de este trabajo es tener un prototipo de un sistema de seguridad para puertas diseñado con el fin de permitir que un usuario privilegiado acceda sin llave, en el cual la autenticación se realiza mediante identificación por radiofrecuencia *(Oke, et al., 2019).*

Dentro de los sistemas de acceso más recientes se pueden encontrar aquellos que involucran procesamiento de imágenes como el reconocimiento facial mediante cámaras instaladas en los accesos, como lo muestra el trabajo de Vega, et al. (2018), que se conforma de cinco nodos de lectura y un nodo de validación. En los nodos de lectura se recopila la información de la tarjeta *RFID* y la imagen del rostro (mediante una cámara de video) del usuario que desea acceder a un área correspondiente, para posteriormente enviarlo al nodo de validación mediante *wi-fi.* Cada nodo de lectura está compuesto por: una tarjeta *Raspberry Pi Zero W*, un lector de tarjetas *RFID*, una cámara de video y una interfaz de salida. El nodo de validación se compone de los mismos elementos que los nodos de acceso, más una pantalla táctil para la interfaz de usuario *(Vega, et al., 2018).*

Como resumen a toda la investigación realizada, se tiene que las principales técnicas de autentificación de personas para los sistemas de control de acceso son el reconocimiento de huella, que consiste en que una persona coloque su dedo en un sensor de huella digital por unos segundos para ser reconocido; la tecnología *RFID* en la cual se utilizan ondas de radio, que generalmente es una tarjeta con una membrana electrónica, que basta con colocarla cerca del receptor para identificar el usuario; el reconocimiento facial, en el cual se coloca la cara a manera de que la cámara integrada en el sistema detecte el rostro para ser identificado; y la autenticación por medio de una clave numérica, en la que se debe ingresar una contraseña por medio de un teclado, que será diferente en cada usuario.

1.2. Descripción Del Problema

La Universidad Autónoma de Querétaro ha sido blanco de robos en sus instalaciones. Ejemplo de ello son los robos ocurridos en 2016 en la Facultad de Ciencias Naturales, en la Facultad de Ingeniería, en la Facultad de Ciencias Políticas y Sociales y en dos ocasiones en el campus Tequisquiapan, de la misma institución *(Estrada, 2016).*

En el 2018, en la Facultad de Bellas Artes y en la Facultad de Informática también acontecieron robos dentro de sus instalaciones, en el que las autoridades universitarias aproximaron el monto de lo robado a los 60 mil pesos mexicanos *(Polenciano, 2018).*

Aunado a lo anterior, en el Laboratorio de Mecatrónica, dentro de la Facultad de Ingeniería de la Universidad Autónoma de Querétaro, se requiere controlar el acceso de los usuarios, donde también se ha sufrido de daños a la infraestructura y pérdida de equipo y material. El sistema de control de acceso a instalaciones que se plantea diseñar debe ser capaz de reconocer a los usuarios permitidos, así como mantener la información a pesar de interrupciones en la energía eléctrica.

1.3. Justificación

Actualmente es indispensable contar con un control de acceso a ciertos espacios, sobre todo si son áreas donde se encuentra equipo costoso, como lo son equipo de cómputo, material de laboratorio, máquinas y herramientas, etc. Esto se da generalmente en edificios de escuelas, centros de investigación, laboratorios de cómputo u hospitales.

Por lo anterior, es de primordial importancia tener un sistema de control de acceso que nos brinde mayor seguridad de que solamente acceden aquellos que estén autorizados.

Controlar el acceso de personas a un lugar se puede lograr al tener un prototipo que pueda almacenar la información de los usuarios permitidos, ya sea con una base de datos de sus huellas dactilares o de claves numéricas, así como un identificador *ID* para cada usuario permitido.

A pesar de que existen muchas alternativas comerciales hoy en día, son soluciones caras y no es posible realizar adecuaciones a las mismas, de acuerdo con las necesidades particulares de cada lugar. El que desarrollemos nuestra propia tecnología de acceso, nos permite tener la versatilidad de poder personalizar el prototipo.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar e implementar el prototipo de un sistema de control de acceso a lugares específicos, basado en un microcontrolador, utilizando identificación por teclado y sensor biométrico.

1.4.2. Objetivos Específicos

a. Realizar la comunicación de un sensor biométrico con un microcontrolador *PIC*.

b. Realizar la comunicación de un teclado matricial con un microcontrolador *PIC*.

c. Usar la memoria *EEPROM* interna de un microcontrolador *PIC* para almacenar las contraseñas.

d. Diseñar la tarjeta de circuito impreso de la electrónica a utilizar, para la implementación en campo del sistema digital.

e. Realizar pruebas reales al sistema para evaluar el desempeño.

1.5. Estado del arte

Los sistemas biométricos se han investigado y probado por algunas décadas, pero han entrado recientemente en auge debido a los grandes avances de procesamiento informático y la ampliación de la comunicación. Además, obligados a cumplir la creciente demanda de seguridad, que surge en la medida que la tecnología avanza, para así reducir la suplantación de las personas *(Giraldo y Gómez, 2017).*

1.5.1. Normalización de la biometría

La normalización entorno a la biometría inició alrededor de los años ochenta cuando surgieron los estándares que permitieron realizar el intercambio de datos. Entre estos se encuentran varios organismos internacionales de normalización como la comisión electrónica internacional (*IEC*) y el sector de telecomunicaciones (*UIT-T*). A mediados de los años noventa se genera la necesidad de la creación de interfaces comunes en donde se involucra el sector privado, lo que logra que en el año de 2002 se realice la conformación del subcomité de identificación biométrica debido al creciente interés de diferentes autoridades *(Giraldo y Gómez, 2017).*

1.5.1.1. Sector de normalización de telecomunicaciones UIT

El *UIT-T X34* Organismo del Sector de las Telecomunicaciones, inició los trabajos sobre biometría alrededor del año 2001, con la responsabilidad del estudio de la identidad y las metodologías adecuadas para identificar los individuos, así como la protección de la identidad *(Giraldo y Gómez, 2017).*

1.5.1.2. Estándar internacional ISO/IEC

Esta norma internacional proporciona orientación para la protección de la información biométrica bajo varios requisitos de confidencialidad e integridad, durante el almacenamiento y la transferencia de datos biométricos. Además, este estándar provee requisitos y pautas para la gestión y el procesamiento seguros, conforme a la privacidad de la información biométrica *(Norma Internacional ISO/IEC).*

1.5.2. Tendencias en sistemas de seguridad

En la actualidad existen en el mercado muchos proveedores que suministran cerraduras inteligentes, siendo los dispositivos de identificación biométrica los más comunes, que poseen sensores de acuerdo a la autenticación ya sea por huella dactilar, facial, iris, voz, etc. También son frecuentes las cerraduras de radiofrecuencia, que son aquellas que emplean tarjetas o llaveros electrónicos que dan acceso al acercarlos a un lector digital. Es usual encontrar estos tipos de reconocimiento de personas en accesos a oficinas, aportando un alto nivel de seguridad.

Hoy en día los sistemas de control de acceso combinan varios mecanismos de seguridad. Existen sistemas híbridos que combinan dos o más técnicas de autenticación, por ejemplo, los que tienen código numérico y huella dactilar, huella dactilar y reconocimiento de iris, algunos con identificación *RFID* y huella dactilar, etc.

Se investigan tres empresas que se dedican a la venta y/o renta de equipos de sistemas de control de acceso, las cuales brindan sus servicios en México. A continuación, se da una breve explicación de cada una y del equipo más sofisticado que ofrecen.

La empresa mexicana *Sistemas en Electrónica* ofrece soluciones de seguridad para el hogar, negocio u oficinas. Los modelos de control de acceso con los que cuenta se observan en la Tabla 1.

Modelo: *ZKTeco K40*  Costo: MXN $3,199.00	✓ Acceso por huella dactilar y/o contraseña ✓ Capacidad de 1000 huellas ✓ Control de asistencia ✓ Pantalla *TFT* de 2.8 pulgadas ✓ Bateria de respaldo
Modelo: *ZKTeco X629-c*  Costo: MXN $3,899.00	✓ Acceso por huella dactilar ✓ Pantalla *TFT* de 3 pulgadas ✓ Capacidad de 3000 huellas ✓ Reloj checador
Modelo: *Face AXS*  Costo: MXN $8,949.00	✓ Acceso por reconocimiento facial y/o *RFID* ✓ Pantalla *TFT* de 3.5 pulgadas ✓ Capacidad para 1000 usuarios ✓ Control de asistencia

Tabla 1. Modelos de sistemas de control de acceso *(Sistemas en electrónica).*

La compañía *Cucorent México* cuenta con equipo para control de accesos y asistencia, ya sea para venta o renta. La Tabla 2 muestra algunos de sus productos más destacados.

Modelo: *Access Finger VI*  Costo: € 508	✓ Acceso por huella dactilar ✓ Capacidad para 10000 usuarios ✓ Pantalla *TFT* de 3.5 pulgadas ✓ Control de asistencia
Modelo: *Access Finger IP 65*  Costo: € 391	✓ Acceso por huella digital y por *RFID* ✓ Carcasa anti-vandálica. Sin display ni teclado ✓ Menú guiado por voz ✓ Capacidad de 1000 huellas ✓ Capacidad de 10000 tarjetas de proximidad
Modelo: *JARA*  Costo: € 560	✓ Acceso por reconocimiento facial, por huella digital y/o contraseña ✓ Capacidad de 3000 huellas ✓ Capacidad de 700 rostros ✓ Pantalla a color de 4.3 pulgadas

Tabla 2. Modelos de sistemas de control de acceso *(Cucorent).*

DR SECURITY es una empresa especializada en Tecnologías de Seguridad dedicada a la fabricación, importación y distribución en México de los más avanzados productos de seguridad. Algunos ejemplos de los productos para control de accesos con tecnología biométrica que maneja dicha empresa se observan en la Tabla 3.

Modelo: *ANVIZ*  Costo: MXN $10,799.00	✓ Acceso por huella digital, *RFID* y/o contraseña ✓ Capacidad de 35000 huellas ✓ Capacidad de 35000 tarjetas *RFID* ✓ Pantalla *TFT* de 3.5 pulgadas
Modelo: *ZK Iface800*  Costo: MXN $7,400.00	✓ Acceso por huella digital o reconocimiento facial ✓ Almacena hasta 2000 huellas y 1200 rostros ✓ Comandos audiovisuales ✓ Pantalla tactil a color de 4.3 pulgadas
Modelo: *IRS TD100*  Costo: USD $1895	✓ Acceso por reconocimiento de iris y/o facial ✓ Display *LCD* de 3.5 pulgadas ✓ Distancia de operación de 14 pulgadas

Tabla 3. Modelos de sistemas de control de acceso *(DR SECURITY).*

Como se puede observar en la anterior investigación, la mayoría de los equipos de control de acceso que se encuentran actualmente en el mercado mexicano usan el reconocimiento de huella dactilar, siendo ésta la tecnología biométrica más comúnmente usada. Con base en dicha información, para este prototipo, se opta por utilizar dos técnicas que permiten identificar a una persona en particular, mediante reconocimiento de huella dactilar y por identificación de contraseña.

En el siguiente capítulo se explican los conceptos clave que se relacionan con toda la investigación y el desarrollo del proyecto. En el capítulo 3, se detalla la metodología seguida en este trabajo, es decir, los pasos que se ejecutaron. En el capítulo 4, se muestran los resultados obtenidos, así como las pruebas a las que se sometió el prototipo final. Por último, en el capítulo 5, se da una conclusión y cierre a la investigación realizada.

Capítulo 2. Marco teórico

La implementación del proyecto está basada en un microcontrolador. A continuación, se explica más a detalle los conceptos relacionados a la investigación y al desarrollo del prototipo aquí presentado.

2.1. Microcontrolador

Un microcontrolador es una microcomputadora digital dentro de un circuito integrado *(chip)*. Una microcomputadora se compone de tres bloques fundamentales: el *CPU (Central Processing Unit)* o microprocesador, una memoria para almacenar el programa, una memoria para almacenar datos y los periféricos. Los bloques se conectan entre sí mediante grupos de líneas eléctricas que tienen un uso común, y se denominan buses. Los buses pueden ser de direcciones, de datos o de control. El *CPU* es el "cerebro" de la microcomputadora y actúa bajo el control del programa almacenado en la memoria. A diferencia de los microprocesadores de propósito general, como los que se usan en los computadores *PC*, los microcontroladores son unidades autosuficientes y más económicas *(Valdez, 2007), (Torriti, 2007).*

El esquema básico de un microcontrolador se puede observar en la Figura 1.

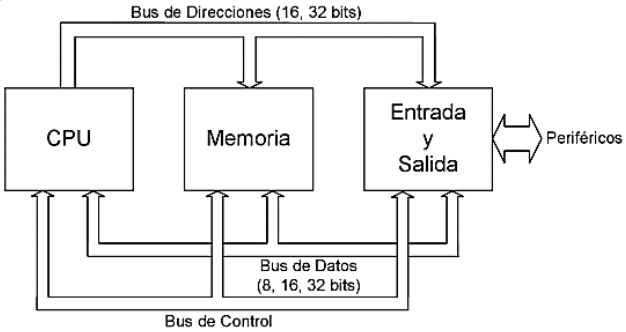


Figura 1. Esquema básico de un microcontrolador. Fuente: *(Valdez, 2007).*

El funcionamiento de los microcontroladores está determinado por el programa almacenado en su memoria. Este puede escribirse en distintos leguajes de programación. Además, la mayoría de los microcontroladores actuales pueden reprogramarse repetidas veces. Por las características mencionadas y su alta flexibilidad, los microcontroladores son ampliamente utilizados como el cerebro de una gran variedad de sistemas embebidos que controlan máquinas, componentes de sistemas complejos, como aplicaciones industriales de automatización y robótica, domótica, equipos médicos, sistemas aeroespaciales, e incluso dispositivos de la vida diaria como automóviles, hornos de microondas, teléfonos y televisores. Frecuentemente se emplea la notación *µC* o las siglas *MCU (Microcontroller Unit)* para referirse a los microcontroladores *(Torriti, 2007).*

2.1.1. Características de los microcontroladores

Las principales características de los microcontroladores son:

- Unidad de Procesamiento Central *(CPU)*: Típicamente de 8 bits, pero también las hay de 4, 32 y hasta 64 bits con arquitectura *Harvard*, con memoria/bus de datos separada de la memoria/bus de instrucciones de programa, o arquitectura de *von Neumann*, también llamada arquitectura *Princeton*, con memoria/bus de datos y memoria/bus de programa compartidas.

- Memoria de Programa: Es una memoria *ROM (Read-Only Memory)*, *EPROM (Electrically Programable ROM)*, *EEPROM (Electrically Erasable/Programable ROM)* o *Flash* que almacena el código del programa que típicamente puede ser de 1 kilobyte a varios megabytes.

- Memoria de Datos: Es una memoria *RAM (Random Access Memory)* que generalmente puede ser de 1, 2 4, 8, 16 o 32 kilobytes.

- Generador del Reloj: Usualmente un cristal de cuarzo de frecuencias que genera una señal oscilatoria de entre 1 a 40 *MHz*, o también resonadores o circuitos *RC*.

- Interfaz de Entrada/Salida: Puertos paralelos, seriales (*UARTs, Universal Asynchronous Receiver/Transmitter*), *I2C* (*Inter-Integrated Circuit*), Interfaces de Periféricos Seriales (*SPI, Serial Peripheral Interface*), Red de Área de Controladores (*CAN, Controller Area Network*), *USB* (*Universal Serial Bus*).

- Conversores Analógicos-Digitales (*A/D, analog-to-digital*) para convertir un nivel de voltaje en un cierto pin a un valor digital manipulable por el programa del microcontrolador.

