

**FACULTAD DE INGENIERÍA**

**DEPARTAMENTO DE INGENIERÍA ELÉCTRICA**

**Avance 1**

**Diseño y construcción de un sistema electrónico para el control de acceso biométrico de huella dactilar gestionado por plataforma WEB.**

**Alumno : Juan Sotomayor Chacón**

**Carrera : Ingeniería civil industrial en electrónica**

**Profesor Guía : Jorge Gianotti Hidalgo**

**Antofagasta, Diciembre de 2016**

# ÍNDICE

[ÍNDICE ii](#_Toc469341403)

[LISTA DE FIGURAS v](#_Toc469341404)

[LISTA DE TABLAS vi](#_Toc469341405)

[LISTA DE ACRÓNIMOS vii](#_Toc469341406)

[1 INTRODUCCIÓN 1](#_Toc469341407)

[1.1 Objetivos 3](#_Toc469341408)

[1.1.1 Objetivo general 3](#_Toc469341409)

[1.1.2 Objetivos específicos 3](#_Toc469341410)

[1.2 Planteamiento de la investigación 4](#_Toc469341411)

[1.1.3 Modelos planteados para el hardware 7](#_Toc469341412)

[1.1.4 Justificación del modelo seleccionado 11](#_Toc469341413)

[1.3 METODOLOGÍA 13](#_Toc469341414)

[2 TÉCNICAS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS 15](#_Toc469341415)

[2.1 Contraseñas 17](#_Toc469341416)

[2.2 Identificación por Radio Frecuencia (RFID) 18](#_Toc469341417)

[2.2.1 Funcionamiento de la Identificación por Radio Frecuencia (RFID) 18](#_Toc469341418)

[2.2.3 Clasificación 21](#_Toc469341419)

[2.2.4 Regulación y estandarización 23](#_Toc469341420)

[2.3 Biometría 24](#_Toc469341421)

[2.3.1 Sistemas biométricos 26](#_Toc469341422)

[2.3.2 Lector huella digital 32](#_Toc469341423)

[3 DISEÑO SISTEMA DE CONTROL DE ACCESO 35](#_Toc469341424)

[3.1 Infraestructura del sistema de control de acceso 35](#_Toc469341425)

[3.2 Módulo control de acceso 37](#_Toc469341426)

[3.2.1 Display LCD 38](#_Toc469341427)

[3.2.2 Teclado matricial 42](#_Toc469341428)

[3.2.3 Módulo RFID MFRC522 45](#_Toc469341429)

[3.2.4 Sensor biométrico 47](#_Toc469341430)

[3.2.5 Microcontrolador 50](#_Toc469341431)

[3.2.6 Led RGB 52](#_Toc469341432)

[3.2.6 Circuito módulo control de acceso 54](#_Toc469341433)

[3.3 Raspberry Pi 3 56](#_Toc469341434)

[3.4 Circuito de control 58](#_Toc469341435)

[BIBLIOGRAFÍA 63](#_Toc469341436)

[ANEXO A 64](#_Toc469341437)

[DATOS TÉCNICOS DE DISPOSITIVOS Y COMPONENTES 64](#_Toc469341438)

[A.1 Display LCD 64](#_Toc469341439)

[A.1.1 Consideraciones sobre las operaciones de lectura y escritura 65](#_Toc469341440)

[A.2 MFRC522 68](#_Toc469341441)

[A.2.1 Características de sincronización 68](#_Toc469341442)

[A.2.2 Configuración de bytes para lectura y escritura SPI 69](#_Toc469341443)

[A.3 ZFM-20 70](#_Toc469341444)

[A.3.1 Protocolo de comunicación 70](#_Toc469341445)

[A.4 Arduino Mega 2560 71](#_Toc469341446)

[A.5 Módulo LM2596 72](#_Toc469341447)

[A.6 Transistor BC548 73](#_Toc469341448)

[A.7 Relé 74](#_Toc469341449)

# LISTA DE FIGURAS

Figura 1.1 Ejemplo de un sistema de control de acceso en red. 5

Figura 1.2 Arquitectura módulo control de acceso, modelo 1. 8

Figura 1.3 Arquitectura módulo control de acceso, modelo 2. 9

Figura 1.4 Arquitectura módulo control de acceso, modelo 3. 10

Figura 1.5 Referencia ubicación control de acceso, modelo 3. 13

Figura 2.1 Esquema de funcionamiento de autentificación mediante contraseña. 17

Figura 2.2 Campos magnético generado por un sistema RFID. 19

Figura 2.3 Esquema y componentes de un sistema RFID. 20

Figura 2.4 Estructura etiqueta RFID. 20

Figura 2.5. Etapas o procesos que componen los sistemas: a. matriculación; b. verificación; c. identificación. 28

Figura 2.6 Imagen capturada por un sensor biométrico. 32

Figura 2.7. Método de lectura de huella digital óptico. 33

Figura 2.8. Método de lectura de huella digital capacitivo. 34

Figura 3.1 Infra estructura del sistema de control de acceso. 37

Figura 3.2 Diagrama módulo control de acceso 38

Figura 3.3 Vista frontal del LCD alfanumérico 4x20 39

Figura 3.4 Teclado de membrana 4x4 42

Figura 3.5 Diagrama del teclado matricial en reposo 43

Figura 3.6 Diagrama del teclado matricial cuando la tecla 6 es presionada 44

Figura 3.7 Módulo MFRC522 45

Figura 3.8 Pines de control y alimentación del MFRC522 46

Figura 3.9 Módulo ZFM-20 series. 47

Figura 3.10 Vista trasera del módulo de huella dactilar. 48

Figura 3.11 Led RGB 52

Figura 3.12 Circuito esquemático resistencia en serie con diodo led 52

Figura 3.13 Especificaciones técnicas led RGB 53

Figura 3.14 Circuito esquemático del módulo control de acceso. 54

Figura 3.15 Vista frontal de la placa de circuito impreso del módulo de control de acceso 55

Figura 3.16 Vista frontal de la placa de circuito impreso con las líneas de conexión. 55

Figura 3.17 Raspberry Pi 3 56

Figura 3.18 Esquema pines GPIO Raspberry Pi 3 57

Figura 3.19 Módulo LM2596 58

Figura 3.20 Reloj de tiempo real DS1307 59

Figura 3.21 Circuito para activar un relé desde la salida de un controlador 59

Figura 3.22 Esquemático circuito de control 61

Figura 3.23 Vista frontal circuito de control 62

Figura 3.24 Circuito impreso 62

# LISTA DE TABLAS

[Tabla 1.1.1 Características microcontrolador v/s Raspberry Pi. 11](#_Toc469341487)

[Tabla 3.1 Descripción de pines del display LCD 40](#_Toc469341488)

[Tabla 3.2 Característica módulo ZFM-20. 49](#_Toc469341489)

[Tabla 3.3 Especificaciones técnicas Arduino Mega2560 50](#_Toc469341490)

[Tabla 3.4 Pines del display LCD 51](#_Toc469341491)

# LISTA DE ACRÓNIMOS

PC: Personal Computer.

LAN: Local Area Network.

WAN: Wide Area Network.

RTC: Real Time Clock

RFID: Radio Frequency Identification

RF: Radio frecuencia

MSB: Most Significant Bit

GPIO: General Purpose Input/Output

LCD: Liquid Crystal Dysplay

IP: Internet Protocol.

TCP: Transmission Control Protocol.

UART: Universal Asynchronous Receiver Transmitter.

RAM: Random Acces Memory.

ROM: Read Only Memory.

SPI: Serial Peripheral Interface.

USB: Universal Serial Bus.

DSP: Digital Signal Processor

TTL: Transistor-Transistor Logic.

CAPÍTULO

# INTRODUCCIÓN

La evolución de la ciencia y de la tecnología ha permitido evolucionar también a los sistemas de seguridad y de control de acceso de los que la sociedad puede disponer. En un principio consistían en medios físicos, tales como cerraduras, rejas, trabadores, etc., fácilmente vulnerables con tiempo y herramientas; animales tales como perros guardianes; vigilantes tales como policías, serenos, veladores. Todos estos sistemas fueron evolucionando hasta crear sistemas más complejos como cerraduras electrónicas, alarmas o sistema de observación por video.

El control de acceso se viene realizando tradicionalmente en grandes edificios y recintos de gran ocupación. Hoy en día estos sistemas representan un plus importante de seguridad para cualquier tipo de empresa o actividad. El control de acceso básicamente permitirá diferenciar:

* Qué personas tienen acceso a las dependencias de trabajo.
* A qué dependencias concretas tienen acceso.
* En que horario tienen acceso.

Una gran ventaja que aportan estos sistemas es tener un registro con todos los accesos que se producen en las instalaciones. De esta manera se puede controlar y prevenir cualquier evento interno (robo, sabotaje, etc.), ya que se pueden recuperar el registro de fichajes de un día determinado a una hora en cualquier punto de la instalación donde exista dicho control.

En la actualidad son muchos los sistemas de control de acceso electrónicos que aparecen en el mercado para solventar la demanda existente. Se pueden encontrar una multitud de lectores, tarjetas, y programas informáticos que lo realizan, pero realmente la diferencia está en el cumplimiento de las expectativas de los clientes.

Una de las soluciones en la actualidad es la identificación de las personas mediante su huella digital. Gracias a su unicidad y constancia a través del tiempo, las huellas digitales han sido utilizadas para la identificación de las personas por más de un siglo, más recientemente volviéndose automatizada debido a los avances en las capacidades de la computación.

El presente proyecto tiene como finalidad diseñar y construir un sistema de control de acceso gestionado por una plataforma web. La forma de identificación de usuarios, es mediante el sistema biométrico de huella digital y a través de identificación por radiofrecuencia (RFID), se estudiará estas tecnologías en detalles para integrarlas a un módulo electrónico para el control de acceso, este debe ser capaz de registrar, identificar y autentificar a los usuarios del sistema, gestionar la información del sistema y manejar base de datos, controlar el actuador del punto de acceso (puerta de seguridad) y cumplir con los parámetros de seguridad, para dificultar la intervención física de terceros.

La plataforma web es la interfaz gráfica con la cual el administrador del sistema gestiona los recursos de los usuarios de forma remota como; ingresar, validar, editar y eliminar usuarios, configurar horarios de ingresos, estadísticas e historial de ingreso, exportar relatorios, etc. Esta herramienta brinda una mayor eficiencia y movilidad al administrador al permitir que desde cualquier lugar con conexión a internet tenga acceso a la plataforma.

## Objetivos

### Objetivo general

Diseñar y construir un sistema electrónico para el control de acceso biométrico de huella dactilar gestionado por una plataforma WEB.

### Objetivos específicos

* Investigación detallada del funcionamiento del sensor biométrico de huella dactilar y sistemas RFID (identificación por radiofrecuencia).
* Diseñar un módulo de control de acceso que sea capaz de identificar huellas dactilares y tarjetas RFID, lograr diferenciarlas entre sí, almacenarlas y modificarlas en la memoria de un microcontrolador, debe contar con un lector de memoria SD para almacenar el registro de los usuarios y el historial de ingreso de estos, de modo de respaldo.

El módulo debe tener conexión estable a una Red de Área Local (LAN), enviar y recibir información a un servidor de base de datos Mysql.

* Desarrollar una plataforma web en donde el administrador del módulo, tenga acceso a los usuarios registrados, con la opción de ingresar e editar datos personales, permitir y denegar acceso, ver historial y estadísticas de ingreso durante un periodo determinado.
* Realizar un estudio económico del sistema de control de acceso.
* Implementar el módulo control de acceso en un lugar determinado y verificar su correcto funcionamiento.

## Planteamiento de la investigación

Un sistema de control de acceso hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones. Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestra huella en un lector para desbloquear un teléfono inteligente. Estos casos, son ejemplos que permiten el acceso a datos. Sin embargo, este trabajo está enfocado en la seguridad electrónica, relacionada al acceso de recursos para la apertura de una puerta.

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica, validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tarjetas de proximidad o biometría) y a su vez controlando el recurso (puerta) por medio de un dispositivo eléctrico como un electroimán, solenoide, pestillo o motor.

Básicamente los controles de acceso se clasifican en dos tipos:

* Sistemas de Control de Acceso Autónomos
* Sistemas de Control de Acceso en Red

Los Sistemas de Control de Acceso Autónomos son sistemas que permiten controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica.

Los Sistemas de Control de Acceso en Red son sistemas que se integran a través de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Van desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados según se requiera. En la figura se representa un ejemplo de un Sistema de Control de Acceso en Red.

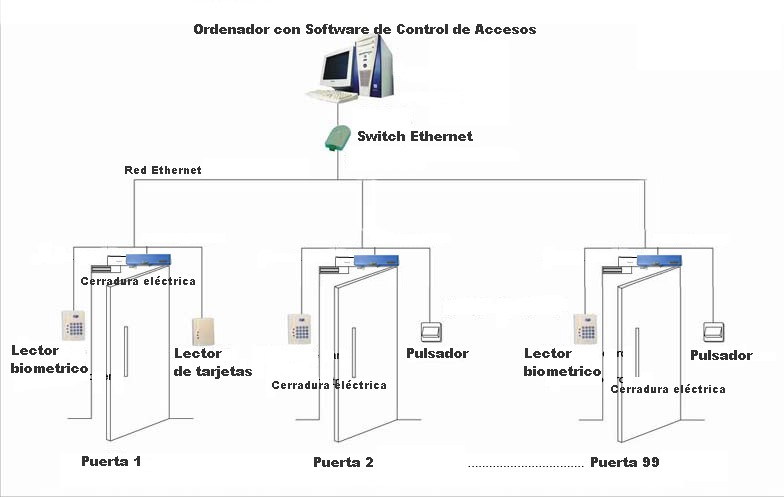


Figura 1.1 Ejemplo de un sistema de control de acceso en red.

En este trabajo se desarrollará un sistema de control de acceso en red, para el control físico de una puerta, se debe implementar un mecanismo electrónico que autentifique al usuario y en base a ello otorgar acceso a alguna dependencia, este sistema involucra el desarrollo de un software y hardware.

El software está asociado a una plataforma web para la gestión de la información, por medio de una interfaz gráfica, el administrador del sistema puede controlar los recursos que están disponibles para los usuarios; crear, editar y eliminar el perfil de los usuarios, configurar permisos, establecer horarios de acceso, exportar e imprimir informes y relatorios, entre otras funciones.

El hardware corresponde a un módulo electrónico de control de acceso, su función principal es realizar la autentificación de usuarios a través de diferentes métodos como; contraseñas, huella dactilar (biometría) y tarjetas RFID.

El módulo electrónico debe contar principalmente con los siguientes componentes:

* **Controlador**, este puede ser un microcontrolador o computador, es el encargado de gerenciar los diferentes sensores y principal comunicador con la plataforma web.
* **Pantalla**, el usuario puede visualizar gráficamente opciones de configuración e instrucciones.
* **Teclado**, necesario para realizar las configuraciones del módulo e ingreso de contraseñas de acceso.
* **Lector RFID**, este puede leer etiquetas RFID a una distancia de varios centímetros, utilizado para el registros de etiquetas al sistema y identificación de las mismas.
* **Sensor biométrico**, Lector de acceso biométrico de huella dactilar. Identifica al usuario a través de su huella dactilar (característica única e irrepetible para cada persona), lo que da un nivel de seguridad superior a cualquier otro sistema que utilice otro tipo de identificadores.
* **Reloj de tiempo real (RTC)**, utilizado para almacenar los horarios de las actividades en los registro.
* **Conector Ethernet o Wifi**, es necesario tener conectividad a una red de área local (LAN[[1]](#footnote-1)) o una red de área extensa (WAN[[2]](#footnote-2)), para realizar la transferencia de datos entre la plataforma y el módulo electrónico.
* **Relé**, dispositivo electromagnético, funciona como un interruptor controlado por un pulso electrónico, es el encargado de activar el circuito eléctrico del control de la puerta.