- Moduladores por Ancho de Pulso (*PWM, Pulse-Width Modulation*) para generar ondas cuadradas de frecuencia fija, pero con ancho de pulso modificable.

La alta integración de subsistemas que componen un microcontrolador reduce el número de *chips*, así como la cantidad de pistas y espacio que se requeriría en un circuito impreso si se implementase un sistema equivalente usando *chips* separados *(Torriti, 2007).*

2.1.2. Interrupciones externas en los microcontroladores

Para responder a eventos externos, los microcontroladores cuentan con un recurso conocido como interrupciones. Las interrupciones son señales que se generan internamente en el microcontrolador que detienen la ejecución normal del programa para ejecutar alguna subrutina de respuesta al evento. Una vez ejecutada la subrutina de interrupción, la ejecución del programa continúa en el punto en que se encontraba antes de generarse la interrupción. Un ejemplo típico es el de un botón pulsador conectado a un pin de entrada; una vez pulsado, se genera una señal de interrupción que iniciará la ejecución de la subrutina de interrupción, que por ejemplo podría activar un pin de salida para encender un *LED (Torriti, 2007).*

2.1.3. Comunicación serial en los microcontroladores

La comunicación serie consiste en el envío de *bits* de información de manera secuencial a través de una única línea. Este tipo de comunicación difiere completamente de la comunicación en paralelo que consiste en enviar simultáneamente un conjunto de datos a

través de varias líneas. De esta manera se conseguiría una velocidad de transmisión mayor, ya que se enviaría un grupo de *bits* a la vez, en vez de uno. La gran desventaja de la comunicación en paralelo es que se requiere una gran cantidad de hilos conductores, pues debe ser establecido un hilo para cada bit de datos, además de las señales de control. Esto encarece notablemente la comunicación en función de la distancia. Por el contrario, la comunicación serie solo requiere 2, 3 o 4 hilos a lo más *(Díaz, 2015)*.

2.1.3.1. Protocolo de comunicación UART

La principal característica de la comunicación *UART* (*Universal Synchronous Receiver-Transmitter*) consiste en que no se intercambia la señal de reloj entre emisor y receptor. Dado que no se tiene un reloj, la comunicación se puede iniciar en cualquier momento. Esto conlleva que cada dispositivo opera con su propio reloj y por tanto se debe acordar una velocidad de transmisión de datos o *baud rate*. En la Figura 2 se observa la trama de datos de la comunicación serie asíncrona. En este caso, la comunicación se compone de dos líneas de datos *(Díaz, 2015)*.

- *TxD*: es la línea de transmisión de datos
- *RxD*: es la línea de recepción de datos

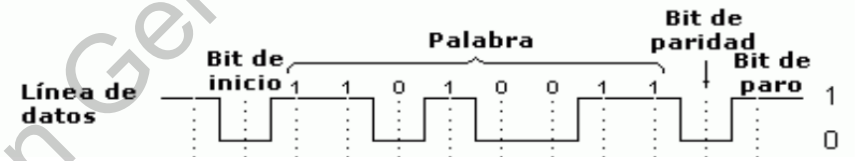


Figura 2. Trama de datos del protocolo de comunicación *UART*. Fuente: *(Rivero, 2018).*

Cada carácter transmitido se compone de los siguientes bits:

- Bit de inicio: es el bit encargado de marcar el inicio de la comunicación. Este bit presenta valor lógico 0.

- Bits de datos: estos bits componen la información que interesa transmitir. Generalmente suelen ser 7 u 8 datos, aunque hay otras configuraciones.

- Bit de paridad: este bit es útil para detectar errores en la transmisión de la información. Se puede emplear tanto paridad par como impar.

- Bit de parada: este bit determina la finalización de la transmisión de un carácter. Este bit tiene valor lógico 1 *(Díaz, 2015)*.

2.1.3.2. Protocolo de comunicación SPI

El bus *SPI* es un estándar de comunicación empleado principalmente para el intercambio de información entre circuitos integrados de sistemas electrónicos. Es un estándar válido para controlar casi cualquier dispositivo electrónico digital que acepte un flujo de datos en serie controlados por un reloj. Nos encontramos ante un protocolo síncrono *(Díaz, 2015)*. En la Figura 3 se observa la trama de datos del protocolo de comunicación *SPI*.

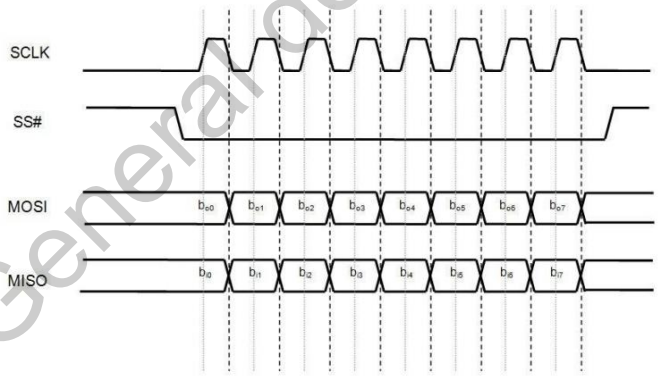


Figura 3. Trama de datos del protocolo de comunicación SPI. Fuente: *(Díaz, 2015)*.

La trasmisión de datos se consigue mediante cuatro líneas:

- *SCLK*: A través de esta línea el maestro manda la señal de reloj a los dispositivos esclavos.

- *MOSI* (*Master Output Slave Input*): Es una línea de intercambio de datos. Concretamente la salida del maestro y la entrada del esclavo.

- *MISO* (*Master Input Slave Output*): Es otra línea de transmisión de datos. A diferencia de la línea *MOSI*, en este caso nos encontramos ante la salida del esclavo y la entrada del maestro.

- *SS* (*chip select*): mediante esta línea el maestro activa el esclavo con el que se intercambia la información *(Díaz, 2015)*.

2.1.4. Memoria en un microcontrolador

La memoria de un microcontrolador es el lugar donde son almacenados las instrucciones del programa y los datos que manipula. En un microcontrolador siempre hay dos tipos de memoria: la memoria *RAM* (*Random Access Memory*) y la memoria *ROM* (*Read Only Memory*). La memoria *RAM* es una memoria de lectura y escritura, que además es volátil, es decir, pierde la información almacenada cuando falta la energía que alimenta la memoria. La memoria *ROM* es una memoria de solo lectura y no volátil.

Un número creciente de microcontroladores dispone de alguna memoria no volátil de tipo *EEPROM* (*Electrically Erasable Programmable Read Only Memory*) para almacenar datos fijos o que solo sean cambiados esporádicamente *(Valdez, 2007).*

2.1.4.1. Memoria RAM

La memoria *RAM* es una memoria de lectura y escritura. Hay dos variantes: la estática y la dinámica. En la memoria *RAM* estática la información almacenada permanece estable indefinidamente mientras no se suprima la tensión de alimentación. Eso las diferencia de las memorias *RAM* dinámicas, que requieren un refrescamiento periódico de la información almacenada. Las *RAM* dinámicas se usan profusamente en los ordenadores personales, pero no en los microcontroladores *(Valdez, 2007).*

2.1.4.2. Memoria ROM

En los microcontroladores que utilizan memoria *ROM*, la información se graba durante el proceso de fabricación del dispositivo y no puede ser alterada ulteriormente. Por ello, la información que se desea grabar en la memoria, que puede ser el programa y algunos datos, debe haber sido comprobada y depurada minuciosamente antes de encargar la fabricación del microcontrolador *(Valdez, 2007).*

2.1.4.3. Memoria FLASH

En las memorias *FLASH* se pueden leer y escribir celdas individualmente, aunque, en general, para escribir en una celda hay que borrar primero su información. El borrado de estas memorias se realiza por bloques de celdas de memoria, no celda a celda. Esto las distingue de las memorias *EEPROM*. La memoria se puede borrar o escribir un numero finito de veces (del orden de 10^5) *(Valdez, 2007)*.

2.1.4.4. Memoria EEPROM

La memoria *EEPROM*, o memoria *FLASH* de datos, es una memoria no volátil de lectura y escritura. La escritura de la memoria se realiza por medios eléctricos. Las celdas pueden ser escritas individualmente sin una operación previa de borrado. La memoria se puede reprogramar un número finito, aunque muy grande, de veces (del orden de 10^6) *(Valdez, 2007).*

2.1.5. Microcontrolador PIC18F46K22

El *PIC18F46K22* es un microcontrolador del fabricante *Microchip*, algunas de sus características son:

- Amplio rango de voltaje de operación (2.3V A 5.5V)
- 64 Kbytes de memoria *FLASH* de programa
- 1024 bytes de memoria *EEPROM* de datos

- 3896 bytes de memoria *RAM*
- 36 pines de entradas/salidas
- 30 canales *A/D* (10 bit)
- 2 puertos *SPI, I2C* o *RS232*
- 3 módulos temporizadores de 8 bit
- 4 módulos temporizadores de 16 bit

El diagrama del microcontrolador es mostrado en la Figura 4 *(Microchip).*

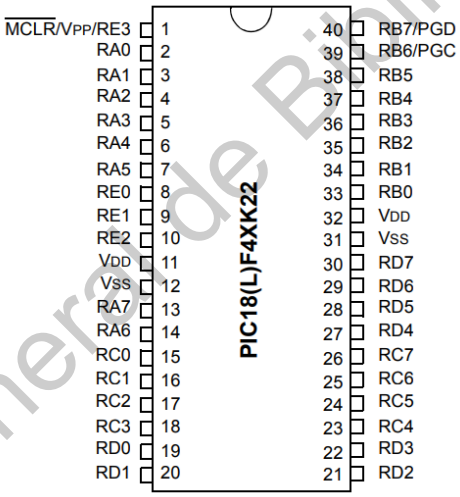


Figura 4. Diagrama del microcontrolador *PIC18F46K22*. Fuente: *(Microchip).*

2.2. Tecnologías de reconocimiento de personas

Dentro de los métodos comúnmente usados en los sistemas de seguridad se encuentran las técnicas de identificación biométrica, la autenticación por contraseña y los que se basan en tecnología de radiofrecuencia.

2.2.1. Identificación por contraseña

La autenticación por contraseña o clave se basa en que el usuario utilice un código para identificarse, que normalmente suele ser una combinación de números o letras. Es económico, práctico y no se necesita de algún objeto físico como podrían ser unas llaves. La Figura 5 ejemplifica un sistema en el que se ingresa una clave *(Ocas, et al., 2019).*

Figura 5. Acceso por contraseña. Fuente: *(Ocas, et al., 2019).*

2.2.2. Identificación por radiofrecuencia (RFID)

En este tipo de reconocimiento de personas, el usuario tiene un artículo identificador, que puede ser una tarjeta o un llavero electrónico.

En el funcionamiento de los sistemas *RFID* son necesarios dos elementos básicos: el dispositivo electrónico (*TAG*) y un lector. Un *TAG* es un elemento que puede almacenar y transmitir información hacia un elemento lector utilizando ondas de radiofrecuencia. El *TAG* y el lector deben estar sintonizados a la misma frecuencia. Lo que ocurre es que cuando se enciende el lector, este empieza a emitir una señal a una frecuencia previamente establecida y cualquier *TAG* que esté asociado a este lector que se encuentre en la proximidad del sensor, detectará la señal y enviará respuesta al lector con la información que contiene en forma de señales de radio modulada. En la Figura 6 podemos observar de manera general el funcionamiento de un sistema *RFID (Montenegro y Marchesin, 2017), (Gordón, 2009).*

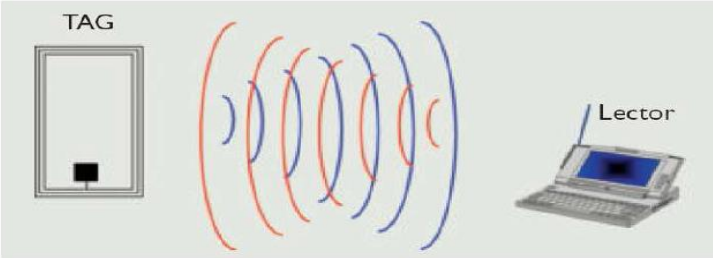


Figura 6. Ejemplo de un sistema RFID. Fuente: *(Gordón, 2009).*

2.2.2.1. Protocolo de comunicación RFID

La trama de datos del protocolo de comunicación *RFID* está conformada como se muestra en la Figura 7 *(Bateman, et al., 2009)*, y en la siguiente lista se definen los términos que están siendo usados.

- *SOF* (*start of frame*): indica el inicio de la trama (1 byte)
- *Length* (longitud de la trama): puede o no incluir la trama de *SOF* (1 byte).

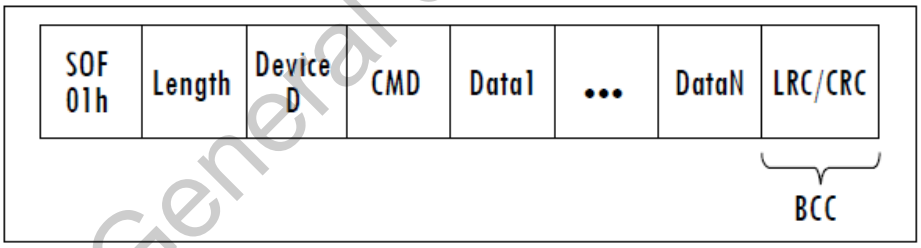


Figura 7. Organización de campos para el protocolo de comunicación RFID. Fuente: *(Bateman, et al., 2009).*

- *Device ID*: es el número de identificación del módulo/tarjeta (1 byte).
- *CMD* (*command*): es el código del comando que indica la operación que se va a realizar (1 byte).
- *Data*: en estos campos va la información deseada para la aplicación (desde 1 hasta 1000 bytes).

- *LRC/CRC*: técnicas aplicadas para el control de errores (1 byte).

2.2.3. Sistemas de identificación biométrica

La biometría es una ciencia que analiza patrones, es decir, las distancias y posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas. Hay varios rasgos biométricos que hoy en día se usan para tal fin, como las huellas dactilares, la cara, el iris, la mano o la retina. La biometría, y más en concreto las huellas dactilares, ya se estudiaban a finales del siglo XIX en aplicaciones forenses. En la actualidad, no solo se usa en estas aplicaciones sino en otras, como el control en los aeropuertos, en los accesos a centrales nucleares, instalaciones militares o incluso, simplemente, para acceder a edificios de oficinas *(Serratosa, 2012).*

2.2.3.1. Reconocimiento facial

Los sistemas basados en reconocimiento facial clasifican la apariencia de la persona e intentan medir algunos puntos nodales del rostro como la distancia entre los ojos, el ancho de la nariz, la distancia del ojo a la boca, o la longitud de la línea de la mandíbula. El análisis tridimensional de la cara elimina algunos inconvenientes que se pueden tener en un reconocimiento bidimensional, como son: la iluminación y las sombras, la orientación o pose de la cara, y la variación de expresiones faciales. El reconocimiento de rostro es un método no invasivo *(Osorio, et al., 2010).* En la Figura 8 se observan puntos comunes que se miden en la biometría del rostro.

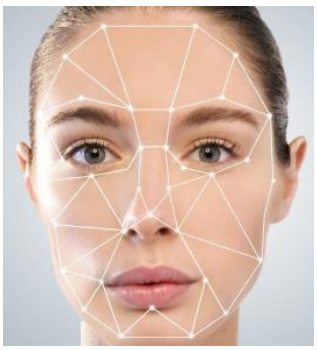


Figura 8. Biometría del rostro. Fuente: *(Serban).*

2.2.3.2. Reconocimiento de iris

La textura visual del iris humano se determina por el proceso caótico y morfo-genético durante el desarrollo embrionario. Se ha postulado ser distintivo para cada persona y cada ojo. Es usual que se capture una imagen del iris usando un proceso de captura sin contacto. Normalmente, la captura de una imagen del iris implica la cooperación del usuario, aunque hay sistemas (en fase de prototipo en el laboratorio) para capturar la imagen del iris sin colaboración por parte del usuario. El usuario colabora ubicando la imagen en el centro del aparato de captura y asegurándose de que el iris está a una distancia predeterminada al plano focal de la cámara. La tecnología del iris ha demostrado ser muy precisa y rápida. En la Figura 9 podemos observar el esquema del ojo humano *(Serratosa, 2012).*

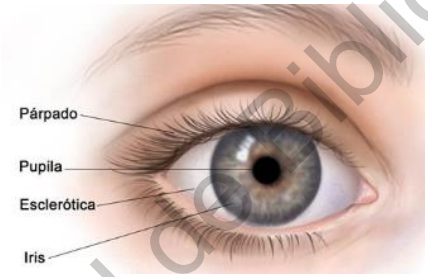


Figura 9. Iris del ojo humano. Fuente: (Instituto Nacional del Cáncer).

2.2.3.3. Reconocimiento de huella

Una huella dactilar normalmente está conformada por una serie de líneas oscuras que representan las crestas y una serie de espacios blancos que representan los valles. Se ha determinado empíricamente que las huellas de gemelos y las huellas de diferentes dedos de una persona son diferentes. Además, desde hace más de un siglo, se ha demostrado que es una tecnología altamente confiable, incluso basándose en datos de más de 50 millones de usuarios. La identificación con huellas dactilares está basada principalmente en la ubicación y dirección de las terminaciones de bifurcaciones, deltas, valles y crestas. El reconocimiento de huella es una tecnología útil en aplicaciones forenses, así como en aplicaciones civiles y de máxima seguridad *(Serratosa, 2012), (Osorio, et al., 2010)*. En la Figura 10 se pueden observar las principales líneas de una huella dactilar.

Figura 10. Líneas de una huella dactilar. Fuente: *(Osorio, et al., 2010).*

2.2.3.4. Reconocimiento de voz

El reconocimiento de voz de una persona utiliza la información dada por las ondas de sonido emitidas. Se ha podido comprobar que los patrones con que una persona dice una palabra son únicos. En general, los sistemas de reconocimiento de voz tienen dos módulos principales: extracción de características y comparación de características.

La extracción de las características consiste en la digitalización de diferentes palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se obtienen 3 o 4 tonos dominantes que son capturados en forma digital y almacenados en una tabla o espectro, que se conoce con el nombre de plantilla de la voz. La comparación de características involucra el proceso de identificar a la persona desconocida comparando las características extraídas de su voz, con las previamente obtenidas, que corresponden a las personas conocidas por el sistema *(Osorio, et al., 2010).* En la Figura 11 se muestra el espectro de la voz humana.

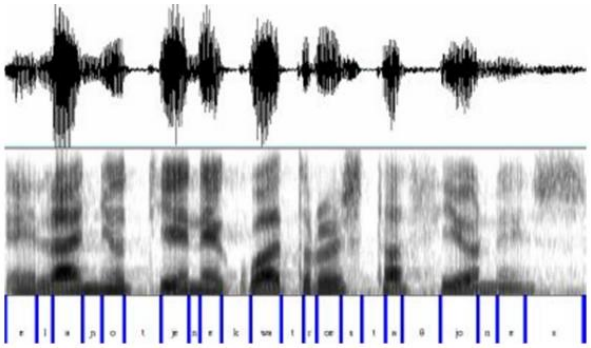


Figura 11. Espectro de la voz humana. Fuente: *(Osorio, et al., 2010).*

De las anteriores tecnologías, se elige para el desarrollo del proyecto la identificación biométrica por huella dactilar y la identificación por contraseña. A continuación, se explican los conceptos relacionados a esto.

2.3. Sensor

Es un dispositivo que está diseñado para recibir y transformar información. Un sensor detecta una determinada acción externa, temperatura, presión, etc. y la transmite adecuadamente. Son dispositivos que nos permiten interactuar con el entorno, de forma que nos proporcionan información de ciertas variables que nos rodean para poder procesarlas y así generar órdenes o activar procesos *(Serna, 2010).*

2.3.1. Sensor de huella dactilar

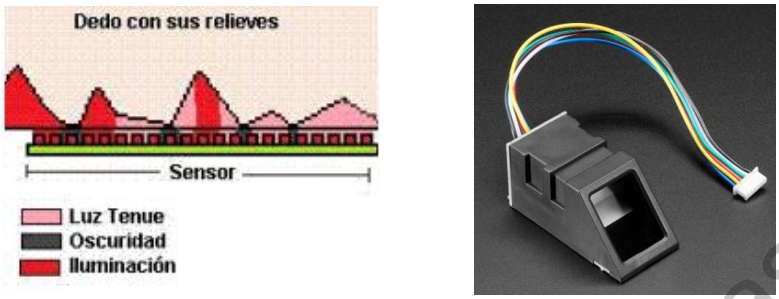
Las imágenes en un sensor de huella se obtienen mediante la adquisición directa de la huella dactilar al colocar el dedo sobre la superficie sensible del sensor electrónico.

Un sensor de huella dactilar lleva a cabo dos tareas: obtener una imagen de la huella y convertirla a una imagen digital y comparar el patrón de valles y crestas de dicha imagen con los patrones de las huellas que tiene almacenadas dentro del sensor. Dependiendo de los principios físicos de funcionamiento del sensor utilizado, se establece la siguiente clasificación de los sensores *(Chulde, 2017), (López, 2009).*

2.3.1.1. Sensores de huella ópticos

Este tipo de sensores se basa en la reflexión de la luz sobre la yema de dedo. En el momento en el que el dedo se apoya sobre la superficie de cristal del sensor (prisma), un diodo LED proyecta un haz de luz difusa por debajo del cristal. La luz que atraviesa el prisma incide sobre las crestas de la huella y se dispersa, reflejándose de manera aleatoria en múltiples direcciones. La luz que incide en el interior de la estructura de crestas (valles) se refleja en una determinada dirección (reflexión total). Esta luz direccional es focalizada mediante un sistema de lentes hacia un dispositivo *CCD* o *CMOS*, capturándose así la

imagen de la huella dactilar *(López, 2009).* En la Figura 12 se muestra la tecnología interna del sensor de huellas óptico y un sensor óptico comercial.



(a) (b)

Figura 12. Sensor de huella óptico. (a) Funcionamiento interno del sensor óptico. (b) Sensor óptico comercial. Fuentes: *(Chulde, 2017), (Adafruit).*

2.3.1.2. Sensores de huella capacitivos

Estos dispositivos se forman por la distribución de un conjunto de micro-capacitores en una superficie plana, sobre la cual se extiende un dieléctrico. Todas las placas conductoras a un lado del dieléctrico forman eléctricamente el mismo punto. Las placas necesarias para completar los capacitadores aparecen al otro lado del dieléctrico cuando se coloca el dedo sobre la superficie. La superficie en contacto con el dedo necesita de una fina capa protectora con toma de tierra, resistente a la abrasión y a las posibles descargas electrostáticas de la piel. Estos sensores permiten el ajuste de algunos parámetros eléctricos con el fin de mejorar la calidad de la imagen adquirida cuando las condiciones de la piel no son las ideales (piel seca o húmeda). Presentan el inconveniente de que deben limpiarse a menudo, ya que la grasa y la suciedad empeoran la calidad de la imagen *(López, 2009).* En la Figura 13 se observa el funcionamiento de un lector capacitivo y un ejemplo de sensor comercial.

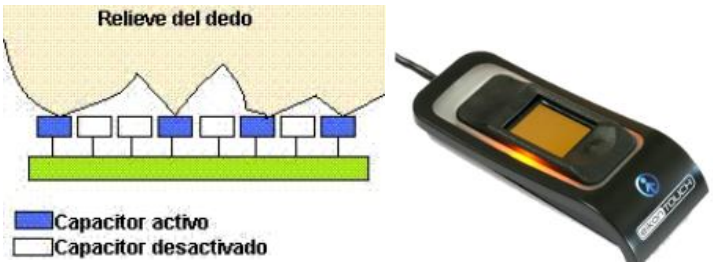


Figura 13. Sensor de huella capacitivo. (a) Funcionamiento del lector capacitivo. (b) Lector capacitivo comercial. Fuentes: *(Chulde, 2017), (Ratio Technologies).*

2.4. Teclado matricial

El teclado matricial es un simple arreglo de botones conectados en filas y columnas. Un teclado matricial 4x4 ocupa 4 líneas para las filas y otras 4 líneas para las columnas. Lo que permite leer 16 teclas utilizando solo 8 líneas de un microcontrolador *(Topón, 2017).* En la Figura 14 se observa la arquitectura interna de un teclado matricial, así como su apariencia comercial.

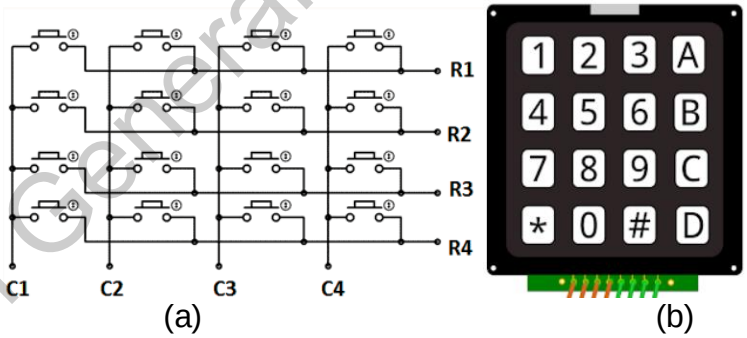


Figura 14. Arquitectura del teclado matricial. (a) Conexiones internas. (b) Teclado matricial comercial. Fuente: *(Arduino para todos, 2017).*

Para manejar un teclado matricial con un microcontrolador, es necesario manipular las filas y columnas de dicho teclado. Se considera las terminales de columna C1, C2, C3 y C4, como las terminales de entrada al teclado, y las terminales R1, R2, R3 y R4 como las de salida. Para saber que tecla ha sido oprimida, se utiliza la técnica de “barrido”. En esta técnica, se envía a la entrada, una secuencia lógica conocida. En las terminales de salida,

se puede leer ciertos valores lógicos, los cuales, al combinarlos con la secuencia de entrada, se puede saber cuál fue la tecla presionada.

2.5. Pantalla *LCD*

Las siglas *LCD* significan *("Liquid Cristal Display")* o pantalla de cristal líquido. Es una pantalla plana desarrollada por *Pierre-Gilles de Gennes*, basada en el uso de una sustancia líquida atrapada entre 2 placas de vidrio, haciendo que, al aplicar una corriente eléctrica a una zona específica, esta se vuelva opaca y contraste con la iluminación trasera. Este principio es aplicado, pero con ciertas modificaciones (ya que se utilizan 3 colores básicos para generar la gama de colores), lo cual permite la visualización de imágenes *(Informática Moderna).*

Las pantallas de cristal líquido tienen la capacidad de mostrar cualquier carácter alfanumérico, permitiendo representar la información que genera cualquier equipo electrónico de una forma fácil y económica *(Zambrano).*

La Figura 15 muestra el funcionamiento interno de una pantalla *LCD*, así como una *LCD* comercial.

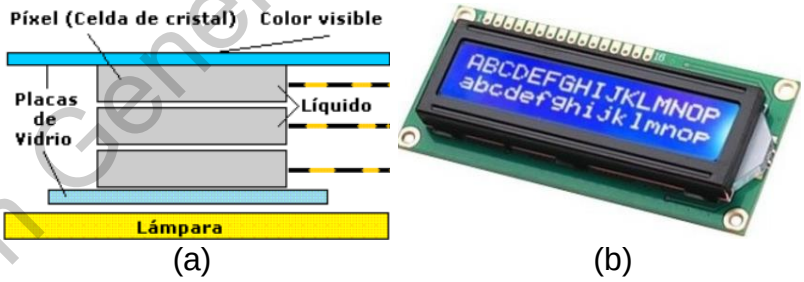


Figura 15. Pantalla *LCD*. (a) Funcionamiento interno. (b) *LCD* comercial. Fuentes: *(Informática Moderna), (Nomada Store)*.

2.6. Pantalla *TFT*

Las pantallas táctiles de transistor de película delgada (*TFT, Thin Film Transistor*) se tratan de pantallas táctiles resistivas con una tecnología basada en transistores de efecto de campo. Los píxeles son generados por dichos transistores, de manera que cada píxel es representado como un led, el cual emite una luz que pasa por diferentes filtros y de esta manera se determina el color que va a tomar el píxel en cada momento *(Loaiza, 2016), (Montenegro y Jonnathan, 2013).* En la Figura 16 podemos observar el funcionamiento interno de una pantalla *TFT*, así como su apariencia comercial.

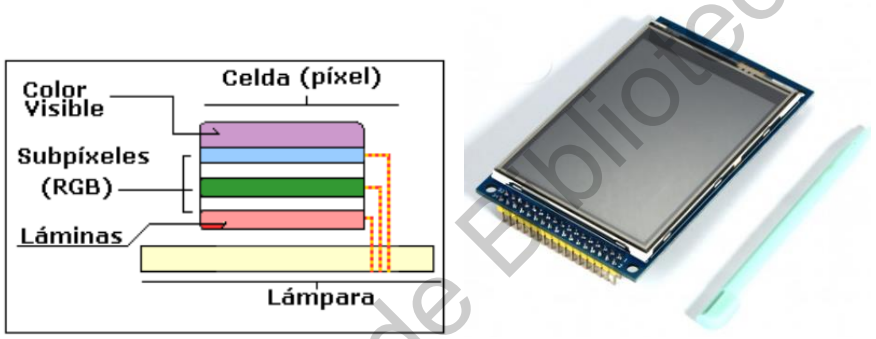


Figura 16. Pantalla *TFT*. (a) Funcionamiento interno. (b) Pantalla *TFT* comercial. Fuentes: *(Nomada Store), (Montenegro y Jonnathan, 2013).*

Capítulo 3. Metodología

La metodología empleada en el desarrollo del presente proyecto, se muestra en la Figura 17.