Conociendo los componentes necesarios para la implementación del módulo de control de acceso, a continuación se plantean diferentes modelos para el hardware.

### Modelos planteados para el hardware

Se proponen 3 modelos para la arquitectura del hardware del módulo de control de acceso:

1. El controlador del hardware es un microcontrolador[[3]](#footnote-3) este es el encargado de gerenciar cada uno de los periféricos, como se muestra en la figura 1.2, este ejecuta instrucciones almacenadas como números binarios organizados secuencialmente en la memoria principal, puede ser programado en diferentes lenguajes de programación como; visual basic, C, C++, assembler, Python, etc.

Este módulo electrónico interactúa con los usuarios, realiza la matriculación, verificación e identificación, controla la activación del relé para el actuador instalado en la puerta, funciona como servidor, este gestiona y administra la plataforma web, incluye un reloj de tiempo real y una memoria externa para el almacenamiento y registro de la información.



Figura 1.2 Arquitectura módulo control de acceso, modelo 1.

1. El controlador del hardware es un computador de placa reducida, se propone utilizar una “Raspberry Pi”, su sistema operativo oficial es RaspBian, una versión adaptada de Debian, aunque es compatible con diversos sistemas operativos, la Raspberry Pi cuenta con pines GPIO (General Purpose Input/Output), un sistema de Entrada/Salida de propósito general, las cuales son utilizadas para el gerenciamiento de los periféricos (ver figura 1.3). Cuenta con 4 puertos USB, adaptador para una memoria µSD, conector Ethernet y Wifi. Es compatibles con diferentes lenguajes de programación como; C++, Visual Basic, Phyton, Java, Javascript, HTML, PHP, Ruby, Node.js, etc.



Figura 1.3 Arquitectura módulo control de acceso, modelo 2.

Este módulo tiene las mismas funciones que el anterior, con la diferencia que este puede ejecutar diferentes procesos y tareas de forma simultáneas, e instalar servidores dedicados para el manejo de la plataforma web, es compatible con diferentes bases de datos (Mysql, MongoDB, Firebase) para el registro de la información.

1. Este modelo está compuesto por 2 hardware, el primero es el módulo de control de acceso, cuyo controlador principal es un microcontrolador, este comanda los sensores que interactúan con los usuarios, encargado de realizar los procesos de matriculación, verificación e identificación de los usuarios. Este hardware es gerenciado por un controlador maestro (Raspberry Pi) a través de un puerto serial (ver figura 1.4).



Figura 1.4 Arquitectura módulo control de acceso, modelo 3.

El segundo hardware corresponde a la computadora (Raspberry Pi), cumple la función de servidor y administra toda la información de la plataforma web, almacena los registros de los usuarios, permite el acceso a estos, contiene los historiales de acceso, etc. Este hardware integra un circuito con un reloj de tiempo real, para llevar el control del tiempo del servidor y un relé para el control del actuador de la puerta.

Este último funciona como un controlador maestro, está siempre recibiendo información del módulo de control de acceso, y cuando recibe una petición de un usuario este gestiona la información y envía una respuesta de vuelta.

### Justificación del modelo seleccionado

Los modelos planteados del hardware para el módulo de control de acceso utilizan como controlador principal un microcontrolador o un computador de placa reducida (Raspberry Pi), en la tabla 1.1 se pueden observar las principales características de cada controlador.

Tabla 1.1.1 Características microcontrolador v/s Raspberry Pi.

|  |  |  |
| --- | --- | --- |
|  | Microcontrolador (ATmega2560) | Raspberry Pi |
| Memoria RAM | 0.008 [MB] | 1 [GB] |
| Pines de Entrada/Salida | 54 | 40 |
| Velocidad de reloj | 16 [MHz] | 1.2 [GHz] |
| Multitarea | No | Si |
| Network | Ninguno | Ethernet y Wifi |
| Voltaje de entrada | 7 a 12 [V] | 5 [V] |
| Memoria Flash | 256 [KB] | Tarjeta SD, 2 a 16 [GB] |
| Puertos USB | 1 | 4 |
| Sistema operativo | Ninguno | Distribuciones de Linux |

La Raspberry Pi es 75 veces más rápido que el microcontrolador y tiene 125.000 veces más de memoria RAM. La Raspberry Pi es una computadora independiente que puede ejecutar un sistema operativo real en Linux. Puede realizar varias tareas, soportar cuatro puertos USB y puede conectarse de forma inalámbrica a Internet. En pocas palabras, es lo suficientemente potente como para funcionar como una computadora personal.

Puede sonar que Raspberry Pi es superior al microcontrolador, pero eso es sólo cuando se trata de aplicaciones de software. Por otra parte el microcontrolador tiene la capacidad de trabajar con pines analógicos y en tiempo real, esta flexibilidad le permite trabajar con casi cualquier tipo de sensor o chip.

Raspberry Pi puede procesar varias tareas, éste puede ejecutar múltiples programas en segundo plano mientras está activado. Por ejemplo, puede estar funcionando como un servidor y transmitiendo información por un puerto USB.

El modelo seleccionado es el número 3, en este modelo se aprovecha las ventajas de usar el microcontrolador y la Raspberry Pi, el módulo de control de acceso es controlado por el microcontrolador, es el encargado de gestionar la parte sensorial, el usuario interactúa con este módulo por medio de una pantalla LCD y un teclado matricial, en este dispositivo se realizan los procesos de matriculación, verificación e identificación de los usuarios. Cada vez que el usuario interactúa con este módulo se envía una petición a la Raspberry Pi, este procesa la información, y envía una respuesta.

La Raspberry Pi es el controlador principal del *sistema de control de acceso*, este aloja la plataforma web y almacena la información del sistema, tiene la capacidad de ejecutar procesos diferentes para la gestión del módulo de control de acceso, por lo que este sistema funcionara en tiempo real, además este integra los adaptadores de red ethernet y wifi de fácil configuración.

El módulo de control de acceso es instalado al exterior del lugar a controlar, y la Raspberry Pi se encuentra en el interior (ver figura 1.5), dando más seguridad e independencia al sistema, los usuarios que interfieran con el módulo exterior no podrán tener acceso a la información del sistema, ni manipular el actuador para la apertura de la puerta.

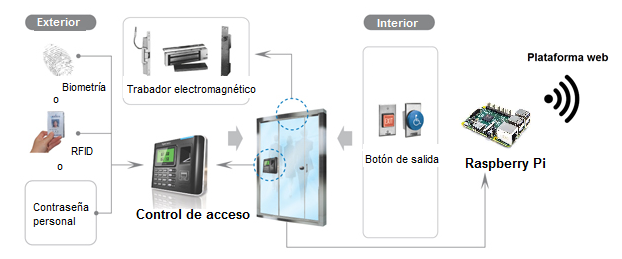


Figura 1.5 Referencia ubicación control de acceso, modelo 3.

## METODOLOGÍA

Para realizar el diseño y construcción de este proyecto, es necesario dividir el trabajo por etapas, el capítulo 1 corresponde a la introducción, en donde se definen los objetivos del proyecto, descripción del planteamiento de la investigación y el análisis de diferentes soluciones para el diseño del hardware del proyecto.

En el capítulo 2, se desarrolla las principales técnicas de identifación y autenticación de usuarios del módulo de control de acceso, es primordial conocer la teoría del funcionamiento de los sensores que realizan estas funciones.

El capítulo 3 aborda el diseño del sistema de control de acceso, en esta etapa se describe el esquema del sistema de control de acceso, selección y justificación de los componentes que se utilizarán y diseño de los circuitos que forman parte del sistema de control de acceso.

En el capítulo 4 se desarrollan las programaciones en general del hardware y de la plataforma web, principalmente la programación de la interfaz gráfica del sistema de control de acceso, se implementa la gestión de perfiles y permisos de usuarios, la exportación de informes e historial de usuarios, configuración del servidor, se comprueba el correcto funcionamiento del software con el hardware.

Una vez creada la plataforma web y con el hardware funcionando, en el capítulo 5 se muestran los resultados obtenidos luego del diseño y construcción del sistema de control de acceso, se menciona el funcionamiento del sistema, la sincronización total entre la plataforma web y el módulo electrónico.

El capítulo 6 aborda el análisis económico del proyecto, los costó de implementación, viabilidad, análisis de mercado y un posible plan de negocio. Finalmente en el capítulo 7, se muestran las conclusiones y los resultados esperados en el corto y mediano plazo luego del término del proyecto.

**CAPITÚLO**

# TÉCNICAS DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

La identificación digital forma parte indisoluble de la mayoría de servicios en Internet y en las tecnologías de la información. Por ejemplo, para subir un vídeo en un servidor web, se pide que el usuario esté registrado y se identifique para poder llevar a cabo la publicación del contenido. Por otra parte, para utilizar una tarjeta magnética de acceso, es preciso que el usuario esté registrado en la plataforma de control. Para realizar acciones tan variadas como hacer un pago mediante tarjeta de crédito, utilizamos esta misma tarjeta para identificarnos. O bien para hacer gestiones bancarias a través de Internet, lo primero que haremos es especificar quién somos.

Esta identificación digital puede ser relativamente sencilla. Basta con disponer de un nombre de usuario, usar como identificador la dirección de correo electrónico o, en el caso de un pago, usar el número de tarjeta de crédito. Ahora bien, para la mayoría de servicios, además de la identificación digital, es necesaria una autenticación de esta identidad.

Mediante la autenticación de la identidad, el servicio se asegura de que el usuario es quien dice ser.

El concepto de "quien dice ser" lo resuelve el identificador de usuario: mediante una cadena de caracteres se denota cuál es la identidad del usuario. Y para demostrar la autenticidad de la identidad del usuario se pueden usar cuatro aproximaciones distintas:

**1)** El usuario es quien dice ser si demuestra conocer algo que solamente este conoce. Por ejemplo, conoce una palabra secreta de acceso.

**2)** El usuario es quien dice ser si posee algún objeto, como por ejemplo una tarjeta magnética para el acceso a un edificio.

**3)** El usuario es quien dice ser si posee alguna característica física que sólo él tiene: por ejemplo, la huella dactilar.

**4)** El usuario es quien dice ser si es capaz de hacer algo de forma única: por ejemplo, el patrón de escritura o la forma de andar.

Pese a tratarse de cuatro formas de abordar la autenticación de la identidad, no existe una frontera clara entre algunas de ellas. Además, es perfectamente posible el uso de varias de estas técnicas de forma combinada, para conseguir mayores grados de seguridad.

Por ejemplo, disponer de una tarjeta con códigos de seguridad para permitir operaciones bancarias a través de Internet (tarjeta de coordenadas) podría verse como una mezcla entre los dos primeros casos: el usuario posee la tarjeta, pero podría decirse que es conocedor de una información, aunque en este caso la tenga escrita.

Por otra parte, todas estas formas de abordar la autenticación no están exentas de problemas de seguridad. Por ejemplo, la tarjeta con códigos podría ser robada y usada por otro usuario. Otro caso podría ser la obtención de una clave de acceso mediante un correo electrónico fraudulento.

La usurpación de identidad consiste en que una entidad use con éxito el mecanismo de identificación que identifica a otra identidad.

En este apartado se exponen las principales técnicas y tecnologías para implantar la identificación y autenticación de usuarios en un sistema de control de acceso de personas.

## 2.1 Contraseñas

La autenticación por medio de contraseñas es relativamente sencilla: el usuario “*A”* envía su identificador “*IDA”* y acto seguido su contraseña “*CSA”*. La implementación del protocolo de identificación puede precisar que ambas informaciones se manden en un mismo mensaje, o bien que primero se pida el nombre de usuario y después la contraseña.

Esta contraseña es usada por el servicio para validar la identidad del usuario. Si *A* es el único conocedor de *CSA*, es altamente probable que el usuario sea realmente *A*. En la figura 2.1, el usuario utiliza su contraseña para validarse al servicio. Este dispone de una lista de pares con usuarios y contraseñas para comprobar las identidades. Ante una contraseña correcta, el servicio manda un mensaje de autenticación correcta al equipo del usuario. Algunos servicios incluye una hora de caducidad de esta autenticación, tras la cual el usuario deberá volver a autenticarse.

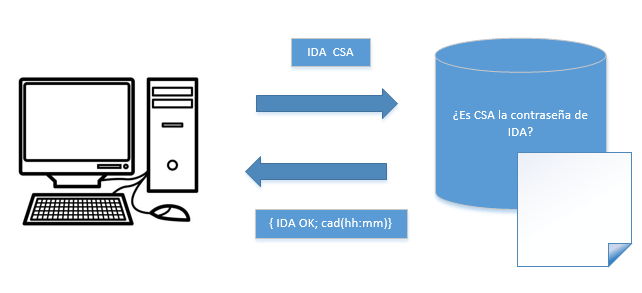


Figura 2.1 Esquema de funcionamiento de autentificación mediante contraseña.

La contraseña es una cadena de caracteres de longitud arbitraria. En algunos escenarios, se usa una versión reducida de la contraseña, formada tan sólo por unos pocos números. En este caso la contraseña se conoce con el nombre de PIN, en algunos entornos se utiliza el término PIN cuando en realidad la contraseña está formada tanto por letras como por números.

Así como un mismo servicio o sistema no permite que haya dos usuarios con el mismo identificador, es perfectamente posible que dos o más usuarios tengan la misma contraseña.

## 2.2 Identificación por Radio Frecuencia (RFID)

La identificación por radio frecuencia (RFID) se está convirtiendo en algo común en la vida cotidiana en estos días la podemos encontrar en tarjetas de pago, también es utilizado en el sistema de cobro de las autopistas o carreteras, por otra parte es utilizado por empresa para llevar el control del inventario de productos y equipos, la mayoría de nosotros encontramos etiquetas RFID al menos un par de veces a la semana y nunca pensamos en lo que se puede hacer con esta tecnología.

### 2.2.1 Funcionamiento de la Identificación por Radio Frecuencia (RFID)

El intercambio de un sistema RFID implica dos actores: un iniciador y un objetivo. El iniciador, es un lector o lector/escritor de dispositivo, este inicia el intercambio mediante la generación de un campo magnético y escucha las respuestas de cualquier objetivo que se encuentre dentro del radio, ver figura 2.2. El objetivo, es una etiqueta, que responde cuando se recoge una transmisión desde un iniciador y responderá con un número identificador único (UID).

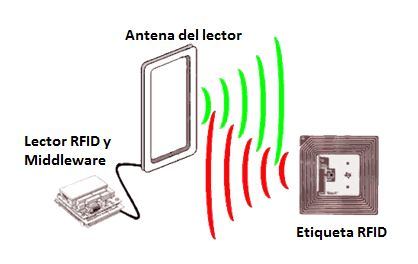


Figura 2.2 Campos magnético generado por un sistema RFID.

Existen 3 componentes básicos en un sistema RFID, ver figura 2.3.

1. La etiqueta o transponder de RFID consiste en un pequeño circuito, integrado con una pequeña antena, capaz de transmitir un número de serie único hacia un dispositivo de lectura, como respuesta a una petición. Algunas veces puede incluir una batería.

2. El lector, (el cual puede ser de lectura o lectura/escritura) está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control, sirve para energizar la tarjeta de identificación y capturar su número, para posteriormente enviarlo a un sistema de control o un computador que se encargue de procesar los datos.