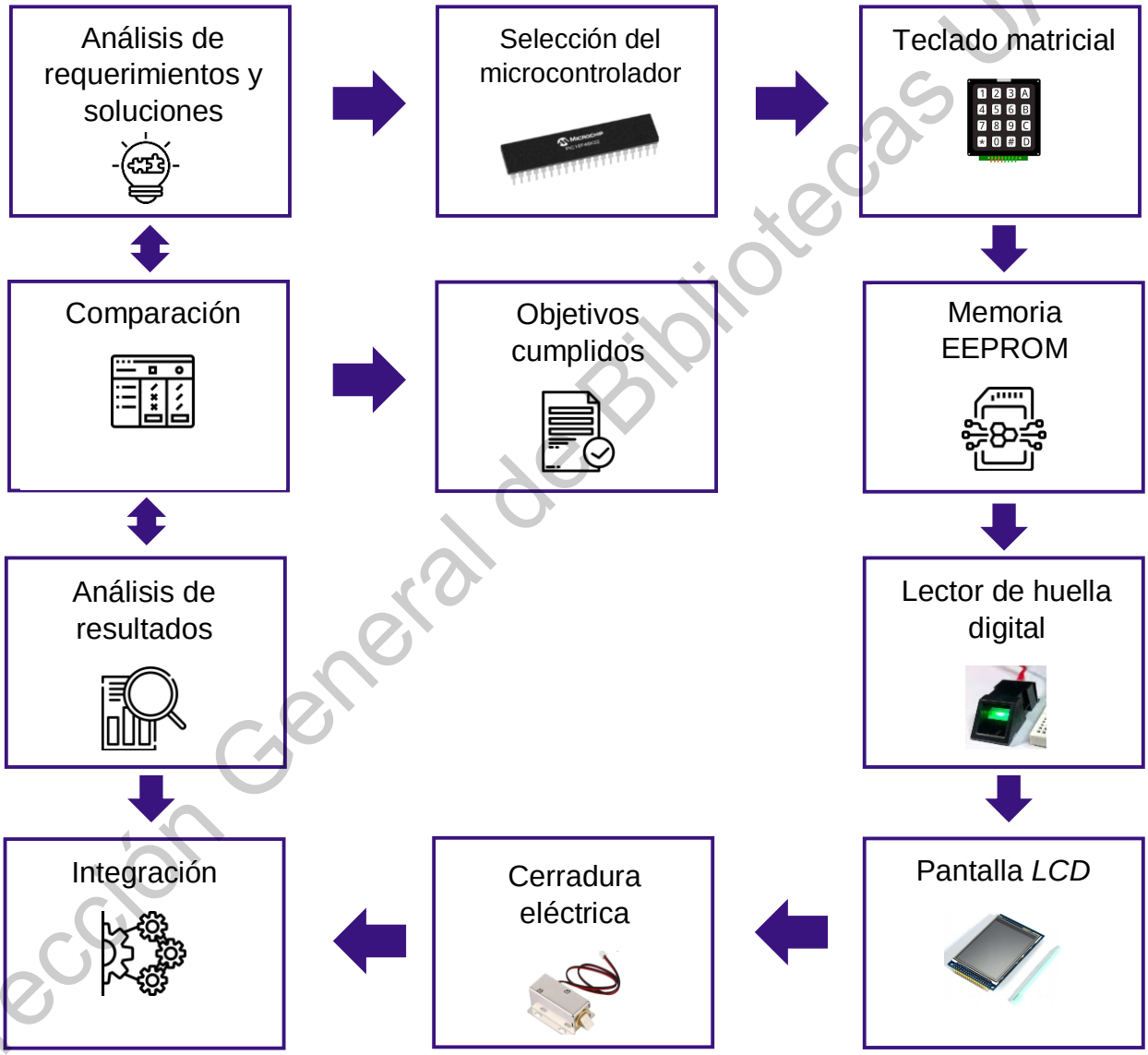


Figura 17. Diagrama de la metodología seguida.

A continuación, se describirá y detallará cada una de las etapas seguidas en la metodología.

3.1. Análisis de requerimientos y soluciones

El proceso comienza al realizar un análisis de los requerimientos, es decir, en plantear las necesidades y los alcances del proyecto, así como los objetivos que se espera cumplir al terminar el desarrollo del prototipo. También, se busca la documentación relacionada con el tema del proyecto y se comienza con la escritura de la tesis. Además, se hace una selección y análisis de los recursos que se pueden utilizar para alcanzar los objetivos, se estudian las tecnologías de reconocimiento de personas y se escogen las más factibles.

Los requerimientos establecidos son:

- Cada usuario tiene un medio de autenticación, ya sea por huella digital o contraseña numérica.
- Si se reconoce a un usuario permitido, el sistema le da acceso, de lo contrario, el proceso de verificación vuelve a comenzar.
- La información, tanto de huellas o contraseñas, debe almacenarse en un medio no volátil.
- Visualizar en una pantalla *LCD* el estatus, como interfaz de usuario.
- Tener un modo administrador para poder agregar y borrar usuarios.

3.2. Selección del microcontrolador

Las primeras etapas del proyecto se desarrollan con el modelo de microcontrolador *PIC18F4550*, una vez que se observa que no es suficiente la memoria interna *EEPROM* que éste maneja, se ve la opción de buscar un microcontrolador en el que se pueda tener una base de datos de los usuarios mucho mayor. Para este fin, se usa el microcontrolador *PIC18F46K22*. La Tabla 4 presenta una comparación entre ambos microcontroladores.

Característica	*PIC18F46K22* 40-pin PDIP	*PIC18F4550* 40-pin PDIP
Rango de voltaje de operación	2.3v a 5.5v	2.0v a 5.5v
Memoria *FLASH* de programa	64K bytes	32K bytes
Memoria *EEPROM* de datos	1024 bytes	256 bytes
Memoria *RAM* de datos	3896 bytes	2048 bytes
Número de pines de entrada/salida	36 pines	36 pines
Número de módulos *UART/SPI/I2C*	2 módulos	1 módulo

Tabla 4. Comparación entre el microcontrolador *PIC18F46K22* y *PIC18F4550.*

3.3. Teclado matricial

Se realiza la técnica de barrido para utilizar el microcontrolador *PIC18F46K22* con el teclado matricial. Se implementa el código en lenguaje *C* para obtener el valor correcto de la tecla presionada. La Figura 18 muestra un diagrama de flujo de la manera como se implementa el programa para manejar el teclado matricial.

Los pasos del algoritmo usado para el manejo del teclado matricial se observan en el Algoritmo 1.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Inicializar variable de barrido ‘c’.
3.	Mandar el valor de ‘c’ por el puerto D.
4.	Leer la respuesta del teclado en el puerto D.
5.	¿Se presionó una tecla? Sí: Ir al paso 8. No:Ir al paso 6.
6.	Corrimiento y ajuste a ‘c’.
7.	¿‘c’ es válido? Sí: Ir al paso 3. No: Ir al paso 2.
8.	Identificar el valor de la tecla.
9.	Entregar el valor de la tecla.
10.	Retorno.

Algoritmo 1. Manejo del teclado matricial.

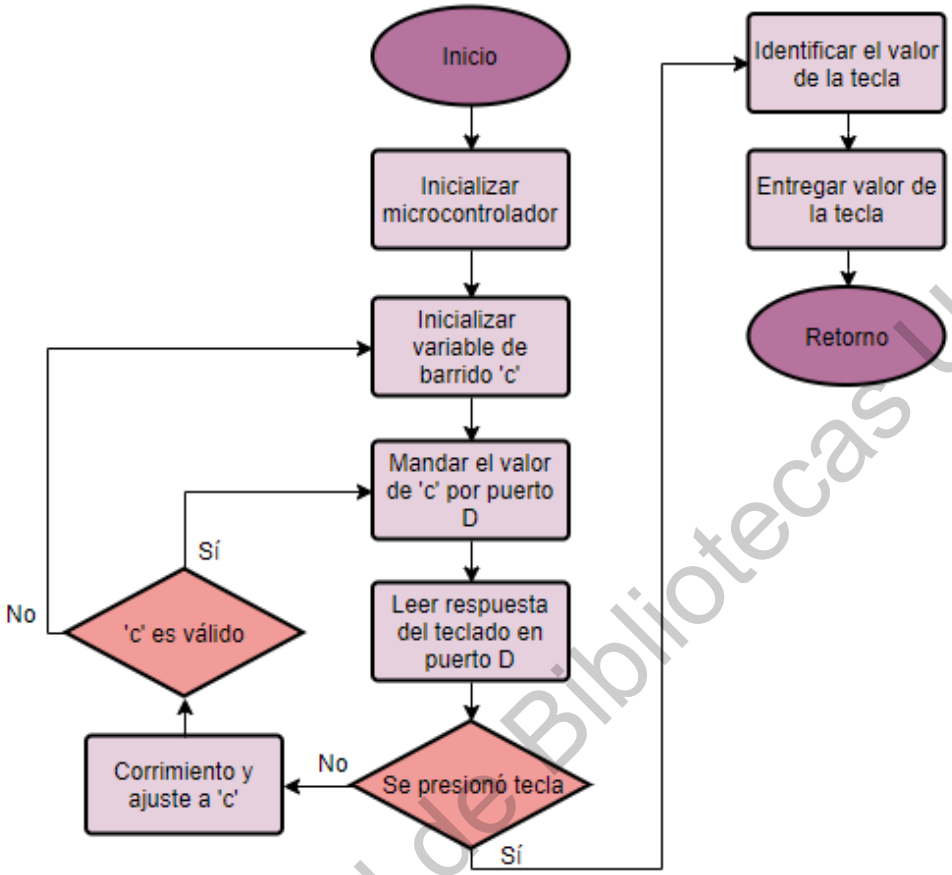


Figura 18. Diagrama de flujo del programa para el manejo del teclado matricial.

3.4. Memoria *EEPROM*

Se investiga el funcionamiento de la memoria *EEPROM* interna del microcontrolador *PIC18F46K22*, tanto para leer como para escribir en ella, se realizan las secuencias a seguir para almacenar la contraseña de un nuevo usuario, para cambiar la contraseña de administrador, así como para hacer una búsqueda de las contraseñas guardadas en la memoria *EEPROM* y evitar que un nuevo usuario use una clave ya establecida. La Figura 19 muestra un diagrama de flujo de la manera como se implementa el programa para agregar una contraseña a la memoria interna *EEPROM* del microcontrolador.

Los pasos del algoritmo usado para agregar un usuario con contraseña se muestran en el Algoritmo 2.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Imprimir mensaje “Ingresar contraseña admin”.
3.	Se ejecuta la función Ingresar Contraseña de Administrador.
4.	¿Contraseña válida? Sí: Ir al paso 5. No: Ir al paso 10.
5.	Imprimir mensaje “Ingresar nueva contraseña de usuario”.
6.	¿La contraseña es válida? Sí: Ir al paso 7. No: Ir al paso 5.
7.	Se ejecuta la función Almacenar Contraseña en Memoria *EEPROM*.
8.	Se incrementa la variable Número de contraseñas.
9.	Imprimir mensaje “Contraseña almacenada correctamente”. Ir al paso 11.
10.	Imprimir mensaje “Contraseña admin incorrecta”.
11.	Retorno.

Algoritmo 2. Agregar un usuario con contraseña.

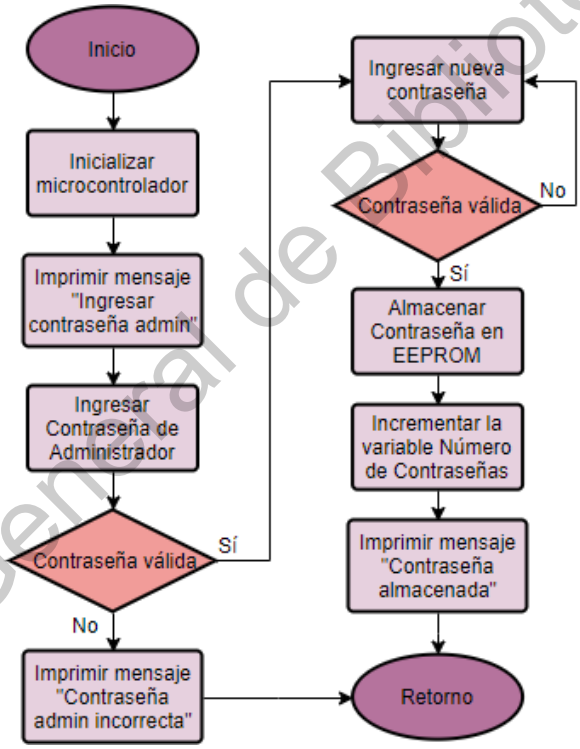


Figura 19. Diagrama de flujo del programa para configurar una contraseña.

En la Figura 20 se puede observar un diagrama de flujo que muestra la manera de como se implementa el programa para validar una contraseña ingresada mediante el teclado matricial, ya sea para permitir un acceso o para comprobar que la contraseña de un usuario nuevo no existe dentro de la memoria *EEPROM* interna del microcontrolador.

Los pasos del algoritmo usado para verificar una contraseña se muestran en el Algoritmo 3.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Inicializar variable ‘i’ para barrido.
3.	Ingresar contraseña a verificar.
4.	Se ejecuta la función Acceder a Memoria interna *EEPROM*.
5.	Se ejecuta la función Verificar Contraseña.
6.	¿Se encontró coincidencia? Sí: Ir a paso 9. No: Ir a paso 7.
7.	Corrimiento y ajuste a ‘i’.
8.	¿‘i’ es válido? Sí: Ir al paso 5. No: Ir al paso 10.
9.	Habilitar una bandera.
10.	Retorno.

Algoritmo 3. Verificar una contraseña.

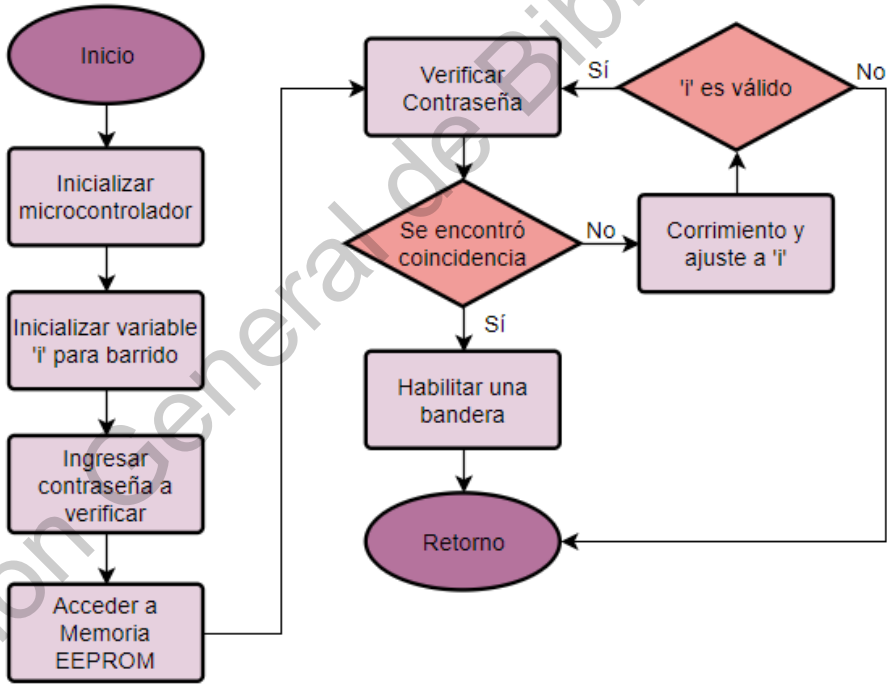


Figura 20. Diagrama de flujo del programa para verificar una contraseña.

En la Figura 21 se puede observar un diagrama de flujo que muestra cómo se implementa el programa para cambiar la contraseña de administrador, dicha contraseña permite acceder a las configuraciones de administrador.

Los pasos del algoritmo usado para cambiar la contraseña del administrador, se observan en el Algoritmo 4.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Imprimir mensaje “Ingresar contraseña admin”.
3.	Se ejecuta la función Ingresar Contraseña de Administrador.
4.	¿Contraseña válida? Sí: Ir al paso 5. No: Ir al paso 10.
5.	Se ejecuta la función Cambiar Contraseña de Administrador.
6.	Imprimir mensaje “Ingresar nueva contraseña admin”.
7.	Se guarda en memoria *EEPROM* la nueva contraseña de administrador.
8.	Imprimir mensaje “Contraseña actualizada”. Ir al paso 10.
9.	Imprimir mensaje “Contraseña admin incorrecta”.
10.	Retorno.

Algoritmo 4. Cambiar la contraseña del administrador.

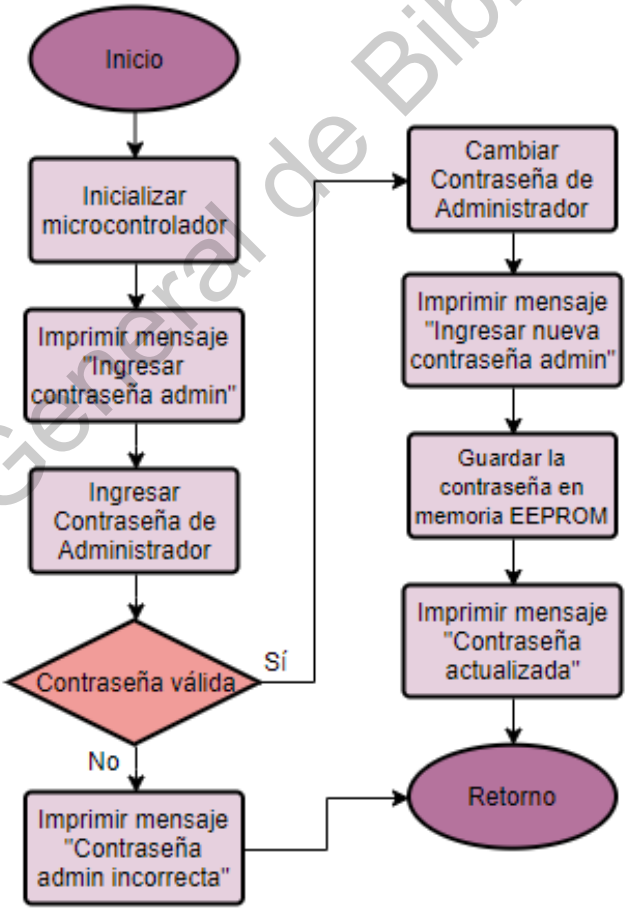


Figura 21. Diagrama de flujo del programa para cambiar contraseña de administrador.

3.5. Lector de huella digital

Primeramente, se busca un modelo de sensor de huella, por su facilidad de encontrarse en el mercado, se elige un sensor óptico. Este sensor funciona con comunicación *UART* asíncrona, lo primero es leer la hoja de especificaciones y entender la secuencia de comandos necesarios para agregar una huella. Se prueba el funcionamiento del sensor mediante una terminal y un módulo convertidor *USB* a serial *TTL*, para corroborar la velocidad de transmisión del sensor, así como los comandos básicos. Una vez comprobado el correcto desempeño del sensor, se trabaja con un *Arduino UNO*, ya que para esta tarjeta de desarrollo existe una librería predeterminada y algunos ejemplos de códigos para el uso del sensor de huella óptico.

Más adelante, se analizan estos códigos para *Arduino* y se toman como base para realizar el código en el microcontrolador a utilizar. Ya hecho lo anterior, se realiza el código en lenguaje *C*, creando las funciones necesarias para la correcta interacción del microcontrolador *PIC18F46K22* y el sensor.

Los pasos del algoritmo usado para agregar un usuario con huella digital son mostrados en el Algoritmo 5.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Imprimir mensaje “Ingresar contraseña admin”.
3.	Se ejecuta la función Ingresar Contraseña de Administrador.
4.	¿Contraseña válida? Sí: Ir al paso 5. No: Ir al paso 14.
5.	Imprimir mensaje “Colocar dedo sobre el sensor”.
6.	Se ejecuta la función Obtener la Imagen del Dedo.
7.	¿Es clara la imagen? Sí: Ir al paso 8. No: Ir al paso 5.
8.	Se ejecuta la función Obtener la imagen del dedo, por segunda vez.
9.	¿Es clara la imagen? Sí: Ir al paso 10. No: Ir al paso 8.
10.	Se ejecuta la función Generar *Template* con la imagen del dedo.
11.	Se ejecuta la función Guardar *Template* en Memoria *FLASH* del sensor.
12.	Se incrementa la variable Número de huellas.
13.	Imprimir mensaje “Usuario agregado exitosamente”. Ir al paso 15.
14.	Imprimir mensaje “Contraseña admin incorrecta”.
15.	Retorno.

Algoritmo 5. Agregar un usuario con huella digital.

La Figura 22 muestra un diagrama de flujo de la manera como se implementa el programa para agregar un usuario con huella digital.

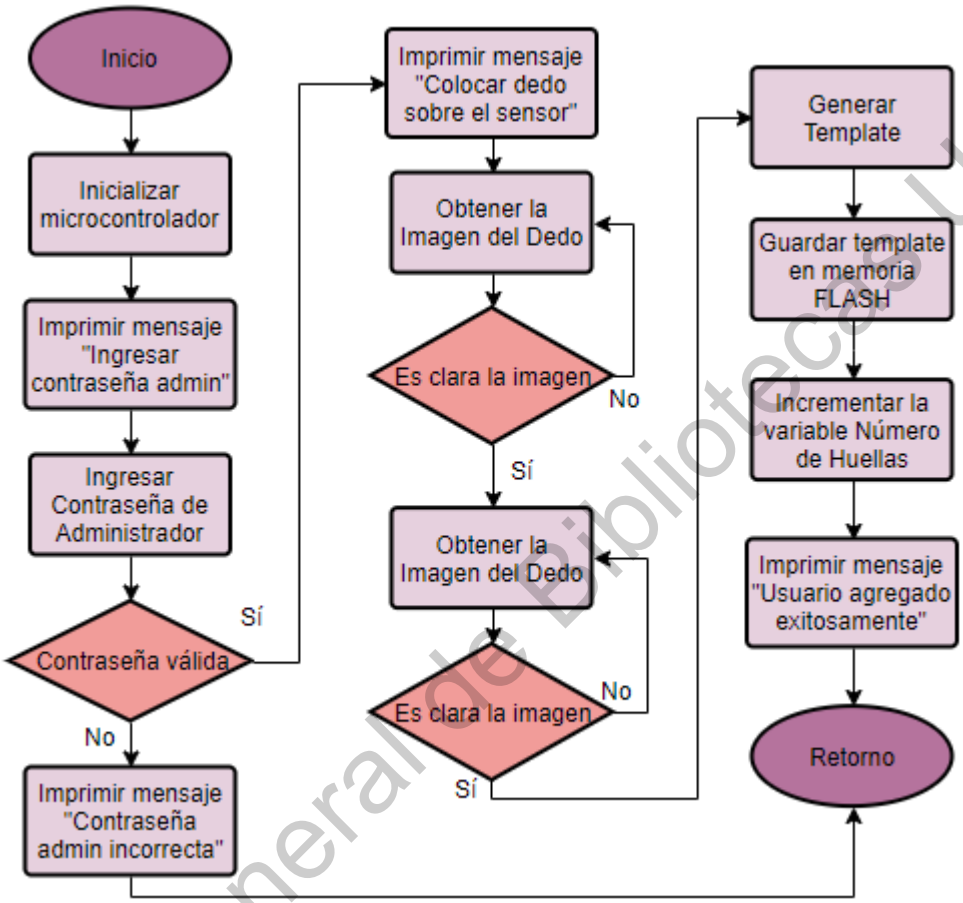


Figura 22. Diagrama de flujo del programa para agregar una huella.

Los pasos del algoritmo usado para reconocer un usuario por huella digital se observan en el Algoritmo 6.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Se ejecuta la función Obtener la Imagen del Dedo.
3.	¿Es clara la imagen? Sí: Ir al paso 4. No: Ir al paso 7.
4.	Se ejecuta la función Buscar Huella en memoria *FLASH* del sensor.
5.	¿Se encontró coincidencia? Sí: Ir al paso 6. No: Ir al paso 7.
6.	Habilitar una bandera.
7.	Retorno.

Algoritmo 6. Reconocer un usuario por huella digital.

La Figura 23 muestra un diagrama de flujo de la manera como se implementa el programa para reconocer un usuario por huella digital.

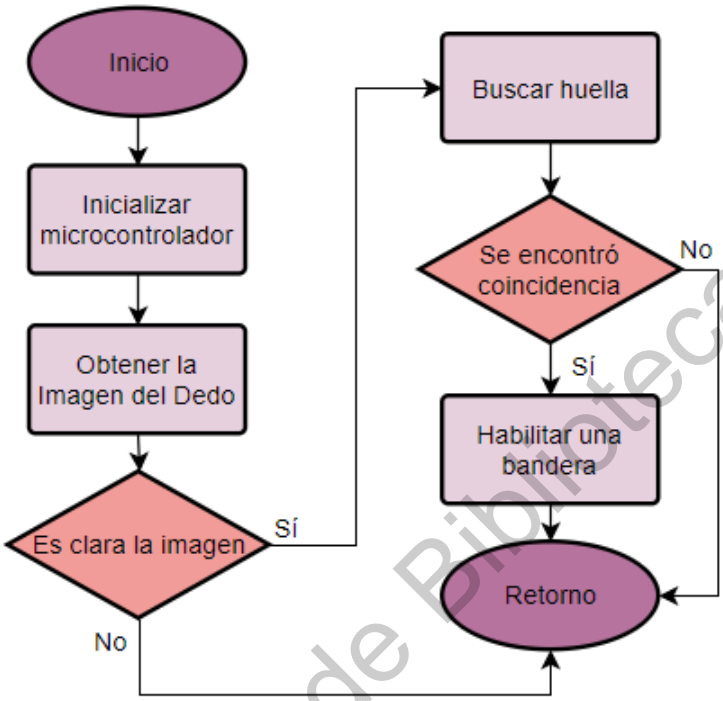


Figura 23. Diagrama de flujo del programa para verificar un usuario por huella.

El algoritmo usado para borrar una huella almacenada en el sensor de huella digital, es el Algoritmo 7.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	Imprimir mensaje “Ingresar contraseña admin”.
3.	Se ejecuta la función Digitar Contraseña de Administrador.
4.	¿Contraseña válida? Sí: Ir al paso 5. No: Ir al paso 10.
5.	Imprimir mensaje “Ingresar *ID* de huella”.
6.	Se ejecuta la función Teclado Matricial, para ingresar el número de *ID*.
7.	Se ejecuta la función Borrar *Template* del *ID* Correspondiente.
8.	Decrementar la variable que lleva la cuenta del número de huellas.
9.	Imprimir mensaje “*ID* * borrado”. Ir al paso 10.
10.	Imprimir mensaje “Contraseña admin incorrecta”.
11.	Retorno.

Algoritmo 7. Borrar una huella digital almacenada.

La Figura 24 muestra un diagrama de flujo de la manera como se implementa el programa para borrar una huella almacenada en el sensor de huella digital.

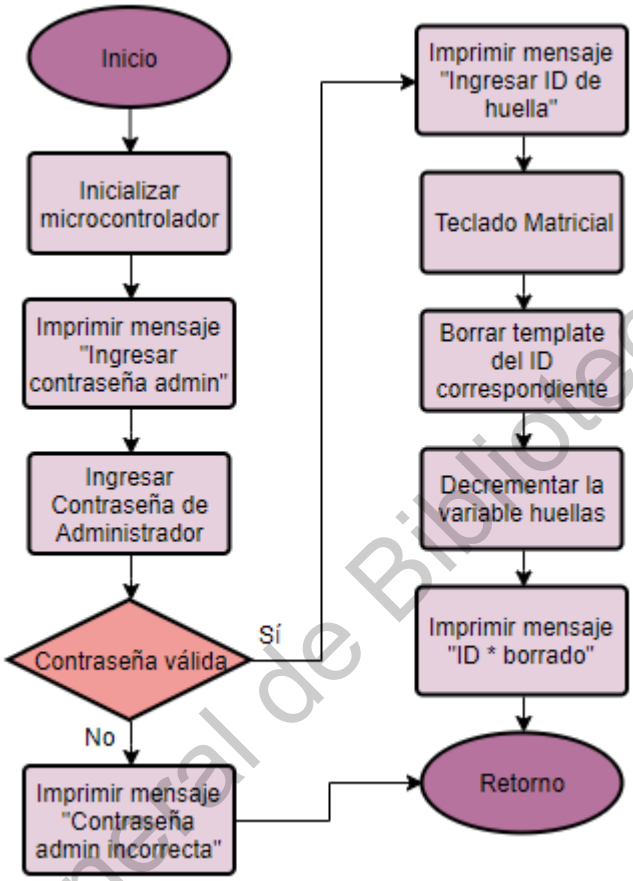


Figura 24. Diagrama de flujo del programa para borrar una huella digital.

3.6. Pantalla LCD

Para la comunicación del usuario con el sistema, se usa una pantalla *LCD*, en la cual se exhiben mensajes que permiten interactuar con la funcionalidad del prototipo. Para lo anterior, se hace uso de la librería *LCD.c* para microcontroladores *PIC*. Para mandar imprimir un texto en la *LCD*, se manda llamar primeramente la función *lcd_gotoxy(x,y),* donde '*x*' y '*y*' son las coordenadas donde se va a desplegar el texto y la función *printf(lcd_putc,"TEXTO")* para poder visualizar el texto que deseamos (ya sea un carácter o el valor de alguna variable que se quiera exhibir).

3.7. Cerradura eléctrica

Se buscan opciones en el mercado de cerraduras eléctricas, se encuentra una chapa de tipo solenoide. La implementación de la chapa con el microcontrolador se realiza de manera muy sencilla, los pasos del algoritmo usado para este fin se muestran en el Algoritmo 8.

PASO	DESCRIPCIÓN
1.	Inicializar microcontrolador.
2.	¿Hubo un acceso correcto? Sí: Ir al paso 3. No: Ir al paso 4.
3.	Poner un pin en alto del puerto E por 5 segundos.
4.	Retorno.

Algoritmo 8. Manejo de la cerradura eléctrica.

La Figura 25 muestra un diagrama de flujo de la manera como se implementa el programa para manejar la cerradura eléctrica.

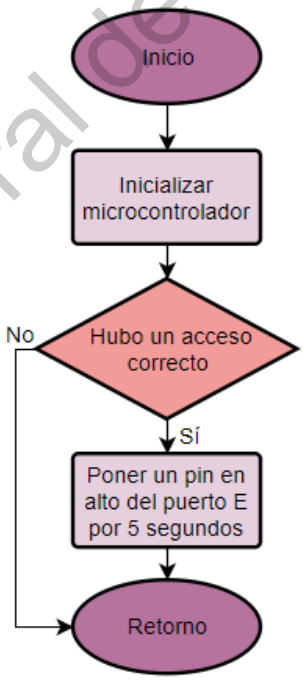


Figura 25. Diagrama del proceso para activar cerradura eléctrica.

En la Figura 26 se puede observar el esquemático de la etapa de potencia, es decir el diagrama electrónico para el manejo de la chapa tipo solenoide.

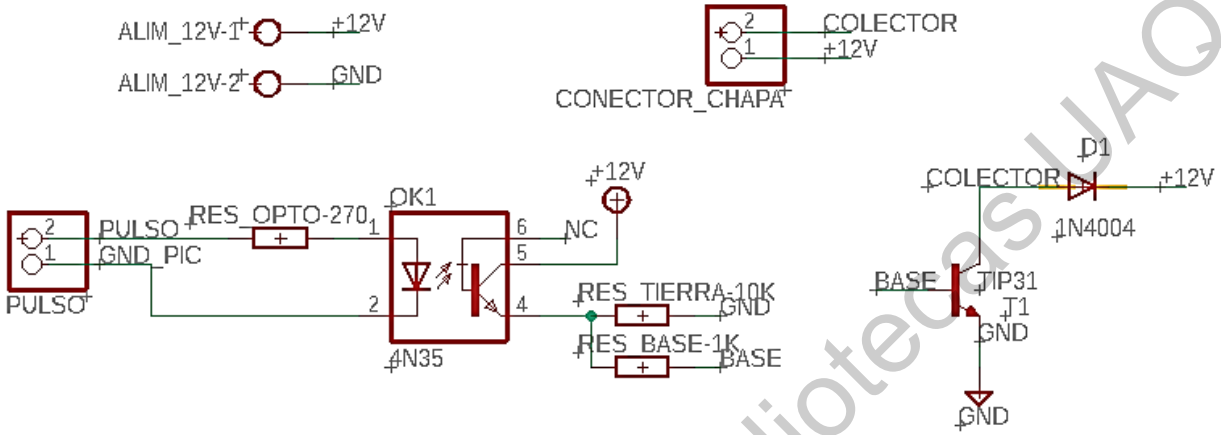


Figura 26. Diagrama esquemático de la etapa de potencia.