3. Un controlador o un equipo anfitrión, comúnmente una PC o Workstation, Este se encarga de recibir y procesar los datos pertenecientes al número de identificación de la etiqueta presentada en la lectora, la cual corre una base de datos y algún software de control

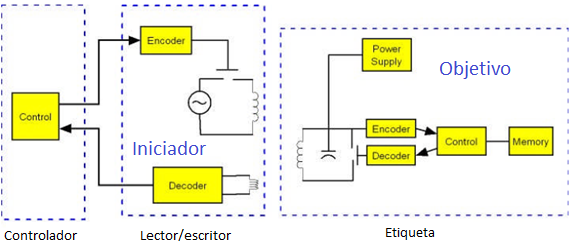


Figura 2.3 Esquema y componentes de un sistema RFID.

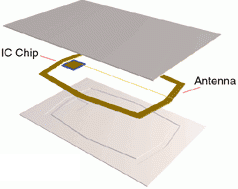
Las etiquetas RFID tienen una pequeña cantidad de memoria a bordo, como se muestra en la figura 2.4, por lo general menos de 1 kilobyte. Un dispositivo iniciador puede leer estos datos, y si se trata de un dispositivo de lectura/escritura, se puede escribir en el etiquetar también. Esto le permite almacenar pequeñas cantidades de información asociados con la tarjeta. Por ejemplo, a veces se utiliza en sistemas de transporte que utilizan RFID, para realizar un seguimiento del valor que queda en la tarjeta. Sin embargo, desde los sistemas de RFID en general, están conectados en red a una base de datos, es más común para almacenar un registro de datos indexada por el UID de la etiqueta en una base de datos remota, y almacenar toda la información acerca de la etiqueta en esa base de datos remota.

Figura 2.4 Estructura etiqueta RFID.

### 2.2.3 Clasificación

La tecnología de identificación por radiofrecuencia puede ser dividida principalmente en 3 categorías según el tipo de etiqueta:

1. Sistemas pasivos, en los cuales las etiquetas de RFID no cuentan con una fuente de poder. Su antena recibe la señal de radiofrecuencia enviada por el lector y almacena esta energía en un capacitor. La etiqueta utiliza esta energía para habilitar su circuito lógico y para regresar una señal al lector. Estas etiquetas pueden llegar a ser muy económicas y pequeñas, pero su rango de lectura es muy limitado.

2. Sistemas activos. Utilizan etiquetas con fuentes de poder integradas, como baterías. Este tipo de etiquetas integra una electrónica más sofisticada, lo que incrementa su capacidad de almacenamiento de datos, interfaces con sensores, funciones especializadas, además de que permiten que exista una mayor distancia entre lector y etiqueta (20m a 100m). Este tipo de etiquetas son más costosas y tienen un mayor tamaño. Pueden permanecer dormidas hasta que se encuentran dentro del rango de algún lector, o pueden estar haciendo broadcast constantemente.

3. Sistemas Semi-Activos. Emplean etiquetas que tienen una fuente de poder integrada, la cual energiza la etiqueta para su operación, sin embargo, para transmitir datos, una etiqueta semi-activa utiliza la potencia emitida por el lector. En este tipo de sistemas, el lector siempre inicia la comunicación. La ventaja de estas etiquetas es que al no necesitar la señal del lector para energizarse (a diferencia de las etiquetas pasivas), pueden ser leídas a mayores distancias, y como no necesita tiempo para energizarse, estas etiquetas pueden estar en el rango de lectura del lector por un tiempo substancialmente menor para una apropiada lectura. Esto permite obtener lecturas positivas de objetos moviéndose a altas velocidades.

Tanto las etiquetas activas como los pasivos pueden adicionalmente ser clasificados de la siguiente forma:

* Solo Lectura (RO)

En estos dispositivos, los datos son grabados en la etiqueta durante su fabricación, para esto, los fusibles en el microchip de la etiqueta son quemados permanentemente utilizando un haz láser muy fino. Después de esto, los datos no podrán ser reescritos. Este tipo de tecnología se utiliza en pequeñas aplicaciones, pero resulta poco práctico para la mayoría de aplicaciones más grandes, que intentan explotar todas las bondades de RFID.

* Una Escritura, Muchas Lecturas (WORM)

Una etiqueta WORM, puede ser programado sólo una vez, pero esta escritura generalmente no es realizada por el fabricante sino por el usuario justo en el momento que la etiqueta es creada. Este tipo de etiquetas puede utilizarse en conjunto con las impresoras de RFID, las cuales escriben la información requerida en él.

* Lectura y Escritura (RW)

Estas etiquetas, pueden ser reprogramadas muchas veces, típicamente este número varía entre 10,000 y 100,000 veces, incluso mayores. Esta opción de reescritura ofrece muchas ventajas, ya que la etiqueta puede ser escrito por el lector, e inclusive por sí mismo en el caso de los tags activos. Estas etiquetas regularmente contienen una memoria Flash o FRAM para almacenar los datos.

### 2.2.4 Regulación y estandarización

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

Contrariamente a la creencia popular, no existe un protocolo RFID universal para esta tecnología. Hay docenas. Los estándares de RFID desarrollado por la Organización Internacional de Estándares (ISO), en conjunción con los principales participantes en el mercado. ISO funciona como un órgano de mediación para ayudar a los competidores en muchas industrias diferentes a desarrollar estándares interoperables de modo que incluso cuando compiten, sus tecnologías pueden a veces trabajar juntas. Los diferentes estándares de RFID definen las frecuencias de radio utilizado, las velocidades de transferencia de datos, los formatos de datos, entre otros parámetros. Por ejemplo, la norma ISO-11784 fue originalmente desarrollada para el rastreo de animales. Se opera en las frecuencias comprendidas entre 129 y 139.4 kHz, y su formato de datos incluye campos adecuados para la descripción de los animales para ser rastreado. También se puede encontrar lectores con el protocolo EM4100 y etiquetas que operan en el 125kHz distancia. Estos se utilizan a menudo como tarjetas de proximidad, y cuentan con una información muy limitada en su protocolo de datos, por lo general sólo un UID. Las normas ISO-14443 se desarrollaron para utilizar con los sistemas de pago y tarjetas inteligentes. Estas operan a 13,56 MHz. Incluyen características en su formato de datos para aumentar o disminuir los valores y para la codificación de datos.

## 2.3 Biometría

La biometría es la aplicación de las matemáticas y la ciencia de la computación para identificar individuos de acuerdo con sus características o rasgos físicos. La palabra biometría deriva del griego bios (que quiere decir vida) y metria (que quiere decir medida). Los rasgos biométricos son medidas extraídas del cuerpo humano vivo. Y, además, todos los rasgos biométricos son una combinación de anatomía y de comportamiento.

La biometría se está convirtiendo en un factor esencial para la identificación eficaz de las personas. Esto se debe a que los rasgos biométricos no se pueden compartir o extraviar y representan intrínsecamente las formas corporales del individuo que identifica. Reconocer a una persona por su cuerpo y después enlazar este cuerpo con una identidad establecida externamente forma una herramienta muy poderosa para la gestión de la identidad con unas consecuencias potenciales enormes, tanto positivas como negativas. En consecuencia, la biometría no es solo un problema fascinante en el campo de la investigación dedicado al reconocimiento de patrones, sino una tecnología que, usada correctamente, puede permitir una sociedad más segura, reducir el fraude y proveer interfaces persona-máquina fáciles de usar.

El reconocimiento biométrico se refiere al uso de diferentes características anatómicas (como huellas dactilares, cara o iris) y de comportamiento (como habla, firma o teclear). Estas características se denominan identificadores biométricos o rasgos biométricos y sirven para reconocer automáticamente a los individuos.

A continuación enumeramos los rasgos biométricos más utilizados, comentando aspectos sobre su calidad y uso:

• **Huellas dactilares**. El uso de las huellas dactilares como medio de identificación es de alta fiabilidad. Tiene buena aceptación y popularidad.

• **Ojo**. La identificación de un individuo a través del análisis del iris tiene una fiabilidad muy alta. El problema es la facilidad de uso. El análisis de la retina para identificar al individuo es más complejo todavía.

• **Forma de la mano**. Este sistema está bastante extendido, pero quizás presenta un poco menos de fiabilidad que los anteriores. Este sistema es susceptible de padecer ataques, puesto que no resultaría difícil recrear la forma de una mano usando un molde.

• **Cara**. El análisis de la cara, ya sea en 2D o 3D, es un buen medio para identificar a un individuo. Aun así, siempre es preferible un estudio 3D, ya que se mejoran los resultados con respecto el mero estudio de una imagen 2D, y se dificulta el éxito de ataques. La desventaja de los equipos 2D es que el sistema no distingue si lo que está capturando es realmente un rostro o una fotografía de un rostro.

• **Venas del dedo o la mano**. El estudio vascular de los dedos o de la mano proporciona alta fiabilidad, además no es muy complejo su análisis.

• **Voz**. Este sistema presenta bastante fiabilidad, pero también es susceptible a los ataques. Además este sistema padece de poca estabilidad, con lo cual deberían ser varias la toma de voces analizadas para reducir la tasa de errores.

Claramente, son varias las características biométricas que pueden usarse para identificar o autenticar. Estas pueden usarse individualmente o bien en combinación entre ellas, o bien procediendo a la autenticación mediante información adicional, como podría ser una contraseña.

### 2.3.1 Sistemas biométricos

En función del contexto de la aplicación biométrica, podemos diferenciar dos tipos de sistemas, los sistemas de verificación y los sistemas de identificación.

Los sistemas de verificación (también llamados de autentificación) autentifican la identificación de la persona mediante la comparación del rasgo biométrico acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema.

El usuario tiene que presentar su identificación mediante un carné o clave secreta. El sistema realiza una única comparación entre el rasgo biométrico que el usuario acaba de presentar con el rasgo biométrico que hay en la base de datos con la misma identificación presentada. La salida de un sistema de verificación es normalmente binaria: es la misma persona si los rasgos biométricos coinciden (son muy similares) o son dos personas diferentes en otro caso. En algunos casos, los rasgos biométricos y la identificación de la base de datos están en la propia tarjeta del usuario en forma encriptada. En este caso, se dice que disponemos de una base de datos distribuida entre todas las tarjetas de los usuarios.

Los sistemas de identificación reconocen a la persona a través de la busca del rasgo biométrico que más se asemeja al usado para identificarlo en toda una base de datos.

El usuario no aporta ninguna información de su identificación, como era el caso del sistema de verificación. El sistema lleva a cabo una comparación uno a muchos. Esto quiere decir que el rasgo biométrico del usuario desconocido se compara con muchos rasgos biométricos de una base de datos. Hay varias salidas a este sistema. La más sencilla es devolver el nombre de la persona (identificador) cuyo rasgo biométrico se asemeja al introducido. Otra posibilidad es deducir que este rasgo biométrico no pertenece a ninguna persona de la base de datos (este caso se da cuando las distancias del rasgo biométrico con todos los rasgos biométricos de la base de datos es superior a un umbral). Finalmente, y es el caso más usual en las aplicaciones forenses, el sistema no devuelve una sola persona sino una lista de candidatos. Es decir, devuelve las personas cuya distancia de sus rasgos biométricos con el rasgo biométrico introducido es inferior a un umbral.

Tanto los sistemas de verificación como de identificación necesitan un proceso previo llamado sistema de matriculación[[4]](#footnote-4). Este proceso se encarga de recoger el rasgo biométrico (o los rasgos biométricos) junto con la identificación de la persona. Este proceso es muy importante puesto que se encarga de relacionar la identificación de la persona con el rasgo biométrico. Normalmente, este proceso tiene lugar ante una persona autorizada que vela por la veracidad de los datos que aporta el usuario (carné de identidad, pasaporte) y controla que realmente sea este usuario el que presenta el rasgo biométrico al sistema. Además, durante el proceso de matriculado, esta persona verifica la calidad de los datos biométricos obtenidos. Si considera que los datos no tienen suficiente calidad, pide al usuario que vuelva a presentar el rasgo biométrico (huella dactilar, cara, iris) al sistema.

Es fundamental que los datos que se almacenan en la base de datos tengan la máxima calidad puesto que en los procesos de identificación o verificación no siempre se puede garantizar esta calidad. Algunos sistemas piden al usuario capturar varias veces el mismo rasgo biométrico (normalmente tres veces). El sistema puede elegir la mejor imagen o fusionarlas y así reducir los errores de captura.

Los tres sistemas antes mencionados usan los procesos siguientes (ver la figura 2.5):

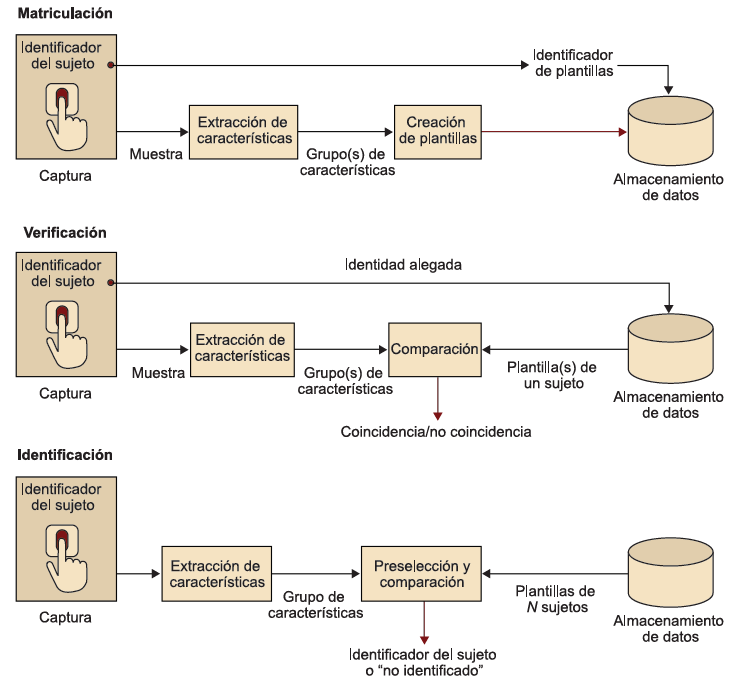


Figura 2.5. Etapas o procesos que componen los sistemas: a. matriculación; b. verificación; c. identificación.

• Captura: La representación digital del rasgo biométrico tiene que ser capturada. El sensor biométrico es usualmente un sistema para capturar una imagen (excepto la identificación del hablador, que es una máquina de grabar voz). Normalmente, la información capturada se denomina muestra[[5]](#footnote-5). A veces, el sistema de captura también incorpora otros periféricos para introducir información no biométrica o mostrar información.

• Extracción de las características: Con el objetivo de facilitar la comparación, aumentar la información y reducir el ruido, la representación original digital (imagen digital) se procesa normalmente con un extractor de características para generar una representación compacta y más identificadora llamada registro de identificación[[6]](#footnote-6) o conjunto de características[[7]](#footnote-7).

• Creación de la plantilla: La plantilla[[8]](#footnote-8) es una forma compacta de representar un conjunto de muestras de una sola característica biométrica (por ejemplo, se puede crear una plantilla de dieciséis muestras diferentes de la imagen de la cara de una misma persona). El proceso de creación de la plantilla recibe como entrada los registros de identificación y crea una información más compacta donde se intenta extraer la información que persiste en todas las muestras puesto que se consideran los rasgos característicos.

En algunos casos, esta plantilla está formada por una única muestra y por lo tanto se puede representar como un registro de identificación.