3.8. Integración

Todos los módulos que componen el proyecto se realizan por separado, al final se hace una integración de los códigos. Para su fácil manejo, todo se realiza con base en funciones y rutinas.

El Algoritmo 9 muestra los pasos que sigue el sistema para su funcionamiento general.

PASO	DESCRIPCIÓN
1.	¿Hay dedo en el sensor? Sí: Ir al paso 2. No: Ir al paso 4.
2.	Se ejecuta la función de Reconocer Usuario por Huella.
3.	¿Se reconoció la huella? Sí: Ir al paso 10. No: Ir al paso 1.
4.	Se ejecuta la función de Teclado Matricial.
5.	¿Se presionó tecla? Sí: Ir al paso 8. No: Ir al paso 1.
6.	¿El valor de la tecla está entre 0 y 9? Sí: Ir al paso 7. No: Ir al paso 9.
7.	Se ejecuta la función Leer el Resto de la Contraseña.
8.	¿Se reconoció la contraseña? Sí: Ir al paso 10. No: Ir al paso 1.
9.	Se ejecuta la función Funciones de Administrador. Ir al paso 1.
10.	Imprimir mensaje ”Reconocimiento correcto”.
11.	Se ejecuta la función de Acceso Correcto.

Algoritmo 9. Funcionamiento general del sistema.

En la Figura 27 se puede observar un diagrama de flujo del funcionamiento del sistema de control de acceso.

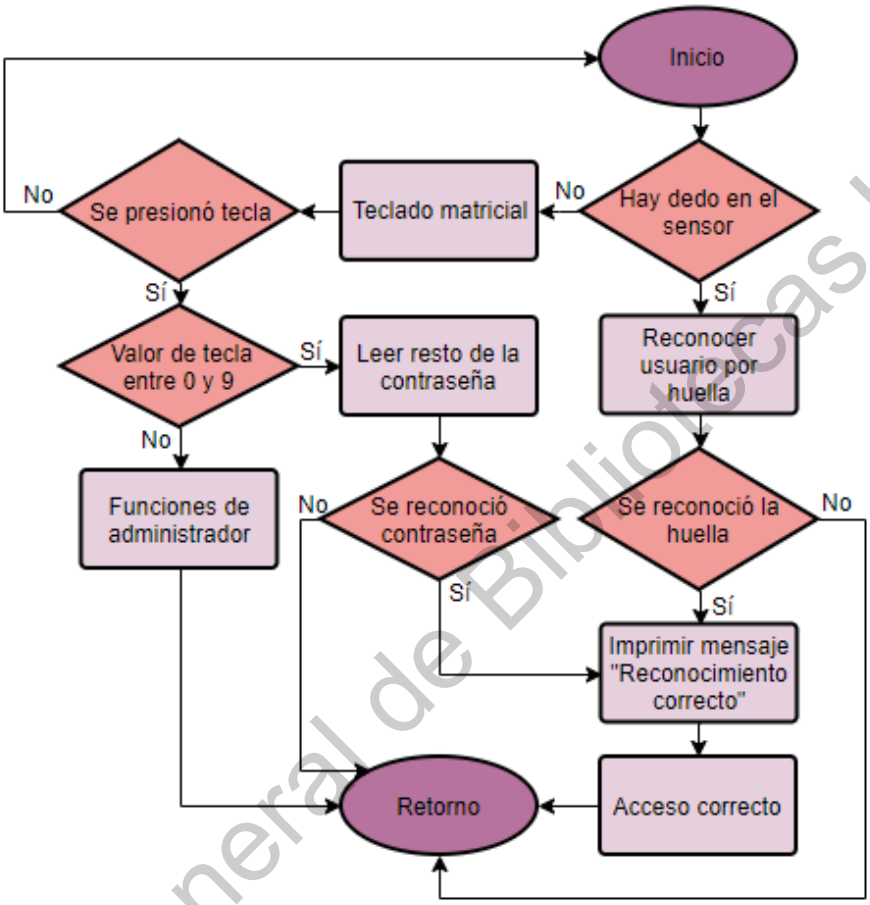


Figura 27. Diagrama de flujo del funcionamiento del sistema de control de acceso.

Se realiza el diseño del esquemático con todos los componentes necesarios para posteriormente, diseñar la tarjeta *PCB*.

En la Figura 28, se presenta el diagrama electrónico del sistema de control de acceso.

Los diagramas de flujo mostrados en esta sección, son realizados en una herramienta virtual llamada Visual Paradigm Online Diagrams.

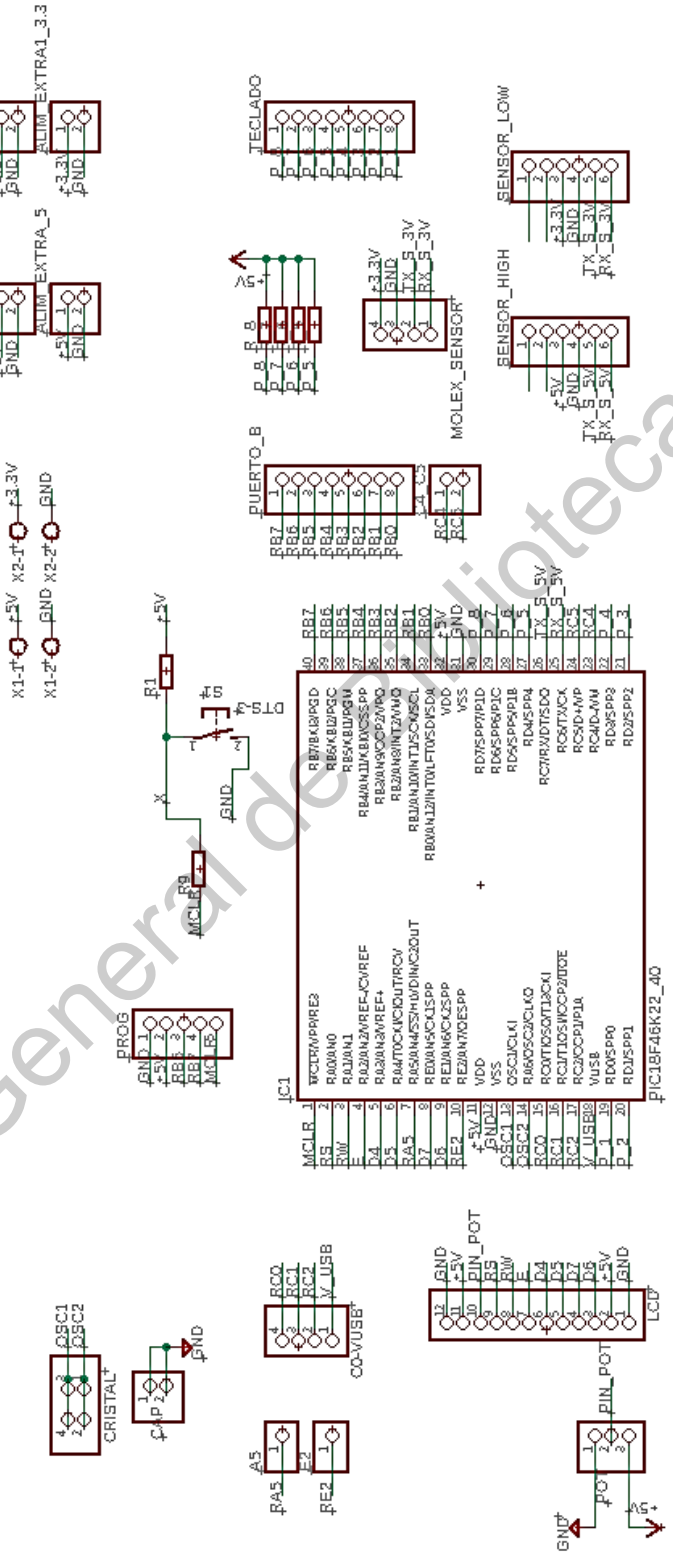


Figura 28. Diagrama esquemático del sistema de control de acceso.

3.9. Análisis de resultados

Se analizan los resultados obtenidos y se realiza una comparación entre dichos resultados y el planteamiento inicial de los requerimientos. Si estos objetivos se satisfacen, entonces el proceso de la metodología finaliza, si pasa lo contrario, es decir, aun no se cumplen los objetivos, se vuelve a iniciar el ciclo para mejorar aquellas partes que no se han cubierto totalmente o eliminar las posibles causas que eviten el correcto desempeño del prototipo.

Capítulo 4. Resultados

Una vez integrados los códigos que resuelven los problemas por separado, y que se mencionan en los puntos 3.4 a 3.7, los resultados obtenidos se muestran a continuación.

Al momento, se tiene un prototipo de un sistema de control de acceso capaz de identificar un usuario permitido, ya sea por huella digital o por contraseña numérica que se ingresa en un teclado. En la Figura 29 se muestran las partes principales del sistema.

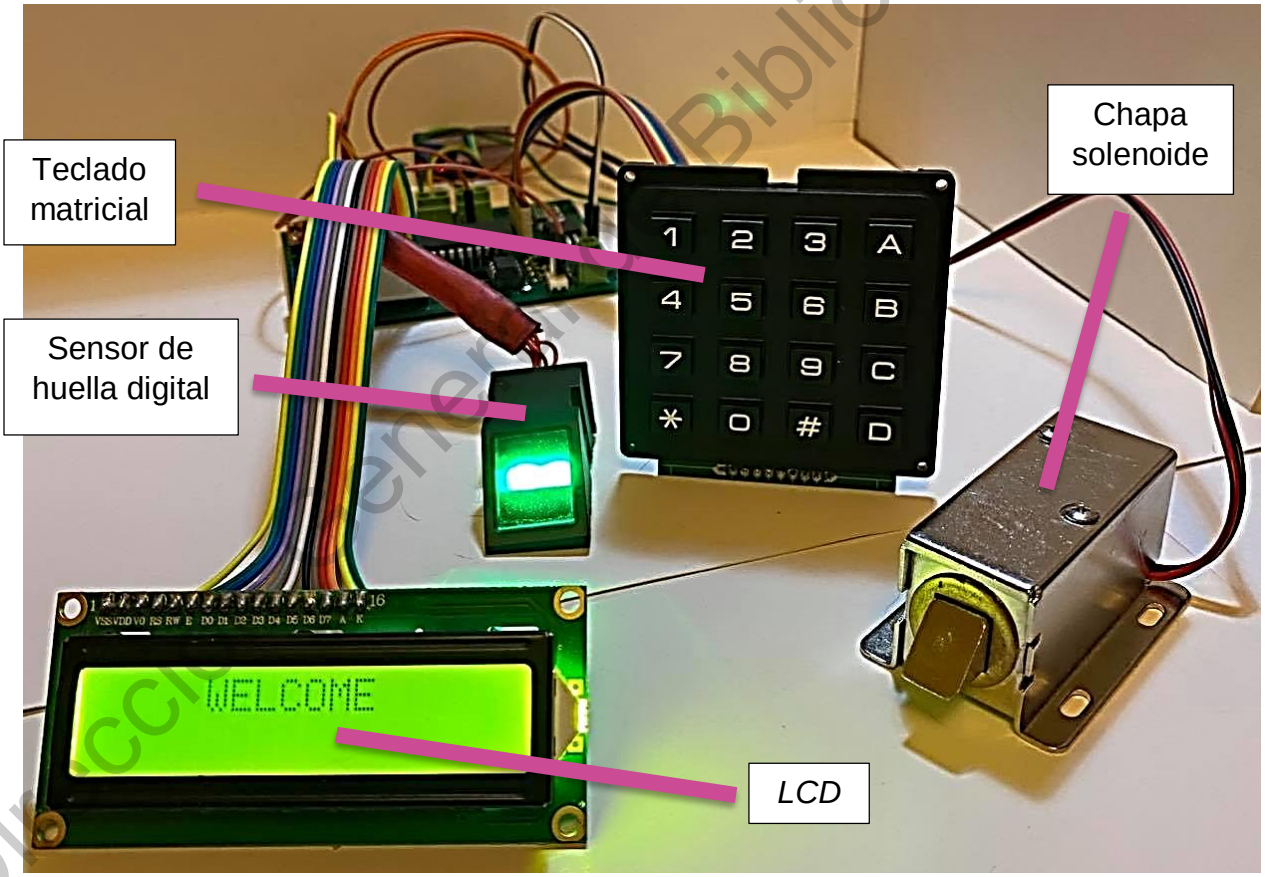


Figura 29. Componentes principales del sistema

A continuación, se enlista en la Tabla 5 las diferentes funcionalidades y las teclas que corresponden para acceder a ellas.

TECLA	FUNCIÓN
A	Añadir un usuario
B	Cambiar contraseña maestra
C	Borrar un usuario por *ID*
D	Borrar todo
#	Número de usuarios registrados
*****	Cancelar operación

Tabla 5. Funcionalidades del prototipo.

4.1. Placa *PCB*

A continuación se muestra en la Figura 30 la placa *PCB* del prototipo del sistema de control de acceso. El diseño se realiza en el software *EAGLE*. Se decide agregar los pines para el programador, para así poder realizar los últimos ajustes necesarios sobre la placa. También, se dejan algunos pines (como el puerto B), los cuales no se utilizan, pero se dejan como opción para poderlos usar en caso de ser necesario.

Se manda realizar el diseño de la placa a una empresa china, en la Figura 31 y Figura 32 se puede observar la placa antes de soldar los componentes de las capas TOP y BOTTOM, respectivamente.

En la Figura 33 se muestra la placa terminada, con todos los componentes soldados y en la Figura 34 podemos observar la placa PBC con el teclado, el sensor y la pantalla LCD conectados.

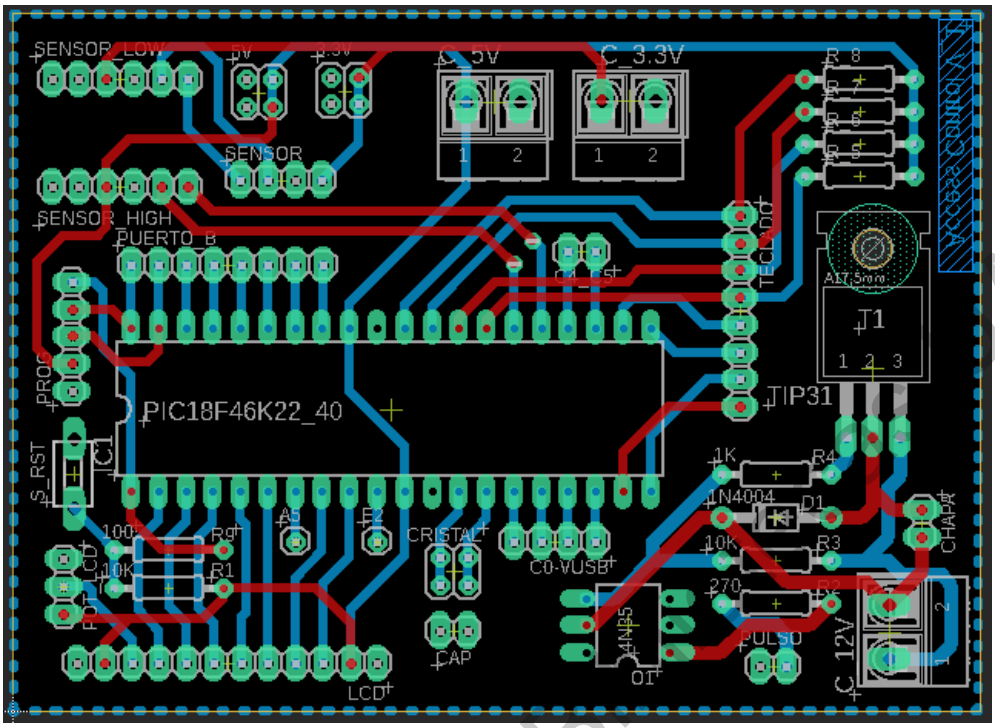


Figura 30. Diseño de placa *PCB*.