• Comparación: El proceso de comparación recibe como entrada un registro de identificación y una plantilla y calcula una distancia entre los dos. A veces, en lugar de una distancia obtiene una probabilidad de que representen un mismo individuo. En el proceso de verificación, hay un umbral interno al sistema que solo lo puede modificar el administrador del sistema. Si la distancia es inferior al umbral (o la probabilidad es superior al umbral), el sistema considera que los dos datos provienen de la misma persona, de lo contrario, se considera que provienen de dos personas diferentes.

• Selección o filtrado: En los sistemas de identificación con muchos datos (podemos hablar de 50 millones de huellas dactilares), el filtrado es un método para aumentar el tiempo de respuesta del sistema. Con técnicas típicas de las bases de datos, logran no tener que explorar la base de datos entera y así ganar tiempo.

• Almacenamiento de los datos: Es el proceso para almacenar la información del usuario. Esta información está compuesta por un identificador único (por ejemplo, el número del DNI o del pasaporte), la plantilla biométrica y otros datos (por ejemplo, la dirección o la profesión). En función de la aplicación, los datos se almacenan en sistemas de almacenamiento centralizados (para poder llevar a cabo la identificación) o en tarjetas inteligentes[[9]](#footnote-9) (para poder llevar a cabo la verificación). Además, se aplican técnicas de encriptación con todos los datos para que así el registro formado por el número del DNI más los rasgos biométricos sea indivisible.

Dependiendo del dominio de la aplicación, un sistema biométrico puede operar como un sistema en línea o como un sistema fuera de línea.

a) Los sistemas en línea requieren que la comparación se lleve a cabo rápidamente y se requiere una respuesta inmediata, por ejemplo es el caso del permiso para iniciar una aplicación o la entrada física de una persona a unas instalaciones. Normalmente, son sistemas de verificación.

b) Los sistemas fuera de línea no requieren que la respuesta sea inmediata y se tolera que haya un admisible retraso en la respuesta. Normalmente, son sistemas de identificación. Los sistemas en línea suelen ser completamente automáticos, requieren que el rasgo biométrico sea capturado con un sensor electrónico y no hay control humano de la calidad de los datos. Por otro lado, los sistemas fuera de línea son usualmente semiautomáticos. La captura del rasgo biométrico puede haber sido con un sistema no electrónico (por ejemplo, la captura de una huella dactilar dejada en la escena de un crimen) y hay un control de la calidad de los datos por parte de un especialista. Además, este especialista dispone de herramientas informáticas para arreglar los datos o ayudar al programa a que lleva a cabo la comparación biométrica.

Dependiendo de la aplicación, se llevan a cabo dos tipos de buscas en los sistemas de identificación, que son las buscas positivas y las buscas negativas:

a) Las buscas positivas son aquellas por las que queremos comprobar si aquel rasgo biométrico se encuentra en la base de datos, es decir, si el usuario ha sido matriculado. Deseamos saber la identificación de aquel rasgo biométrico. El caso más típico es introducir en el sistema una huella dactilar que hemos encontrado en una escena de un crimen o una cara que hemos podido fotografiar y queremos saber a quién pertenece.

b) Por otro lado, las buscas negativas son aquellas por las que queremos comprobar que aquel individuo no se ha matriculado. Deseamos saber que no hay ninguna persona matriculada con aquellos rasgos biométricos. La aplicación más usual es asegurarse de que una persona no quiere usar más de una vez un servicio que solo tiene derecho a usar una sola vez, como, por ejemplo, no cobrar varias veces una ayuda estatal o no votar varias veces en unas elecciones.

### 2.3.2 Lector huella digital

Los seres humanos tienen tarjetas de identificaron integradas, muy fácilmente accesibles, las cuales son diseños virtualmente únicos. Estas son diminutos “Valles y crestas” de piel en la punta de los dedos, en la figura 2.6 se muestra la imagen generada por un lector biométrico. Estas se forman por una combinación de factores genéticos y ambientales aleatorios, por lo que es única para cada persona.



Figura 2.6 Imagen capturada por un sensor biométrico.

Un lector de huellas dactilares es un dispositivo de [hardware](http://www.alegsa.com.ar/Dic/hardware.php) que permite escanear o leer una huella digital de un ser humano con el fin de identificarlo.

El funcionamiento de un lector de huella digital cumple dos tareas principales:

* Obtener una imagen de la huella digital.
* Comprar el patrón de valle y cresta de dicha imagen con los patrones de las huellas que tiene almacenadas.

El uso más típico de un lector de huellas dactilares es la [autentificación](http://www.alegsa.com.ar/Dic/autentificacion.php) de un [usuario](http://www.alegsa.com.ar/Dic/usuario.php) para permitirle o no el acceso a un dispositivo o servicio. También se incluyen en cerraduras para abrir puertas o para control de entrada-salida de personas de una empresa.

Hay 2 tipos de tecnología empleadas para estos dispositivos:

**Lector óptico:** esta tecnología utiliza diminutos [diodos](http://www.informaticamoderna.com/Electricidad_y_computadoras.htm#elem) que emiten luz, integrados en un sensor denominado CCD (Charged Coupled Device), el cuál detecta los relieves por medio de sombras e iluminación de la superficie del dedo, posteriormente forma un mapa digital con la información y determina que tenga la iluminación correcta y una vez realizada esta verificación, esta puede ser enviada a la computadora para su almacenamiento, de lo contrario seguirá creando la imagen digital. En la figura 2.7 se observa el método de lectura de un sensor óptico.

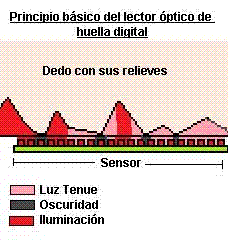


Figura 2.7. Método de lectura de huella digital óptico.

**Lector capacitivo:** esta tecnología utiliza diminutos [capacitores](http://www.informaticamoderna.com/Electricidad_y_computadoras.htm), los cuáles se cargan con diferentes cantidades de corriente de acuerdo a la posición de los relieves del dedo, de este modo crea un mapa digital con la información y no es necesario verificarla, sino que se envía de manera inmediata a la computadora, siendo una tecnología más fiable y veloz. En la figura 2.8 se observa el principio de funcionamiento del lector capacitivo de huella digital.

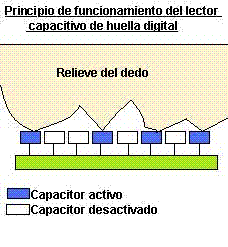


Figura 2.8. Método de lectura de huella digital capacitivo.

En general existen distintos problemas a los que hacer frente. El primero es el de la recogida de características: los sistemas deben obviar ruidos, imperfecciones o distintos matices que los sistemas captadores y sensores recogen a cada acceso de un individuo. En segundo lugar, se deben minimizar las tasas de errores del sistema de identificación: no se debe permitir la autenticación de un individuo no registrado o no válido y, al contrario, no se debe denegar la correcta autenticación de un individuo registrado o válido.

**CAPITÚLO**

# DISEÑO SISTEMA DE CONTROL DE ACCESO

El sistema de control de acceso consiste en controlar el acceso de personas a un lugar físico determinado, con la finalidad de aumentar la seguridad y llevar el control de ingreso de personas. En el capítulo 1 se describió el modelo para el sistema de control de acceso, se desarrollará un sistema en red, el módulo de control de acceso que identifica a los usuarios está conectado a un computador que gerencia una plataforma web como software de control de los recursos del sistema.

En este capítulo se desarrollará el diseño de los hardwares necesarios para el sistema de control de acceso, y se verá en detalle las características y funcionalidades de cada uno de los componentes del sistema.

## 3.1 Infraestructura del sistema de control de acceso

A continuación se describe la infraestructura necesaria para el funcionamiento del sistema.

* **Módulo control de acceso**, este dispositivo es el principal hardware que interactúa con los usuarios, integra una pantalla LCD y un teclado numérico en los cuales los usuarios pueden visualizar e ingresar información al sistema. Además este realiza los procesos de registro, verificación e identificación de usuarios, por medio del sensor biométrico de huella dactilar, etiquetas RFID o por contraseñas.

El microcontrolador del módulo de control de acceso es gerenciado por un computador, este envía y recibe la información a través de comunicación serial **UART**, acrónimo de **U**niversal **A**synchronous **R**eceiver-**T**ransmitter, este protocolo de comunicación será expuesto más adelante en este capítulo.

* **Computador**, corresponde a un computador de placa reducida, cumple la función administrar la información del módulo de control de acceso, incluye una base de datos para almacenamiento de la información del sistema y ejecuta en tiempo real un servidor web que contiene la interfaz gráfica para la gestión del sistema de control acceso.
* **Circuito de control**, el computador está conectado a un circuito a través de sus pines de entrada y salida, este controla el relé que activara el actuador de la puerta, tiene reloj para el control del tiempo de los registro, regula la tensión de entrada para alimentar el computador y el actuador de la puerta.
* **Cerradura eléctrica**, este es el actuador eléctrico encargado de controlar la apertura de la puerta, consiste en un electroimán que es activado por un pulso electromagnético.
* **Botón de apertura**, se debe instalar un pulsador al interior del lugar a controlar, este cuando es pulsado envía una señal al circuito del computador para la apertura de la puerta.
* **Fuente de poder**, este es el encargado de la alimentación eléctrica del sistema de control de acceso, para que el sistema de control de acceso funcione en todo momento se debe utilizar un sistema de alimentación ininterrumpida en inglés *uninterruptible power supply* (**UPS**).

En la figura 3.1 se puede observar la infraestructura necesaria para el funcionamiento del sistema de control de acceso e indica la conexión de los componentes.

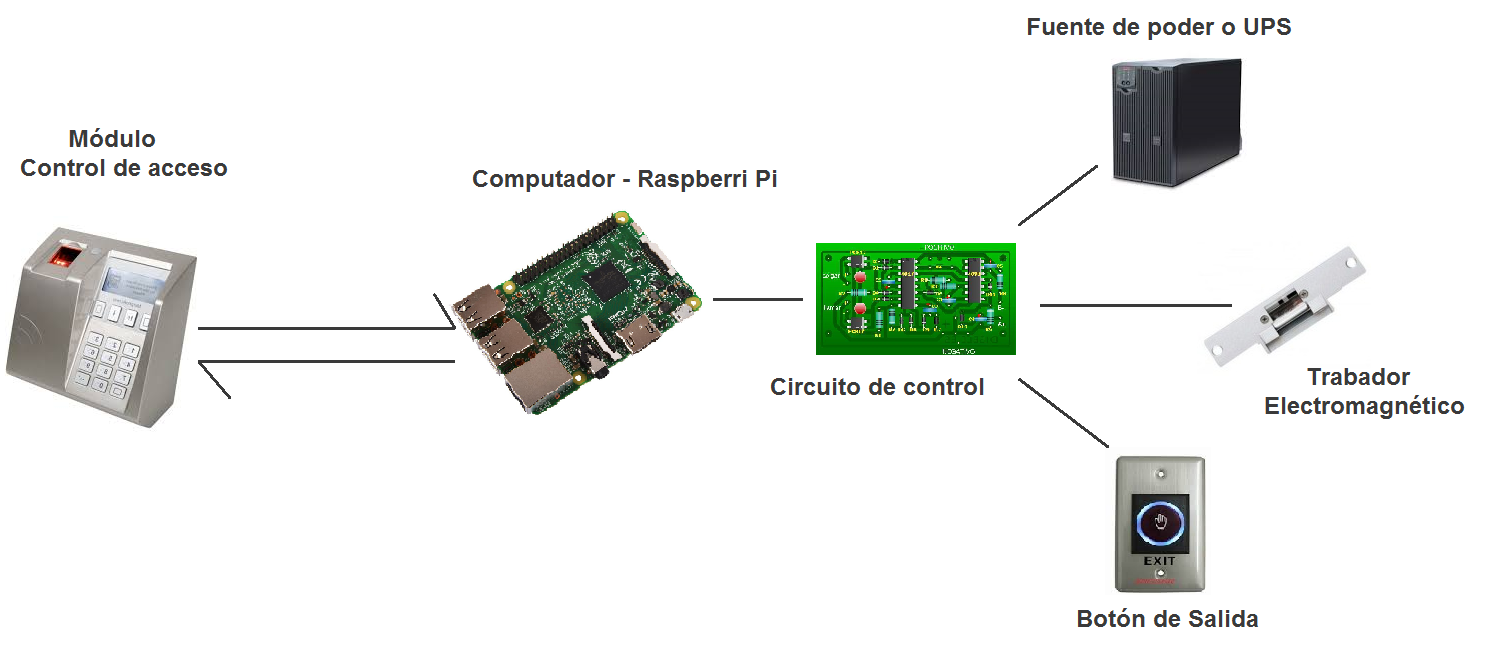


Figura 3.1 Infra estructura del sistema de control de acceso.

A continuación se detalla y describe cada uno de los dispositivos mencionados anteriormente.

## 3.2 Módulo control de acceso

Como se ha mencionado anteriormente este dispositivo es el encardo de registrar, autentificar e identificar a los usuarios, para poder realizar estas funciones este módulo debe integrar la tecnología necesaria. En el capítulo 1 se describió de forma general los componentes de este módulo, en la figura 3.2 se observa el diagrama del módulo de control de acceso con los componentes que este debe integrar.



Figura 3.2 Diagrama módulo control de acceso

El principal desafío para la implementación de este módulo de control de acceso, es la integración de cada uno de los dispositivos y sensores electrónicos en el microcontrolador y que estos funcionen de manera correcta, a continuación se detallará los componentes propuestos.

### 3.2.1 Display LCD

El display LCD (Liquid Crystal Dysplay) o pantalla de cristal líquido es el dispositivo empleado para la visualización de contenidos, instrucciones de manejo o información, de una forma gráfica, mediante caracteres o símbolos (ver figura 3.2 ), permitiendo así la comunicación entre el módulo de control de acceso y los usuarios. Se encuentran en diferentes formatos, por ejemplo, 2x8, 2x16, 4x20, etc. El primer digito indica el número de filas del display y el segundo el número de columnas, es decir, 4x20 significa que tiene 4 filas y 20 columnas.



Figura 3.3 Vista frontal del LCD alfanumérico 4x20

Este dispositivo es gobernado por el controlador HD44780 de Hitachi, está incorporado sobre la misma placa de circuito impreso que soporta el LCD. El controlador se encarga de gestionar el display líquido: polarizar los puntos de la pantalla, generar los caracteres, desplazar la pantalla, muestra el cursor, etc. El usuario se despreocupa de todos estos problemas y simplemente necesita conocer una serie de comandos o instrucciones de alto nivel (limpia display, posiciona cursor, etc.) que le permitirán mostrar mensajes o animaciones sobre la pantalla de forma sencilla. Para comunicarse con el controlador del display se dispone de una interfaz paralela al exterior, de fácil conexión a otros microcontroladores o microprocesadores.

El LCD dispone de una zona de memoria interna no volátil llamada ROM[[10]](#footnote-10) donde se almacena una tabla con los 192 caracteres que pueden ser visualizados. Cada uno de los caracteres tiene su representación binaria de 8 bits. Para visualizar un carácter debe recibir por el bus de datos el código correspondiente. La tabla de la representación binaria de caracteres se puede consultar en el apartado A.1.1 del Anexo.

El fabricante reserva una pequeña zona de memoria RAM[[11]](#footnote-11) donde se pueden definir algunos caracteres especiales, como por ejemplo la letra ñ que no suele venir, o si se desean, pequeños gráficos.

El display alfanumérico dispone de 16 pines y son compatibles con pulsos TTL. En la tabla 3.1 se muestra el significado de las señales de cada pin. Hay tres tipos de señales en el LCD: alimentación, control y datos.

Tabla 3.1 Descripción de pines del display LCD

|  |  |  |
| --- | --- | --- |
| **N° PIN** | **Símbolo** | **Descripción** |
| 1 | Vss | Tierra de alimentación. |
| 2 | Vdd | Alimentación 5 V. |
| 3 | Vo | Contraste de pantalla. |
| 4 | RS | Selección de comandos de control y datos. |
| 5 | R/W | Señal de lectura o escritura. |
| 6 | E | Habilitación. |
| 7-14 | D0-D7 | Bus de datos. |
| 15 | A | Ánodo retroiluminación |
| 16 | K | Cátodo retroiluminación |

**Señales de alimentación**: Son tres señales correspondientes a los pines 1, 2 y 3. El pin 1 corresponde a la tierra, el 2 a la alimentación positiva (+5Vdc) y el 3 al ajuste del contraste. Habitualmente, al dar alimentación y sin haber mandado todavía ningún comando, el display muestra en su pantalla la primera fila con todos sus caracteres en negro. Si no fuera así, se debería proceder al ajuste del contraste. Para ello, se debe instalar un potenciómetro de unos 5 KΩ tal y como se observa en la figura 3. Cuanto menor es el voltaje en el pin 3 (VO) mayor será el contraste.

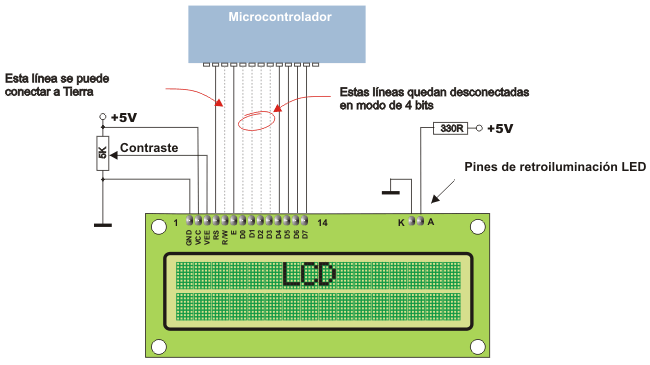


Figura 3 Conexión del potenciómetro de ajuste del contraste

**Señales de control**: Los pines 4, 5 y 6 forman las señales de control del LCD. El pin 4 (RS) sirve para seleccionar el registro de datos (DR) o el de instrucciones (IR), poniendo RS=1 o RS=0, respectivamente. El pin 5 permite leer (R/W =1) o escribir (R/W = 0) en el módulo LCD tanto datos como instrucciones. Y por último, el pin 6 (E) permite habilitar, con E=1, o deshabilitar el display (E=0). Sólo cuando está habilitado nos podemos comunicar con él.

Ver apartado A.1.1 del anexo A para las temporizaciones de los procesos de escritura y lectura.

**Señales de datos**: Por último, los pines del 7 al 14 forman un bus de datos bidireccional de 8 bits (DB7 – DB0) por donde se pueden escribir datos e instrucciones y se puede leer el estado del display (si está o no ocupado, la posición actual del cursor, etc.). El LCD también puede ser gobernado con un bus de datos de 4 bits (utilizando el nibble más significativo).

### 3.2.2 Teclado matricial

La configuración e introducción de contraseñas en el módulo de control de acceso se realiza a través de un teclado matricial. Este es un simple arreglo de botones conectados en filas y columnas, de modo que se pueden leer 16 teclas utilizando solamente 8 pines de un microcontrolador. Se utilizará un teclado matricial de membrana 4x4 como se ve en la figura 3.4.



Figura 3.4 Teclado de membrana 4x4

El funcionamiento es sencillo y similar a lo que se realiza para multiplexar leds o displays de 7 segmentos. Se debe configurar 8 pines digitales del microcontrolador de la siguiente forma: RB4 a RB7 funcionan como salidas y RB0 a RB3 como entradas. Las filas del teclado matricial se conectan a los bits más significativos que funcionan como salidas, mientras que las columnas se conectan a los bits menos significativos del puerto que funcionan como entradas con resistencias pull-down[[12]](#footnote-12), en la figura 3.5 muestra el diagrama esquemático del teclado matricial conectados a los pines de un microcontrolador, además muestra el tecla en reposo, sin teclas oprimidas.

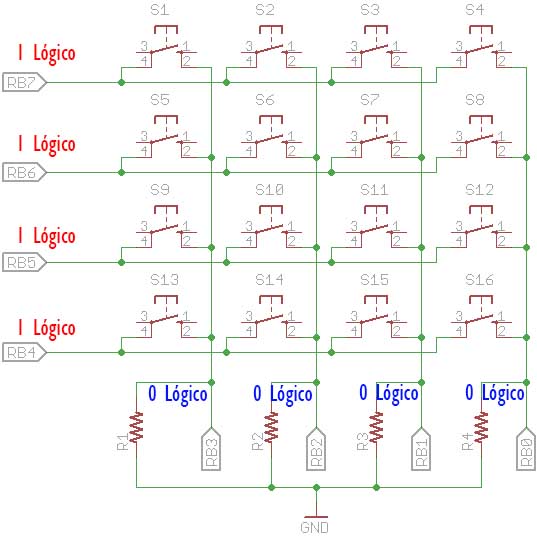


Figura 3.5 Diagrama del teclado matricial en reposo

Cuando se oprime una tecla la corriente fluye a través del switch y el voltaje de los pines conectados a las filas del teclado (5 V o 1 lógico) aparece ahora también en alguno de los pines RB0 a RB3 según la columna en la que se encuentra la tecla oprimida. La figura 3.6 ilustra lo que sucede al oprimir una tecla, al oprimir la tecla 6 se provoca un cambio en el PIN RB2 que ahora recibe un 1 o estado alto. Esto nos indica que se ha pulsado un botón en la segunda columna y se muestra como un nivel lógico alto en RB2.

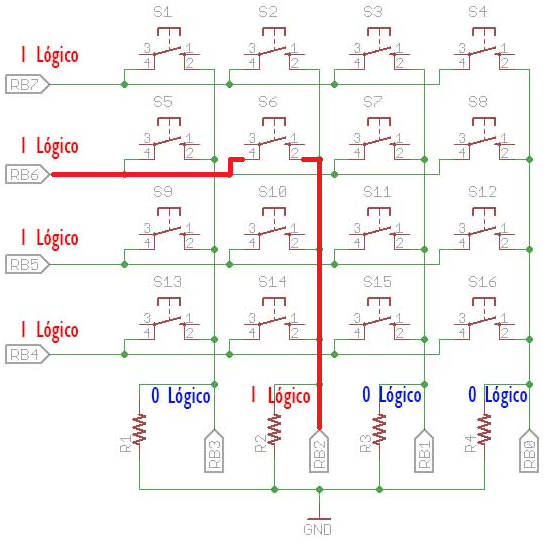


Figura 3.6 Diagrama del teclado matricial cuando la tecla 6 es presionada

Esta es la forma del microcontrolador detectar que se ha oprimida una tecla en alguna columna, dependiendo del bit activo RB3 a RB0, pero aún no se reconoce en cual fila fue presionada la tecla, para esto debemos realizar un proceso de escaneo del teclado, colocaremos en secuencia un 1 lógico (estado alto) en los 4 bits más significativos del puerto y leeremos el estado de los 4 bits menos significativos.

El microcontrolador escanea en forma sucesiva los pines de salidas, mientras lee las entradas en la parte baja del puerto, de manera que puede detectar que teclas están oprimidas en cada fila.

### 3.2.3 Módulo RFID MFRC522

Uno de los medios de identificación de usuarios es a por medio de etiquetas RFID, en el capítulo 2 se expuso las principales características de la tecnología RFID.

El Módulo Lector RFID MFRC522 está basado en un circuito integrado que realiza la lectura y escritura de información a través de radio frecuencia. Utiliza un sistema avanzado de modulación y demodulación para todo tipo de dispositivos pasivos de 13.56Mhz, tiene una distancia de lectura de etiquetas de un par de centímetros, en la figura 3.7 se observa el módulo MFRC522.



Figura 3.7 Módulo MFRC522

Este módulo tiene un voltaje de alimentación de 3.3V y posee un cristal de cuarzo de 27.12 MHz. Se puede controlar a través de los protocolos; SPI[[13]](#footnote-13), I2C[[14]](#footnote-14) o UART, por lo que es compatible con la mayoría de los microcontroladores.

En este proyecto se utilizara el protocolo SPI para la comunicación con el microcontrolador. En la figura 3.8 se presenta los pines del módulo MFRC522.

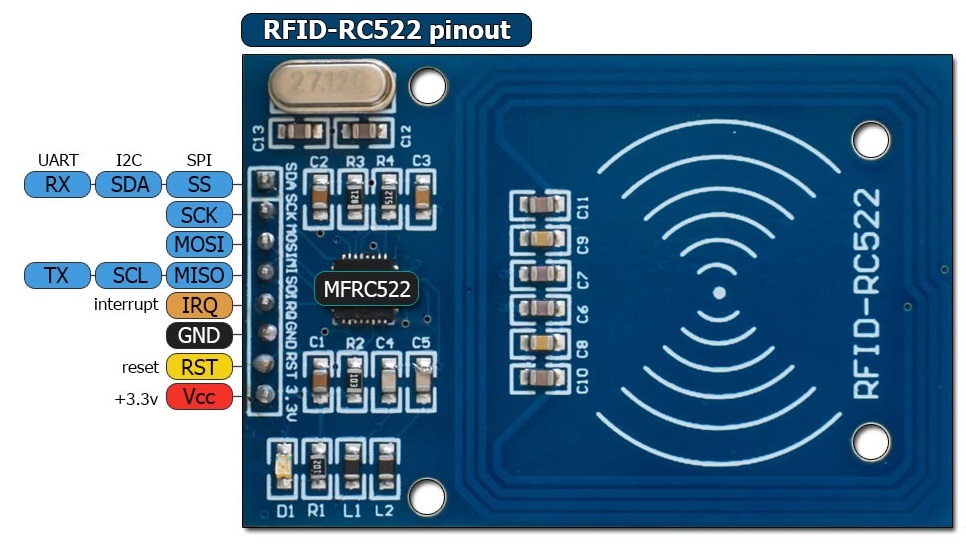


Figura 3.8 Pines de control y alimentación del MFRC522

El protocolo SPI permite una alta velocidad de comunicación con el microcontrolador, puede manejar velocidades de datos hasta 10 Mbit/s, cuando el MFRC522 actúa como esclavo, recibe datos desde el microcontrolador para la configuración de los registros, envío y recepción de datos relevantes para la interfaz. En el apartado A.2.1 del anexo A se entrega las características de sincronización.

El MFRC522 actúa como esclavo durante la comunicación SPI. La señal de reloj SPI SCK debe ser generada por el maestro. La comunicación de datos desde el maestro al esclavo utiliza la línea MOSI. La línea MISO se utiliza para enviar datos desde el MFRC522 al maestro.

Los bytes de datos en las líneas MOSI y MISO se envían primero con el bit más significativo o MSB (Most Significant Bit). Los datos de las líneas MOSI y MISO deben ser estables en el flanco ascendente del reloj y se pueden cambiar en el borde descendente. Los datos son proporcionados por el MFRC522 en el borde de reloj descendente y son estables durante el flanco ascendente del reloj. En el apartado A.2.2 del anexo A se exponen la configuración de bytes para los procesos de lectura y escritura por SPI.

### 3.2.4 Sensor biométrico

El control por huella digital es una de las principales características de este proyecto, el sensor biométrico de huellas dactilares permite a los usuarios registrar e identificar su huella dactilar como medio de acceso, en el capítulo 2 se expuso en detalle el funcionamiento de esta tecnología y los tipos de sensores más populares.

En este proyecto se usara el módulo óptico de las series ZFM-20 (ver figura 3.9), son módulos separados de identificación de huellas dactilares, propuestos por Hangzhou Zhian Technologies Co., Ltd., que toma un chip DSP[[15]](#footnote-15) como el procesador principal y el sensor óptico. El módulo realiza una serie de funciones como la huella digital Matriculación, procesamiento de imágenes, emparejamiento de huellas digitales, almacenamiento de plantillas y almacenamiento de imágenes. Es compatible con cualquier microcontrolador o sistema con comunicación serial TTL[[16]](#footnote-16), envía paquetes de datos para tomar fotos, detectar impresiones, hash[[17]](#footnote-17) y búsqueda. Tiene la capacidad de inscribir nuevos datos directamente, hasta 162 impresiones digitales se pueden almacenar en la memoria FLASH integrada.



Figura 3.9 Módulo ZFM-20 series.

El módulo de huellas dactilares es pequeños y fácil de montar, se comunica con el microcontrolador usando el protocolo de comunicación en serie. El conector de la tarjeta tiene cuatro pines: Vin, GND, Rx y Tx. En la figura 3.10 se observa la identificación de los pines.

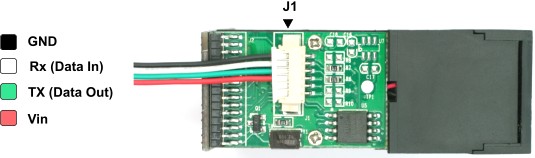


Figura 3.10 Vista trasera del módulo de huella dactilar.

Este módulo hace todo el trabajo pesado detrás de la lectura y la identificación de las huellas dactilares con un sensor óptico integrado y su CPU de 32-bit. La configuración de este módulo es sencilla solo se debe enviar simples comandos.

El procesamiento de huellas dactilares incluye dos partes: inscripción de huellas digitales y emparejamiento de huellas digitales (la coincidencia puede ser 1: 1 o 1: N). Al inscribirse, el usuario debe ingresar el dedo dos veces. El sistema procesará las dos imágenes de los dedos, generará una plantilla del dedo basándose en los resultados del procesamiento y almacenará la plantilla.

Al coincidir, el usuario introduce el dedo a través del sensor óptico y el sistema generará una plantilla del dedo y la comparará con las plantillas de la biblioteca de dedos.

Para la comparación 1:1, el sistema comparará el dedo ingresado con la plantilla específica almacenada en el módulo, para 1: N que coincida, o que busca, el sistema buscará la biblioteca entera del dedo para el dedo que coincida. En ambas circunstancias, el sistema devolverá el resultado coincidente, el éxito o el fracaso.

En el apartado A.3.1 del anexo 3 muestra el protocolo de comunicación y los paquetes de datos.

El escáner de huellas dactilares puede almacenar hasta 162 huellas digitales diferentes y la base de datos incluso se puede descargar de la unidad y distribuirse a otros módulos. En la tabla 3.2 se observan las principales características de este sensor.

Tabla 3.2 Característica módulo ZFM-20.

|  |  |
| --- | --- |
| **Supply voltage** | 3.6 - 6.0VDC |
| **Operating current** | 120mA max |
| **Peak current** | 150mA max |
| **Fingerprint imaging time** | <1.0 seconds |
| **Window area** | 14mm x 18mm |
| **Signature file** | 256 bytes |
| **Template file** | 512 bytes |
| **Storage capacity** | 162 templates |
| **Safety ratings** | 1-5 low to high safety |
| **False Acceptance Rate** | <0.001% (Security level 3) |
| **False Reject Rate** | <1.0% (Security level 3) |
| **Interface** | TTL Serial |
| **Baud rate** | 9600, 19200, 28800, 38400, 57600 (default is 57600) |
| **Working temperature rating** | -20C to +50C |
| **Working humidy** | 40%-85% RH |
| **Weight** | 20 grams |

### 3.2.5 Microcontrolador

El microcontrolador es un circuito integrado que en su interior contiene una unidad central de procesamiento (CPU), unidades de memoria (RAM y ROM), puertos de entrada y salida y periféricos. Estas partes están conectadas entre sí y en conjunto forman lo que se le conoce como microcontrolador.