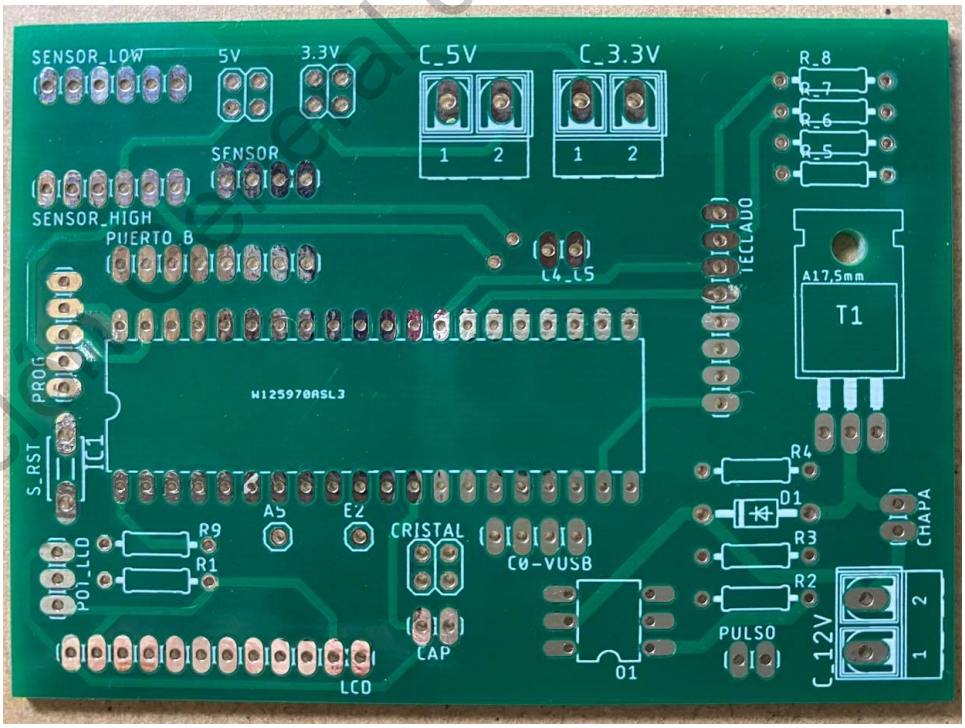


Figura 31. Placa PCB (Capa TOP).

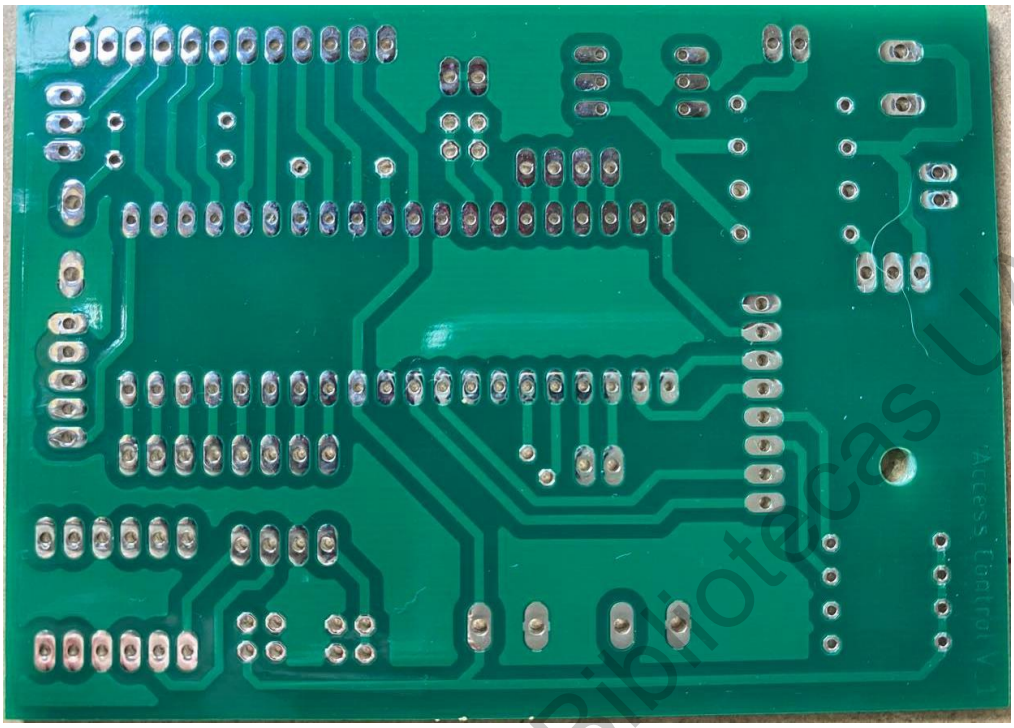


Figura 32. Placa PCB (Capa BOTTOM).

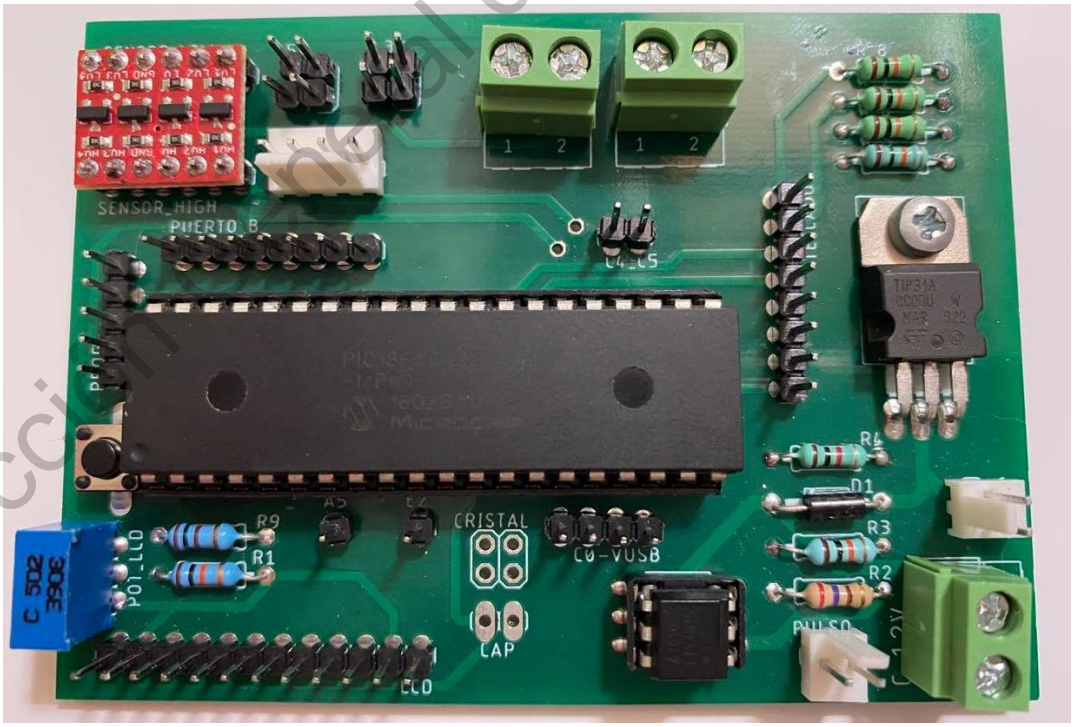


Figura 33. Placa PCB con los componentes soldados.

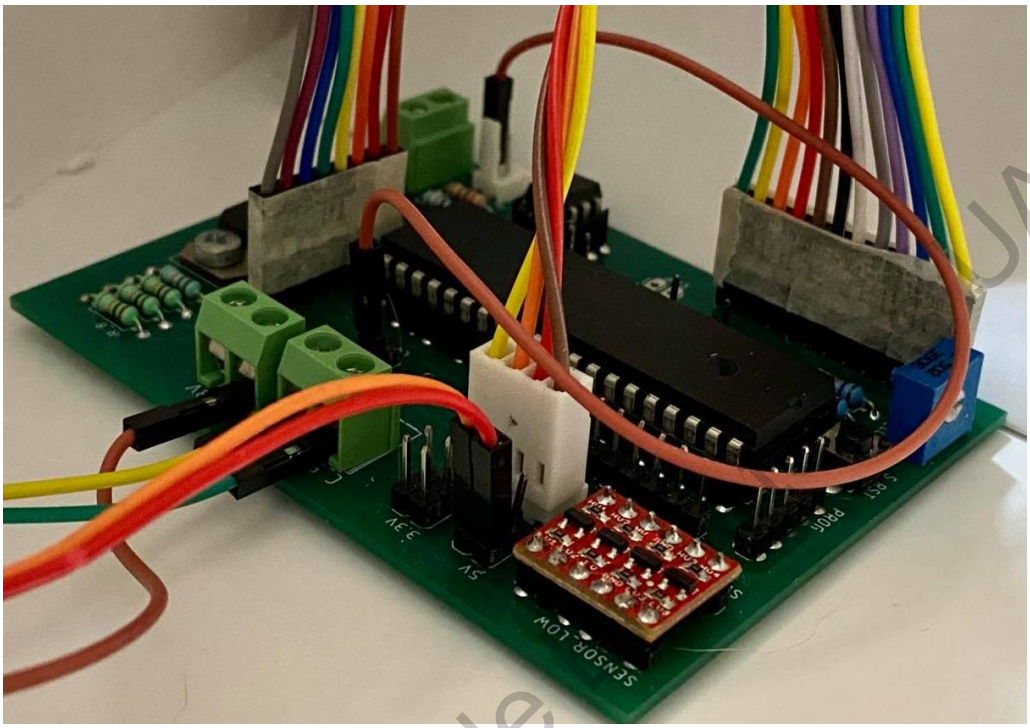


Figura 34. Placa con los dispositivos conectados.

4.2. Contraseña de administrador

El prototipo cuenta con una contraseña maestra que sirve al administrador para realizar cualquier cambio en el sistema, como registrar un usuario, eliminar un usuario, conocer el número de usuarios registrados o restaurar el sistema a su configuración de fábrica. La clave maestra por defecto es 1234, pero se puede cambiar en cualquier momento. Para cambiarla, en el menú principal se presiona la tecla “B”, el sistema pide la contraseña de administrador actual para poder realizar el cambio de contraseña. Una vez que el administrador ingresa la nueva contraseña, se imprime el mensaje de “Contraseña maestra actualizada”. En la Figura 35 podemos ver el proceso para cambiar la contraseña maestra.

Figura 35. Proceso para cambiar la contraseña maestra.

4.3. Agregar usuarios

Para agregar un usuario, ya sea por huella digital o por contraseña, el administrador debe presionar la letra “A”, posteriormente se pide la clave maestra. Una vez en el menú de Agregar Usuarios, se le pregunta al administrador el método por el cual desea agregar el usuario. En la Figura 36 se observa la vista del menú para agregar usuarios.

Figura 36. Menú para agregar usuarios.

4.3.1. Agregar usuarios por contraseña

Si en el menú Agregar Usuarios, el administrador elige “agregar usuario por contraseña”, se le pide al nuevo usuario que establezca una contraseña. El sistema busca en su base de datos las contraseñas ya almacenadas para evitar que alguna se repita, si la contraseña es correcta, se muestra el mensaje “contraseña almacenada” y también se visualiza el número total de contraseñas almacenadas. Lo anterior se puede ver en la Figura 37.

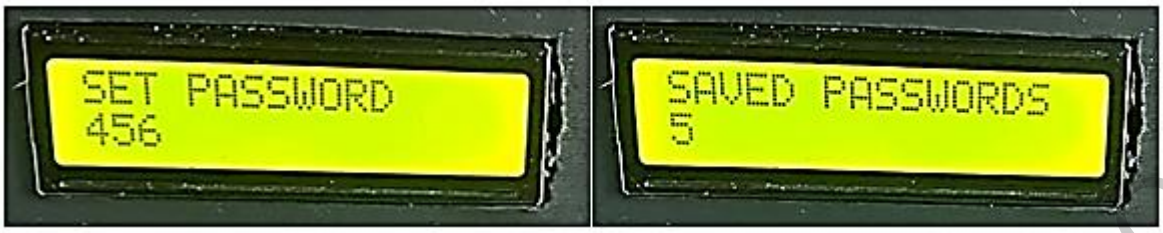


Figura 37. Proceso de agregar un usuario por contraseña.

4.3.2. Agregar usuarios por huella digital

Cuando el administrador escoge la opción de agregar un usuario por huella digital en el menú Agregar Usuarios, se comienza con un proceso, en el que es necesario colocar el dedo dos veces sobre el sensor, en la *LCD* se van mostrando los mensajes con las instrucciones. Al final se muestra el número de identificación asignado al nuevo usuario. El proceso se observa en la Figura 38.

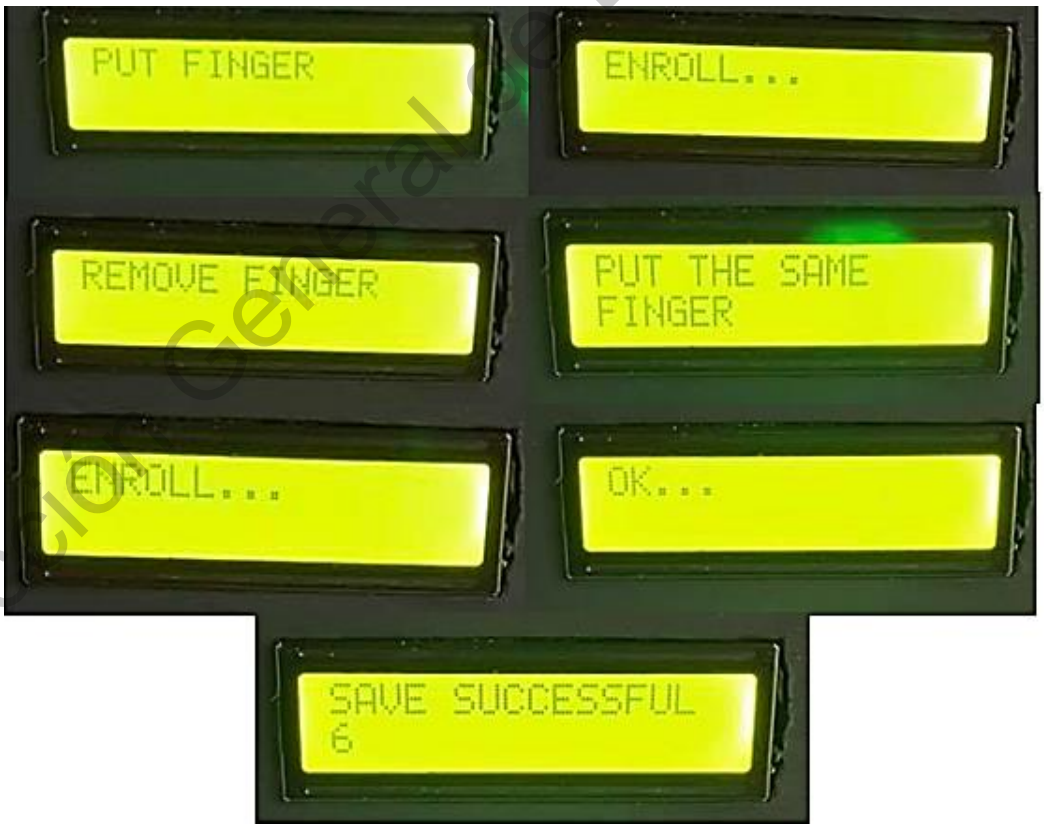


Figura 38. Proceso para agregar un usuario por huella digital.