El microcontrolador es el dispositivo encargado de gobernar todos los componentes y dispositivos electrónicos asociados al módulo electrónico de control de acceso, se ha elegido una placa Arduino Mega2560, está basado en el microcontrolador ATmega2560, cuenta con 54 pines digitales de entrada / salida, 16 entradas analógicas, 4 puertos UART, un oscilador de cristal de 16 MHz, tiene un conector USB para comunicarse con otro dispositivos, en tabla 3.3 se observan las especificaciones técnicas del microcontrolador.

Tabla 3.3 Especificaciones técnicas Arduino Mega2560

|  |  |
| --- | --- |
| Microcontrolador | Atmega2560 |
| Voltaje de operación | 5V |
| Voltaje alimentación | 7 – 12V |
| Pines de entrada/salida digitales | 54 |
| Pines de entrada análoga | 16 |
| Corriente dc por pin de entrada/salida | 20mA |
| Memoria flash | 256 KB |
| SRAM | 8 KB |
| Velocidad de reloj | 16 Mhz |
| Dimensiones | 101.52 x 53.3 mm |
| Peso | 37g |

Se verifica que la placa de arduino mega es compatible para el desarrollo del módulo electrónico de control de acceso, tiene un voltaje de operación de 5V al iguales que los otros dispositivos, cuenta con la cantidad de pines necesarios para conectar los componentes anteriormente vistos y con los protocolos de comunicación compatibles, en el apartado A.4 del anexo A se observa el arduino mega y su disponibilidad de pines.

A continuación se describe los pines que necesita cada componente:

* **Display LCD:** el display requiere de 7 pines digitales. En la tabla 3.4 se observa la asignación de pines del arduino Mega para el display LCD:

Tabla 3.4 Pines del display LCD

|  |  |  |
| --- | --- | --- |
| **N° pin LCD** | **Símbolo** | **Pin arduino Mega2560** |
| 4 | RS | D13 |
| 6 | E | D12 |
| 11-14 | D4-D7 | D4, D5, D6, D7 |
| 15 | A | D3 |

* **Teclado matricial:** Este utiliza 8 pines digitales se designaran los pines del A0 al A7 respectivamente.
* **MFRC522:** El microcontrolador tiene pines específicos para la comunicación SPI, los pines D51, D50 y D52 del arduino corresponde a MOSI, MISO y SCK respectivamente, y el pin SS está conectado al pin D2.
* **Sensor biométrico:** Este sensor usa el protocolo de comunicación UART, el microcontrolador usará los pines D10 y D11 del arduino para la comunicación serial.
* **Led RGB:** Este tipo de led utiliza 3 pines digitales, se designan los pines D14, D15 y D16 del arduino mega.

### 3.2.6 Led RGB

El led RGB[[18]](#footnote-18) es la unión de tres LEDs de los colores básicos, en un encapsulado común (ver figura 3.11), compartiendo el cátodo, en función de la tensión que se envié a cada pin se puede conseguir la mezcla del color deseado. Se usará este led para iluminar el módulo de control de acceso, cuando el acceso del usuario sea permitido, este brillará de color verde, el caso contrario brillará rojo.

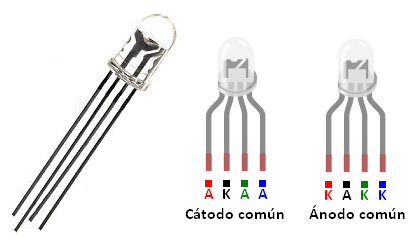


Figura 3.11 Led RGB

Para que este dispositivo funcione correctamente con el microcontrolador se tiene que utilizar una resistencia limitadora en serie para evitar que la excesiva corriente lo queme. En la figura 3.12 se representa el circuito esquemático del led para proceder a hacer el cálculo de la resistencia.



Figura 3.12 Circuito esquemático resistencia en serie con diodo led

La fórmula a aplicar es la tradicional ley de ohm en un circuito en serie presentada por la ecuación 3.1.

Ecuación 3.1

Donde:

*Rs*: Resistencia, en Ω;

*Vs*: Voltaje de entrada, en V;

*Vd*: Voltaje de operación del diodo, en V;

*Id*: Corriente de operación del diodo, en A

En la tabla 3.12 se observa las especificaciones técnicas del led RGB.

Figura 3.13 Especificaciones técnicas led RGB

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Color | Corriente [mA] | Vmin [V] | Vtyp [V] | Vmáx [V] |
| Rojo | 20 mA | 1.8 | 2.0 | 2.2 |
| Verde | 3.0 | 3.2 | 3.4 |
| Azul | 3.0 | 3.2 | 3.4 |

El voltaje de operación de los pines del microcontrolador son de 5V (*Vs*) con una corriente de 20mA, de la tabla anterior se observa que el led rojo tiene un voltaje de operación diferente a los otros dos, se debe hacer el caculo de la resistencia para cada uno de los led. Reemplazando los datos en la ecuación 3.1 se obtiene:

Ecuación 3.2

Ecuación 3.3

Ecuación 3.4

Ecuación 3.5

La resistencia del led rojo de ser de 180Ω y 100Ω para el led verde y azul.

### 3.2.6 Circuito módulo control de acceso

Es necesario integrar todos los componentes del módulo electrónico de control de acceso, para este se diseñara un circuito que cumpla esta función. El diseño del circuito impreso es realizado con el software EAGLE V.7.3, este nos permite diseña el circuito esquemático y el circuito impreso, en la figura 3.14 se observa el circuito esquemático del módulo de control de acceso que integra todos los componentes con el microcontrolador, en la figura se utilizan etiquetas para facilitar la lectura del esquemático.

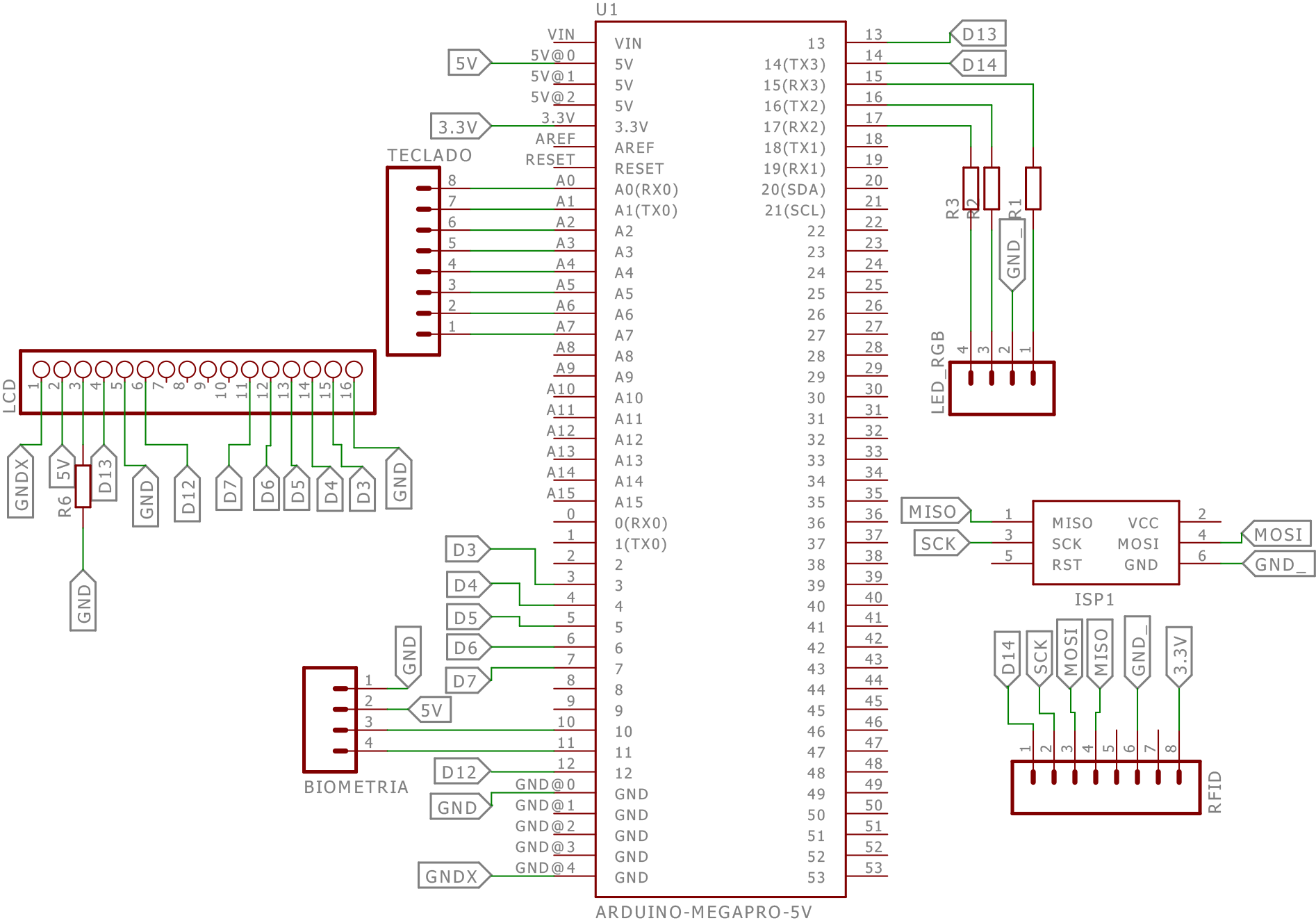


Figura 3.14 Circuito esquemático del módulo control de acceso.

En la figura 3.15 se observa la vista frontal de la placa de circuito impreso, esta es una placa que se monta en el arduino mega y tiene los conectores para cada componente.

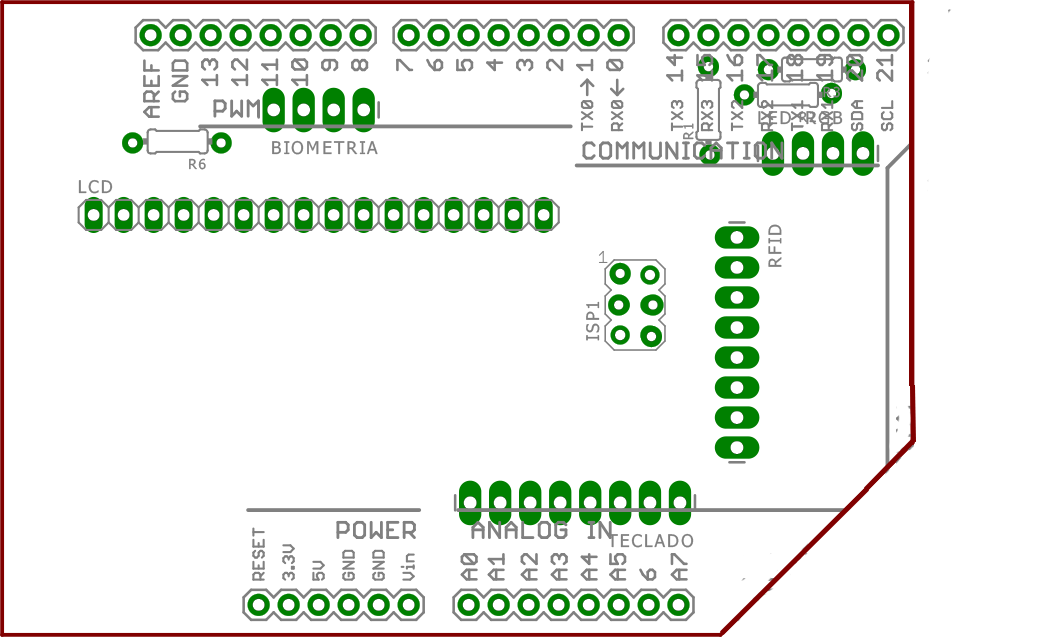


Figura 3.15 Vista frontal de la placa de circuito impreso del módulo de control de acceso

En la figura 3.16 se muestra la vista frontal del circuito impreso con las líneas de conexión correspondiente, esta figura es la que debe ser grabada en la placa de cobre.

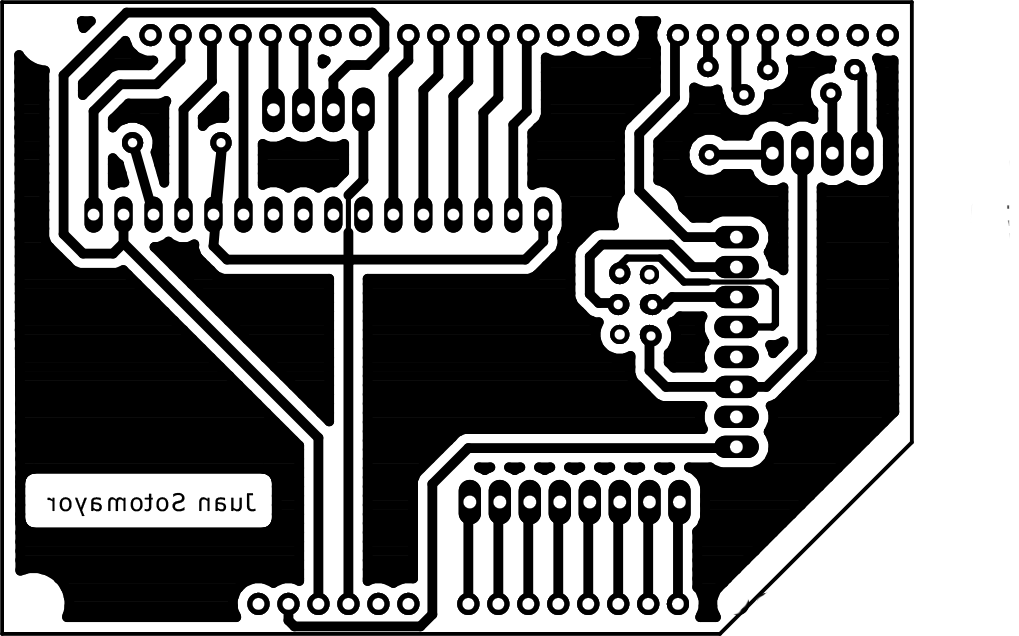


Figura 3.16 Vista frontal de la placa de circuito impreso con las líneas de conexión.

## 3.3 Raspberry Pi 3

La Raspberry Pi 3 es el computador de placa reducida que controlar el módulo de control de acceso y ejecuta la plataforma web. La Raspberry pi 3 está basada en un procesador multimedia Broadcom BCM2837, este contiene un procesador central ARMv8 de 64 bits con cuatro núcleos, trabaja a una velocidad de 1.2 [GHz], memoria RAM de 1 [GB], conectividad Bluetooth 4.1 y Wi-Fi 802.11n, salida HDMI, x4 puertos USB, interfaz GPIO de 40 PINS, puerto ethernet, jack audio de 3,5 mm, slot para tarjeta micro SD, VideoCore IV 3D graphics y una interfaz para cámara y pantalla externas. En la figura 3.17 se observa el hardware y algunas características de la Raspberry Pi 3.



Figura 3.17 Raspberry Pi 3

El puerto de alimentación de la Raspberry es un puerto micro USB, el voltaje debe ser de 5 [V] y una corriente de 2 [A].

La Raspberry Pi está diseñada para ejecutar un sistema operativo GNU/Linux. A diferencia de Windows u OS X, Linux es de código abierto. Esto quiere decir que es posible descargar el código fuente del sistema operativo por completo y hacer los cambios que uno desee. Esto nos permitirá crear la aplicación para el gerenciamiento del módulo de control de acceso y ejecutar a tiempo real la plataforma web.

La Raspberry Pi tiene 40 pines GPIO (General Purpose Input/Output), es un sistema de Entradas/Salidas de propósito general, este representa la interfaz entre la Raspberry Pi y el exterior. Se usaran estos pines para conectar el circuito que controlara el relé para activa el actuador de la puerta, estos pines trabajan a un nivel lógico de 3.3 [V] e corriente máxima de 50 [mA]. En la figura 3.18 se observa el esquema de pines GPIO de la Raspberry Pi.

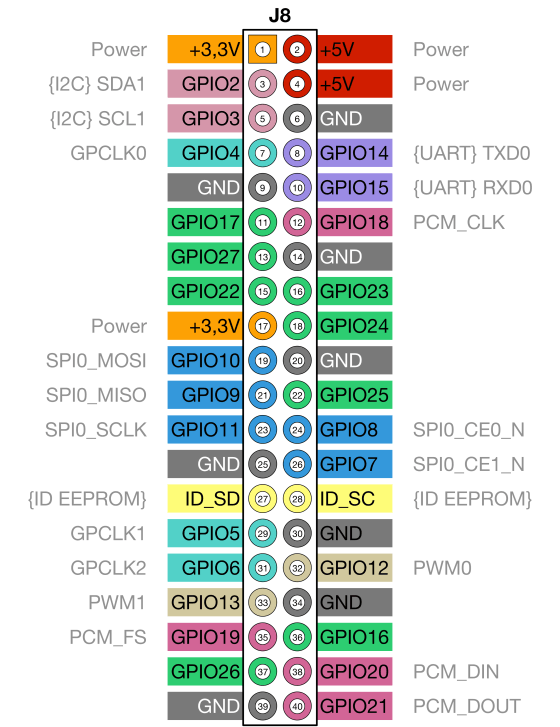


Figura 3.18 Esquema pines GPIO Raspberry Pi 3

## 3.4 Circuito de control

La función principal de este circuito es controlar el trabador electromagnético, además de regular la alimentación y llevar el tiempo para la Raspberry pi.

Este circuito tiene que tener un voltaje de entrada igual al necesario para activar el actuador de la puerta, este puede ser desde 12 [V] hasta 18 [V], luego pasará por una fase de regulación de tensión a 5 [V], para alimentar el resto de dispositivos del circuito y principalmente la Raspberry PI, se utilizará el módulo LM2596 convertidor de voltaje DC-DC Buck (ver figura 3.19). El voltaje permitido de entrada es de 4.5-40 [V] y un voltaje de salida de 1.5-35 [V], es capaz de conducir una corriente de hasta 3A. Maneja una carga con excelente regulación de línea y bajo voltaje de rizado. En el apartado A.5 del anexo A se expone el circuito esquemático y otras especificaciones.

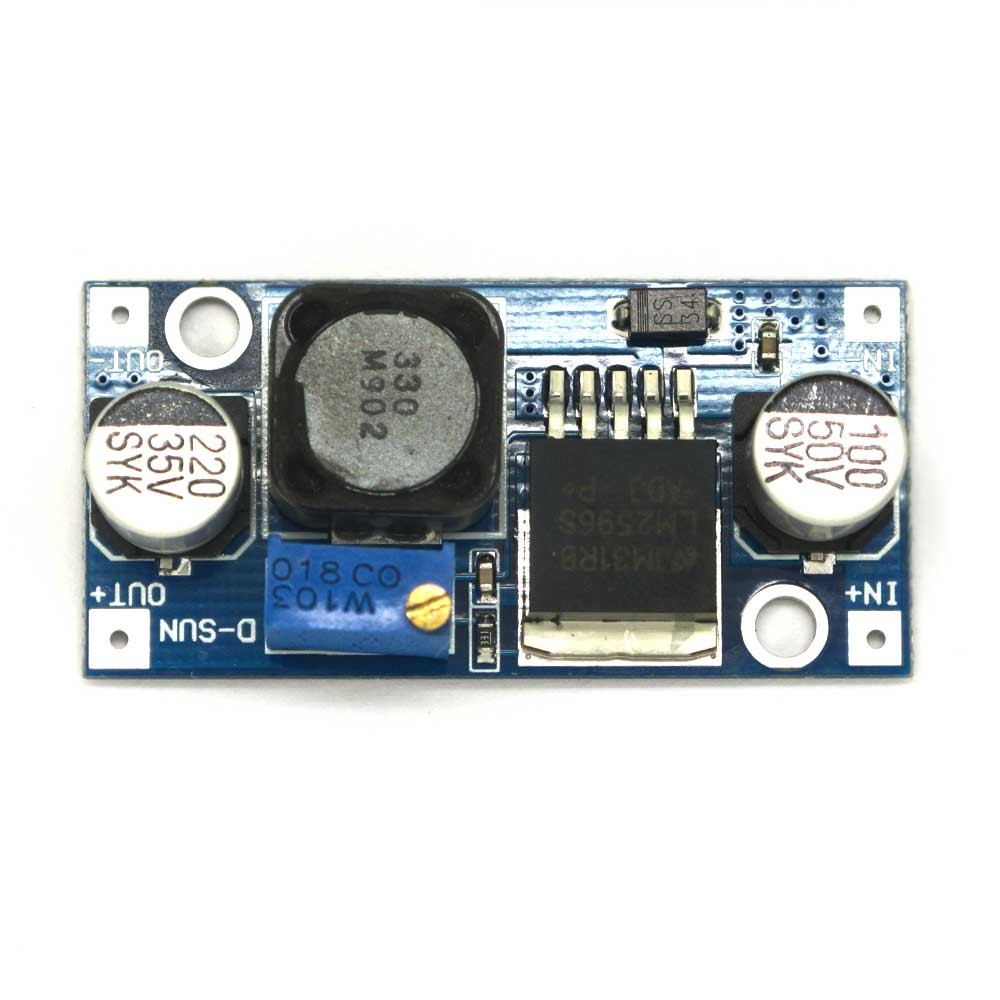


Figura 3.19 Módulo LM2596

El circuito de control integra un módulo de reloj de tiempo real, RTC, con basado en el circuito integrado DS1307, montado en un soporte de conexión, con un cristal de 32.768 [Hz], una batería de 3 [V] en el respaldo, utiliza el protocolo de comunicación I2c, el pin SDA y SCL van conectados con los pines GPIO2 y GPIO3 de la Raspberry respectivamente. En la figura 3.20 se observa el reloj de tiempo real DS1307.

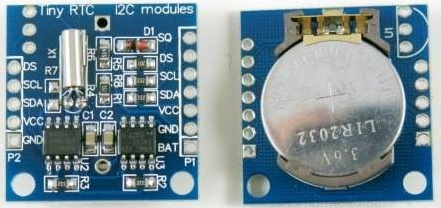


Figura 3.20 Reloj de tiempo real DS1307

Este reloj es utilizado para la Raspberry lleve el registro del tiempo de forma continua, es necesario que el registro de la información tenga el respaldo cronológico en que suceden las actividades.

El circuito de control debe activar un relé para cerrar el circuito del trabador electromagnético, este es activado a través de un pin GPIO de la Raspberry, El problema se encuentra que la corriente y voltaje que suministra el pin GPIO es insuficiente para activar el relé. Se propone utilizar un transistor que funcione como switch para controlar el relé. En la figura 3.21 se observa el circuito propuesto.

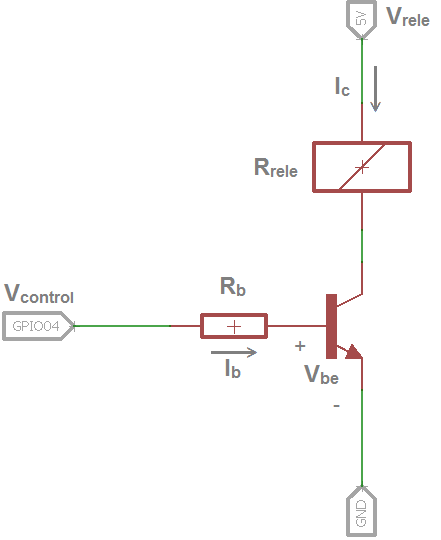


Figura 3.21 Circuito para activar un relé desde la salida de un controlador

El cálculo de la resistencia del circuito anterior está dado por la siguiente ecuación.

Ecuación 3.6

Dónde:

*Vrele:* Voltaje necesario para activar el relé.

*Rrele:* Resistencia interna del relé.

*β:* Ganancia de corriente del transistor.

*Vbe:* Voltaje entre base y emisor.

*Rb:* Resistencia para controlar la corriente que pasa por la base del transistor.

*Vcontrol:* Voltaje del pin de salida del GPIO.

Se propone utilizar el transistor bipolar BC548, este es un transistor del tipo NPN[[19]](#footnote-19) tiene una ganancia de corriente de 110 y un voltaje de saturación entre base y colector es de 0.7 [V]. Este transistor controlará el relé JQC-3F (T73), este tiene un voltaje de operación de 5 [V] y una resistencia de 60 [Ω], en el apartado A.6 del anexo A se exponen las especificaciones técnicas de estos componentes. El voltaje de operación de los pines GPIO de la Raspberry es de 3.3 [V], ahora que se conocen las todas las variables se procede a calcular la resistencia Rb desde la ecuación 3.6.

Ecuación 3.7

Ecuación 3.8

El valor de la resistencia que controla el transistor debe ser de 3.4 [KΩ], pero se aproximará a la resistencia comercial más próxima de 3.3 [KΩ], esta es conectada en el pin GPIO4 de la Raspberry Pi.

El circuito de control se montará sobre los pines GPIO de la Raspberry Pi, para esto se utilizará un pin header hembra 2x20, en la figura 3.22 se muestra el esquemático del circuito de control. Los puntos VIN, VOUT, SELENOIDE y BUTTON, corresponden a conectores de bloque dobles de 5mm, utilizados para conectar el voltaje de entrada del circuito, voltaje de salida para alimentar la Raspberry Pi, el trabador electromagnético y el botón respectivamente. Cuando se presiona el botón este cierra el circuito enviando una señal de 3.3 [V] para activar el transistor, el diodo D1 cumple la función de proteger el pin GPIO de corrientes inversas. JP1 al JP4 corresponden a los conectores del módulo regulador de voltaje que es montado sobre este circuito al igual que el RTC. Además se integraron dos diodos led, el LED1 se ilumina cuando el relé es activado y el LED2 se enciende cuando la placa se encuentra energizada.

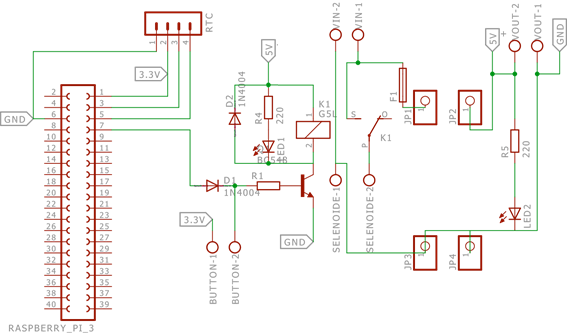


Figura 3.22 Esquemático circuito de control

En la figura 3.23 se observa la vista frontal de la placa de circuito de control, en esta se observa la integración de los componentes electrónicos y los espacio para conectar los módulos LM2596 y DS1307.

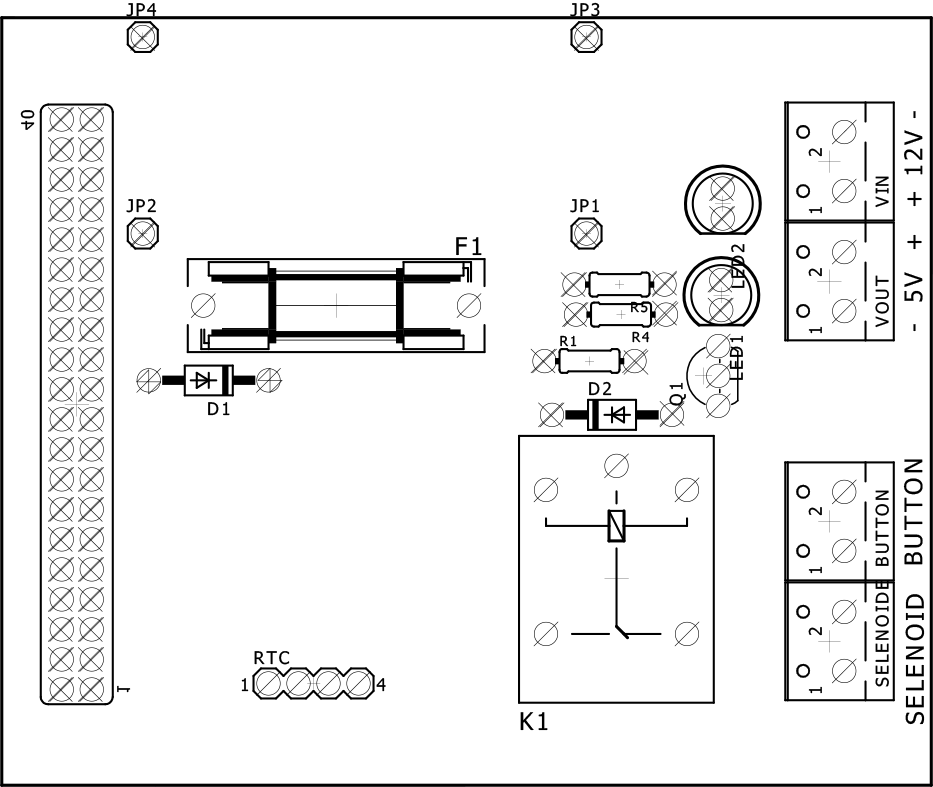


Figura 3.23 Vista frontal circuito de control

El diseño del circuito impreso del circuito de control se puede observar en la figura 3.24.

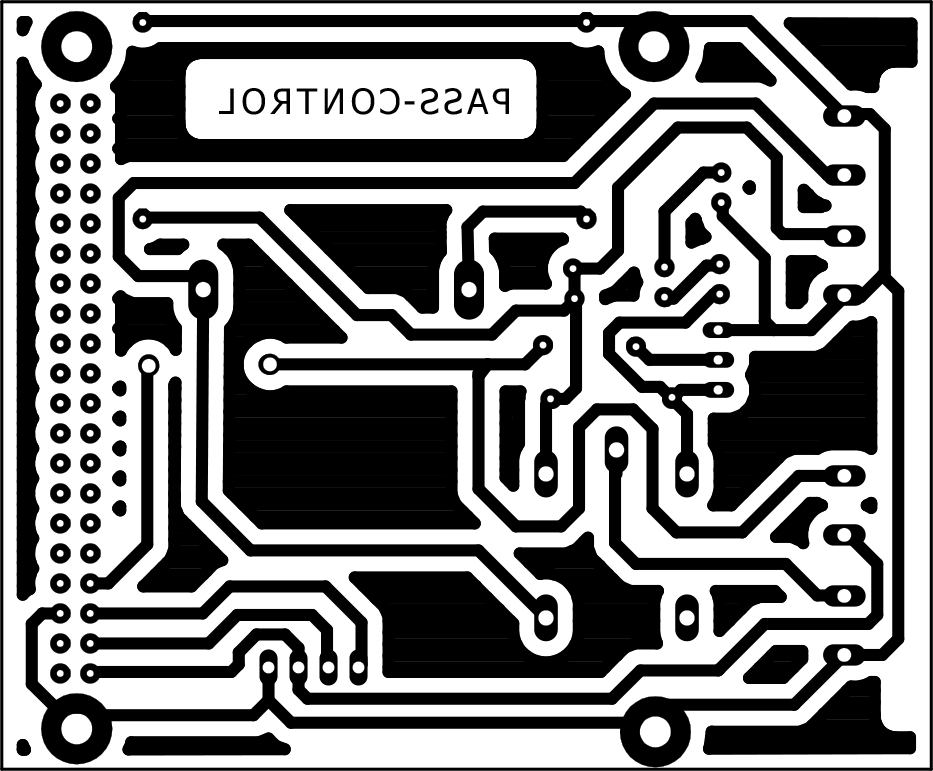


Figura 3.24 Circuito impreso

**CAPITÚLO**

# PROGRAMACIÓN HARDWARE Y PLATAFORMA WEB

En este capítulo se abarcará la programación del módulo de control de acceso, está se realiza a través del IDE[[20]](#footnote-20) Arduino. Además de la configuraciones necesarias para la Raspberry Pi, el desarrollo de la plataforma web y levantamiento de base de datos.