4.4. Borrar usuario por *ID*

El sistema tiene la opción de eliminar un usuario utilizando el *ID* con el que se registró, ya sea por contraseña o por huella digital, para lo anterior, desde el menú principal se presiona la letra "*C*". Como en todas las funcionalidades, se le pide al administrador la clave maestra, luego se muestra un menú en el que se puede elegir entre eliminar un usuario por huella digital o por contraseña. Luego, se solicita el número de *ID* que se eliminará. Finalmente se muestra en la pantalla *LCD* un mensaje que indica el estatus. Podemos ver esto en la Figura 39.

Figura 39. Borrar un usuario por *ID.*

4.5. Borrar todo

El prototipo cuenta con la opción de eliminar todo, tanto los usuarios por huella digital y contraseña, así como la actualización de la contraseña maestra. Es decir, con esta opción, el sistema se restaura a la configuración de fábrica. Dentro del menú principal, se presiona la tecla "D", después, se le solicita al administrador la contraseña maestra y se le pregunta si desea eliminar todo. Al final, se imprime un mensaje en la pantalla *LCD*, indicando si la operación se realiza con éxito. El proceso se muestra en la Figura 40.

Figura 40. Proceso de Borrar todo.

4.6. Número de usuarios registrados

Este prototipo tiene la opción de que el administrador pueda ver cuántos usuarios por huella digital o contraseña están registrados. Para eso, se presiona la tecla “#”, se le pide al administrador la clave maestra, luego se muestra el número de usuarios registrados en la pantalla *LCD*. Un ejemplo de esto se observa en la Figura 41.

Figura 41. Ejemplo de número de usuarios registrados.

4.7. Identificación de usuario por contraseña

El teclado se usa para que el usuario introduzca su contraseña. La contraseña se almacena en 2 bytes. Por la cantidad de memoria que tiene el microcontrolador *PIC18F46K22*, se pueden almacenar hasta 500 contraseñas de usuario. En cambio, si se usa el *PIC18F4550*, se puede almacenar hasta 120 contraseñas.

En la Figura 42 y la Figura 43 se muestran fotos del sistema, donde se introduce la contraseña, y posteriormente se indica si se reconoció correctamente el usuario o no.

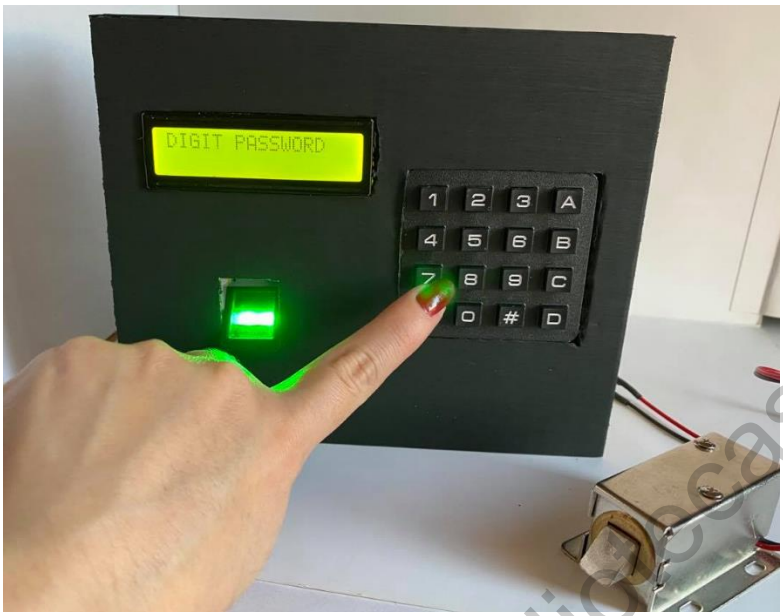


Figura 42. Ejemplo de un acceso mediante contraseña.

En la Figura 43 se puede observar que el acceso mediante contraseña fue correcto y debido a esto la chapa es accionada para permitir el desbloqueo de la puerta.

Figura 43. Ejemplo de un acceso correcto mediante contraseña.

4.8. Identificación de usuario por huella digital

El sensor de huella digital se usa para que el usuario registrado con acceso mediante reconocimiento de huella digital coloque su dedo sobre él por unos cuantos segundos. El sistema puede almacenar hasta 150 huellas digitales. En la Figura 44 se muestra el ejemplo de un acceso por huella digital.

Figura 44. Ejemplo de un acceso por huella digital.

En la Figura 45 se observa que el acceso mediante huella digital es correcto y por lo tanto la chapa es accionada para así permitir el desbloqueo de la puerta.

Figura 45. Ejemplo de un acceso correcto por huella digital.

4.9. Sistema completo

El sistema completo es presentado en Figura 46.

Figura 46. Sistema completo conectado.

En la Figura 47 se muestra una propuesta del prototipo final.

Figura 47. Prototipo del sistema.

4.10. Costos

En la Tabla 6 se muestra un desglose de los materiales usados para el desarrollo del prototipo aquí presentado.

CANTIDAD	DESCRIPCIÓN	TOTAL (MXN)
1	Microcontrolador PIC18F4550	$200.00
1	Microcontrolador PIC18F46K22	$220.00
1	Programador Pickit 4	$1,867.00
2	Protoboard	$145.00
1	Teclado matricial 4x4	$100.00
1	Sensor de huella digital	$490.00
1	Cerradura eléctrica	$346.00
1	Pantalla LCD 16x2	$70.00
1	Convertidor de nivel lógico	$65.00
-	Componentes electrónicos (varios)	$200.00
5	Placa PCB	$1,000.00
	SUBTOTAL	**$4,703.00**
-	Mano de obra (Diseño)	$42,000.00
	TOTAL	**$46,703.00**

Tabla 6. Costos aproximados del prototipo.

Capítulo 5. Conclusiones

El proyecto consiste en un sistema de seguridad para el control de acceso, diseñado para controlar el acceso de los usuarios a cualquier área. Este sistema puede reconocer a los usuarios mediante una contraseña numérica que consta de 4 dígitos, o mediante el reconocimiento de la huella digital.

Los objetivos establecidos al principio, están cubiertos en un 90%, ya que existe un prototipo de sistema de control de acceso funcional al 100%. Las mejoras que se pueden lograr en el prototipo tienen que ver con la interfaz de comunicación. Otro punto que debe cubrirse es diseñar una caja para que el prototipo se instale formalmente en una puerta.

Por otro lado, una característica muy particular del sistema es que no pierde información debido a interrupciones en la electricidad. Es un proyecto de alto impacto porque con su uso, los robos pueden reducirse en el lugar donde sea instalado.

El sistema ha sido probado y se encuentra que puede almacenar un total de 150 usuarios con una huella digital y hasta 500 usuarios con una contraseña numérica. Se prueba que el sistema no pierde información de huellas digitales o contraseñas cuando se desconecta de la alimentación eléctrica y que la etapa de alimentación funciona perfectamente con la chapa solenoide.

Este sistema de control de acceso se diseña con la idea de que es posible agregar otra tecnología de control de acceso, como lo podría ser la tecnología *RFID*. También es posible adaptarlo a las necesidades de futuros clientes y mejorar la interfaz de comunicación con el usuario.

En cuanto al costo, se encuentra que su desarrollo es bastante elevado. Lo anterior sucede debido a que se está considerando el costo de diseño. En el desglose de los costos mostrado en la sección de resultados, podemos ver que se está considerando el material

que no es consumible. Es decir, que ciertos materiales que se necesitan para el desarrollo del proyecto se pueden utilizar más adelante para la realización de nuevos equipos, por lo que se reduciría el costo en cada uno de los prototipos.

Referencias

Adafruit (s.f.). Fingerprint sensor. Recuperado de https://www.adafruit.com/product/751.

Arduino para todos (2017). Teclado matricial con Arduino. Varios ejemplos. Recuperado de http://arduparatodos.blogspot.com/2017/12/teclado-matricial-con-arduino-varios.html.

Bateman, J., Cortés, C., Cruz, P., & Penagos, H. P. (2009). Diseño de un protocolo RFID propietario para una aplicación específica. Ingeniería y universidad, 13(2), 6.

Buendía, J. F. R. (2013). Seguridad informática. McGraw-Hill España.

Chulde, c. y javier, k. (2017). Diseño e implementación de un sistema de comunicaciones unificadas basado en software libre que integra capacidades de voz sobre ip, mensajería instantánea, fax, mail, pbx y un subsistema de registro de asistencia y desbloqueo de cerradura por huella dactilar para la empresa vuelofertas cia. Ltda (bachelor's thesis, quito: universidad israel, 2017).

Chuqui Chicaiza, L. M. (2014). Diseño e implementación de un sistema de control de asistencia de personal, mediante el uso de tecnología biométrica de huella dactilar (Bachelor's thesis, Quito: EPN, 2014.).

Cigso (s.f.). Control de accesos. Recuperado de http://cigso.com/control-de-accesos/.

Cucorent (s.f.). Sistema de control de acceso para empresas. Recuperado de https://www.cucorent.com.mx/control-de-accesos-y-asistencia/.

D.R. Security (s.f.). Lectores biométricos. Recuperado de http://www.drsecurity.net/lectores_biometricos.html.

Díaz Mulas, B. (2015). UART: Universal Asynchronous Receiver-Transmitter (Bachelor's thesis).

Didácticas electrónicas (s.f.). Solenoide para cerradura eléctrica. Recuperado de https://www.didacticaselectronicas.com/index.php/domotica/chapa-solenoide-cerradura.

Electgpl (s.f.). Control de teclado matricial. Recuperado de http://electgpl.blogspot.com/2013/08/control-de-teclado-de-4x4.html.

Electrónica Ecuador (2015). Manejo de teclados matriciales (barrido clásico). Recuperado de http://electronicaecuador.blogspot.com/2015/08/manejo-de-teclados-matricialesbarrido.html.

Electrónica Ingeniería (s.f.). Electrónica digital aplicada. Recuperado de https://tecnologiaelectronica-gustav.blogspot.com/p/electronica-digital-la-electronica.html.

Estrada, M. A. (2016). UAQ: en menos de 3 meses, 5 robos. El Universal. Recuperado de http://www.eluniversalqueretaro.mx/portada/02-09-2016/uaq-en-menos-de-3-meses-5-robos.

Euroeléctrica (s.f.). Kit de control de acceso INTEC. Recuperado de https://euroelectrica.com.mx/producto/kit-de-control-de-acceso-intec/.

Giraldo Giraldo, A., y Gómez Ramírez, D. P. (2017). Estado del arte de la seguridad en sistemas biométricos.

Gordón Díaz, N. Y. (2009). Control de acceso en la entrada del Instituto Geofísico utilizando tecnología RFID (Bachelor's thesis, QUITO/EPN/2009).

Informática Moderna (s.f.). Pantalla LCD. Recuperado de http://www.informaticamoderna.com/Pantalla_LCD.htm.

Instituto Nacional del cáncer (NIH) (s.f.). Definición de iris. Recuperado de https://www.cancer.gov/espanol/publicaciones/diccionario/def/iris.

Loaiza Jiménez, K. E. (2016). Desarrollo de un prototipo controlador para un sistema domótico por medio de una pantalla tft touch shield v2. 0 y arduino (Bachelor's thesis).

López García, J. (2009). Algoritmo para la identificación de personas basado en huellas dactilares.

Microchip Technology Inc. (s.f.). Data sheet PIC18F4550. Recuperado de http://ww1.microchip.com/downloads/en/DeviceDoc/40001412G.pdf.

Microchip Technology Inc. (s.f.). Data sheet PIC18F46K22. Recuperado de http://ww1.microchip.com/downloads/en/DeviceDoc/40001412G.pdf.

Microchip Technology Inc. (s.f.). PIC18F4550. Recuperado de https://www.microchip.com/wwwproducts/en/PIC18F4550.

Mindiamart (s.f.). RFID Card. Recuperado de https://www.indiamart.com/proddetail/rfid-card-16544615897.html.

Montenegro, G. A. y Marchesin, A. E. (2007). Sistema de identificación por radiofrecuencia (RFID). Comisión Nacional de Comunicaciones.

Montenegro, L. y Jonnathan, G. (2013). Diseño, construcción e implementación de un sistema de control automático basado en microcontroladores para el proceso de pasteurización de leche en la empresa Gustalac SA (Bachelor's thesis, CIENCIAS DE LA INGENIERÍA E INDUSTRIAS FACULTAD: INGENIERÍA EN ELECTROMECANICA Y AUTOMATIZACION).

Nomada Store (s.f.). Pantalla LCD. Recuperado de https://nomada-e.com/store/interfaces/128-lcd-alfanumerica-16x2.html.

Nomada Store (s.f.). Pantalla TFT 3.2". Recuperado de https://nomada-e.com/store/interfaces/148-pantalla-tft-32-tactil-con-stylus.html.

Norma Internacional ISO/IEC (s.f.). Técnicas de seguridad – Protección de la información biométrica.

Ocas Quiroz, C. E., Pedro, S. y Jonatan, E. (2019). Sistema de seguridad para el control de acceso a una vivienda mediante el reconocimiento de voz utilizando coeficientes cepstrum MFCC Y DTW.

Oke, A. O., Olaniyi, O. M., Arulogun, O. T. y Olaniyan, O. M. (2009). Development of a microcontroller-controlled security door system. The Pacific Journal of Science and Technology, 10(2), 398-403.

Osorio, J. A. C., Aguirre, F. A. M. y Escobar, J. A. M. (2010). Sistemas de seguridad basados en Biometría. Scientia et technica, 17(46), 98-102.

Polenciano, V. (2018). UAQ anuncia acciones para mayor seguridad. El universal. Recuperado de http://www.eluniversalqueretaro.mx/sociedad/27-04-2018/uaq-anuncia-acciones-para-mayor-seguridad.

Ratio Technologies (s.f.) Lector de huellas dactilares capacitivos USB 2.0. Recuperado de http://www.ratiotechnologies.com/pages/DP_Eikon710.aspx.

Rivero Arbelo, E. (2018). Comunicaciones de sistemas empotrados utilizando el estándar IEEE 802.15. 4.

Serban (s.f.). Biometría facial: El sistema de reconocimiento mediante el rostro. Recuperado de https://www.serban.es/biometria-facial-el-sistema-de-reconocimiento-mediante-el-rostro/.

Serna, A., Ros, F. y Rico, J. C. (2010). Guía práctica de sensores. Creaciones Copyright SL.

Serratosa, F. (2012). La biometría para la identificación de las personas. Editorial UOC. España.

Sistemas en Electrónica (s.f.). Tienda catálogo de venta online. Recuperado de https://www.sistemasenelectronica.com.mx/.

Topón Guallichico, J. M. (2017). Diseño e implementación de un prototipo para un sistema electrónico temporizado en puertas y ventanas, empleando módulos Arduino, para el restaurante “El Pailón de Mushuñan” (Bachelor's thesis, Quito, 2017.).

Torriti, M. T. (2007). Tutorial Microcontroladores PIC. Pontificia Universidad Católica de Chile, (1.0), 3.

Valdés, F. y Areny, R. P. (2007). Microcontroladores fundamentos y aplicaciones con PIC (Vol. 1149). Marcombo.

Vega-Luna, J. I., Cosme-Aceves, J. F., Sánchez-Rangel, F. J. y Salgado-Guzmán, G. (2018). Control de Acceso Usando RFiD y una Tarjeta Raspberry Pi Zero W.

Vergara, V., y Verónica, Z. (2013). Sistema de Control de acceso y monitoreo con la tecnología RFID para el departamento de Sistemas de la universidad Politécnica Salesiana Sede Guayaquil (Bachelor's thesis).

Zambrano, A. A., Ulloa, H. C. y Valdiviezo, C. (s.f.). Medidor LC Utilizando Pantalla LCD 2x16 para Visualización con Programa Embebido en un Microcontrolador.