## 4.1 Programación módulo control de acceso

El microcontrolador integrado en el módulo de control de acceso ejecuta el programa que controla los sensores y la comunicación con la Raspberry Pi, esto se denomina código ejecutable y está compuesto por combinaciones binarias (bytes), este código es almacenado en su memoria flash. El programa debe ser estructurado con un inicio y fin perfectamente definidos, el diseño de los algoritmos de programación se realizan con diagramas de flujos, este nos facilita la visualización de los principales procesos, y con el uso de secuencias de instrucciones denominadas *pseudocódigo* nos facilita la escritura y lectura del programa.

En la figura 4.1 se expone el diseño del algoritmo del módulo de control de acceso, en este se logra visualizar que siempre tiene que verificar la comunicación con las Raspberry Pi, debido a que es esta quien gestiona la información del sistema, luego el módulo de control de acceso queda a la espera de la interacción de los usuarios, cuando esto sucede envía la información captada de estos a la Raspberry Pi, el módulo recibe la respuesta y la interpreta en el LCD para que los usuarios observen lo que está sucediendo.

Figura 4.1 Diagrama de flujo programación módulo de control de acceso

Cuando un usuario se identifica con una etiqueta RFID, el módulo toma la ID única de esta y la Raspberry Pi verifica en su base de datos si esa ID corresponde a un usuario registrado y si este tiene acceso permitido o denegado.

El sensor biométrico es quien procesa la información de las huellas digitales de los usuarios, además almacena las plantillas e imágenes. Cuando un usuario se identifica por este medio, el módulo busca en los registros del sensor si este usuario está almacenado, si la verificación es correcta, el módulo envía la ID\_BIOMETRIA a la Raspberry Pi quien verifica si este usuarios está registrado y el estado del acceso.

A través del teclado matricial los usuarios pueden identificarse para tener acceso a la instalación o también por este medio el administrador puede ingresar al menú para agregar los medios de identificación de los usuarios registrado en la plataforma previamente.

En la figura 4.2 se observa el proceso que debe realizar el administrador para agregar nuevos usuarios, en este menú el administrador puede presionar la tecla 1 para agregar un medio de identificación del usuario, la tecla 0 para volver al proceso inicial o en caso que se demore más de 12 segundos en interactuar con el módulo, en el caso que se presione la tecla 1 se solicitará ingresar el número serial de 9 dígitos generado por la plataforma web al momento de registrar al usuario, luego el módulo envía este serial a la Raspberry Pi para la verificación, cuando es verificado el módulo da la opción para agregar el medio de identificación del usuario, se debe presionar la tecla 1 para agregar identificación por biometría, la tecla 2 para identificación por RFID o la tecla 0 para volver al menú de administrador nuevamente.



Figura 4.2 Menú de administrador para agregar usuarios

El caso de agregar un usuario por biometría, este debe situar el dedo índice derecho en el lector biométrico, este verifica si las lectura coinciden con las de otro usuarios, de manera de verificar que este usuario no tenga registrada su huella dactilar, luego el sensor almacena en su memorias las plantillas e imágenes obtenidas, generando una ID\_BIOMETRIA única para el usuario, se envía esta ID para la Raspberry Pi, en donde verifica que el usuario no tenga registrada una huella existente, esto debido a que el sistema permitirá almacenar una huella dactilar por usuario, posterior a la verificación el módulo mostrará en su pantalla durante un corto tiempo la respuesta recibida (Usuario biométrico adicionado o Usuario existente), al finalizar este proceso se regresa al menú del administrador.

El proceso anterior se puede visualizar en la figura 4.3, por otra parte, se tiene la función para agregar el usuario por RFID, el usuarios debe aproximar la etiqueta RFID al lector del módulo, este espera durante 12 segundos la interacción del usuario, esto aplica también al proceso anterior. El lector RFID recibe la ID única de la etiqueta y se la envía a la Raspberry Pi, recordando que esta quien procesa y almacena la información de los usuarios, recibida la ID verifica en el registro de usuarios que esta no exista, verificando que esa etiqueta no esté siendo utilizada por otra persona, además de verifica que el usuario no tenga una etiqueta RFID ya designada, en el caso que se desee modificar dicha información se debe realizar a través de la plataforma web previamente, posterior a todas las acciones el usuarios visualiza en el LCD lo que está sucediendo.



Figura 4.3 Procesos para agregar usuarios por biometría y RFID

Ahora que se tienen definidos los principales procesos del algoritmo del módulo de control de acceso, se debe escribir la programación del microcontrolador encargado de ejecutar las acciones de los procesos, para esto se utilizará el IDE de Arduino, quien depura y compila la programación al microcontrolador, el lenguaje de programación se basa C++, aunque es posible programarlos en otros lenguajes.

Los códigos de programación del sistema de control de acceso se encuentran de forma digital adjunto a este documento ya sea en CD, pendrive o por correo electrónico, debido a que las programaciones son demasiados extensas para incluirlas en los anexos de este documento. El directorio principal del proyecto se llama “cpass”, al interior del directorio se encuentran 3 carpetas; Arduino, Node y Plataforma web. Dentro de la carpeta “Arduino” se encuentran todas las programaciones correspondientes al microcontrolador del módulo de control de acceso, el archivo principal se llama “cpass-tesis.pde”, la extensión “.pde” está asociado con Processing Development Environment (PDE), ejecutable con el software de Arduino , compatible con Windows, Mac Os X y Linux. De otra forma para la visualización de los códigos se puede utilizar un editor de texto.

La programación del microcontrolador incluye librerías desarrolladas por terceros para facilitar la programación, estas integran diferentes funciones que se pueden utilizar para el cumplimiento de los procesos. Luego de incluir las librerías necesarias, se definen las diferentes viables que se utilizarán a los largo de la programación, algunas de estas variables están relacionadas a la configuración de los pines de entrada y salida del microcontrolador, la programación en arduino involucra dos funciones principales la primera es ***void setup(){...}***, en esta los códigos que se encuentren en su interior de ejecutan por una sola vez y al momento de encender el microcontrolador, la segunda función es ***void loop(){...}***, esta función ejecuta los códigos de forma secuencial y cíclica, por lo que al interior se encuentran los códigos o funciones encargadas de cumplir con la funcionalidad del módulo de control de acceso.

El módulo de control de acceso se comunica con la Raspberry Pi a través del protocolo de comunicación UART o también conocido como serial. La información que se transmite es una cadena de caracteres o también conocidas como *String*, ejemplo “RFID-ADMIN-1-BC DF 87 07”, se utiliza este formato de texto para la interpretación de la información que se desea transmitir, tanto el microcontrolador como la Raspberry pi, al recibir esta información separan las instrucciones por medio de un guion y son almacenadas al interior de un Array[[21]](#footnote-21), el array del ejemplo mencionado del string quedaría de la siguiente forma:

Data[] = {‘RFID’, ‘ADMIN’, ‘, ‘BC DF 87 07’, ‘1’};

En donde:

Data[0] = ‘RFID’;

Data[1] = ‘ADMIN’;

Data[2] = ‘457854789’;

Data[3] = ‘BC DF 87 07’’;

Data[4] = ‘1’;

El ejemplo anterior corresponde al string que envía el módulo de control de acceso a la Raspberry Pi, luego que el lector RFID identifica la etiqueta para agrega un usuario, la forma que se interpreta el mensaje es a través de operadores lógicos, en este caso se utiliza ‘if’, ‘else if’ y ‘else’, en la figura 4.4 se muestra como la Raspberry utiliza estos operadores y ejecuta funciones para realizar las acciones.

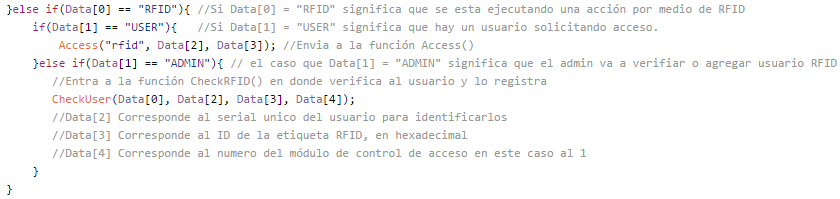


Figura 4.4 Ejemplo operadores lógicos para la interpretación de los mensajes

## 4.2 Configuración y programación Raspberry Pi

# BIBLIOGRAFÍA

[ 1 ] OSCAR TORRENTE ATEROS. Arduino curso práctico de formación, primera edición, Alfaomega Grupo Editor, S.A. de C.V., México

[ 2 ] EBEN UPTON, Raspberry PI 200 ejercicios prácticos, primera edición, Multímedia, 2013.

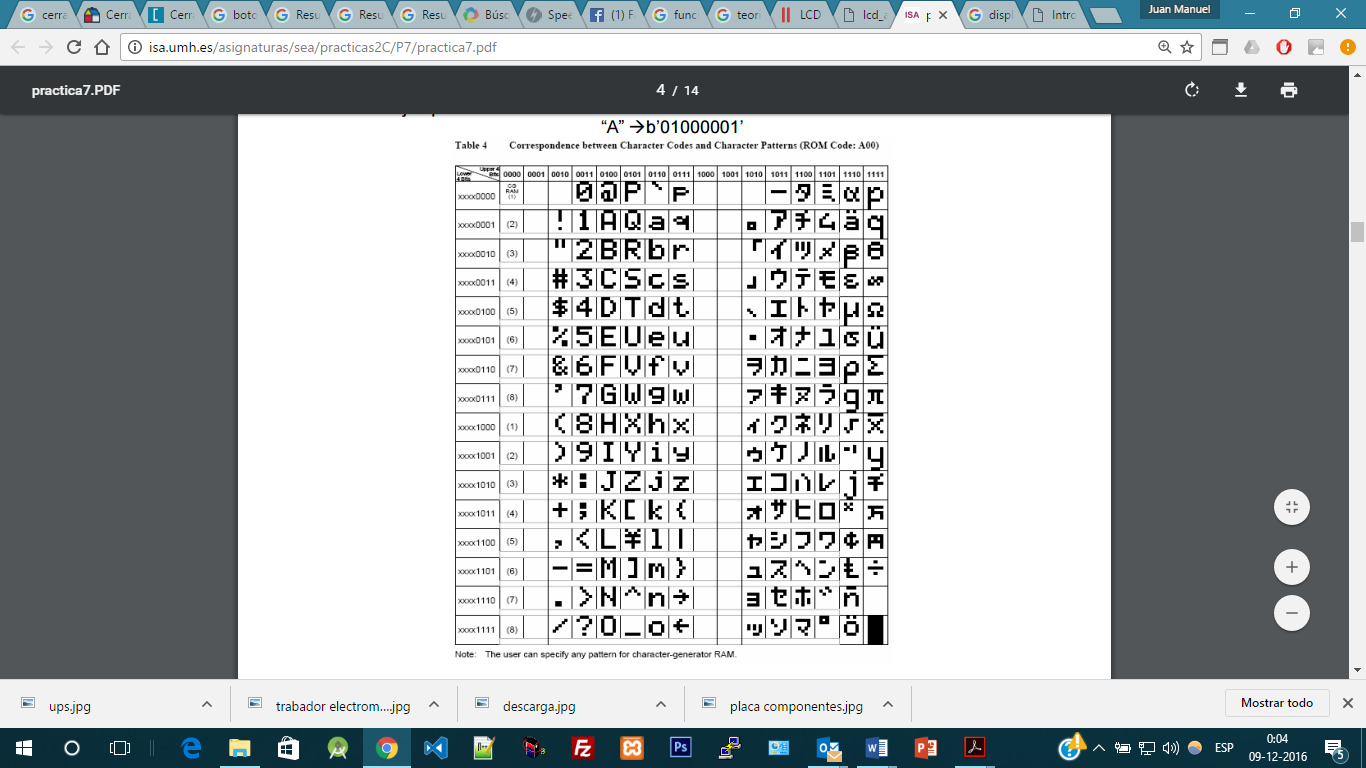
[ 3 ] J. ORTEGA; F. ALONSO; R. COOMONTE, Biometría y seguridad, primera edición, Universidad Autónoma de Madrid, 2008.

# **ANEXO A**

# DATOS TÉCNICOS DE DISPOSITIVOS Y COMPONENTES

## A.1 Display LCD

Tabla A.1 Representación binaria de caracteres



### A.1.1 Consideraciones sobre las operaciones de lectura y escritura

Para que las instrucciones lleguen correctamente al controlador del display se debe respetar la secuencia de activación de las señales así como los tiempos mínimos y máximos expresados por el fabricante.

En primer lugar se ha de partir con la señal ENABLE (E) a nivel bajo. En esta situación se activan las señales RS y R/W a sus valores correspondientes (R/W a cero para la escritura, o a uno para la lectura) y tras dejar pasar un tiempo tAS (tiempo de establecimiento de la dirección), se pone E en alto. Tras este flanco ascendente en E se nos pueden presentar dos casos: escritura o lectura.

**Escritura:** Si estamos en una escritura, tras el flanco ascendente de E enviamos el dato al bus de datos (DB[0..7]) y debemos dejarlo puesto un tiempo mínimo tDSW (tiempo de establecimiento de los datos en escritura). Posteriormente ponemos E a nivel bajo, pero antes de bajar hay que asegurarse de que haya estado en alto por lo menos un tiempo PWEH (ancho del pulso de habilitación en alto). El flanco de bajada en E hace que se cargue la instrucción en el interior del controlador HD44780, pero para ello hay que mantener activas las señales de datos durante un tiempo tH (tiempo de mantenimiento de los datos) y las señales RS y R/W un tiempo mínimo tAH (tiempo de mantenimiento de la dirección).

**Lectura:** Si estamos en una lectura, tras el flanco ascendente de E debemos esperar un tiempo mínimo tDDR (tiempo de retardo de los datos) antes de leer el dato del bus de datos (DB[0..7]). Posteriormente ponemos E a nivel bajo, tras asegurarse de que haya estado en alto por lo menos un tiempo PWEH (ancho del pulso de habilitación en alto). El flanco ascendente de E ha hecho que el controlador HD44780 haya entregado el dato en el bus, y tras el flanco descendente de E mantendrá los datos un tiempo mínimo tDHR (tiempo de mantenimiento de los datos en la lectura). Las señales RS y R/W las podremos desactivar tras pasar un tiempo mínimo tAH (tiempo de mantenimiento de la dirección) desde el flanco descendente de E. Tanto en lectura como en escritura, el tiempo mínimo entre dos flancos ascendentes en la señal E es tcycE (tiempo de ciclo de habilitación).

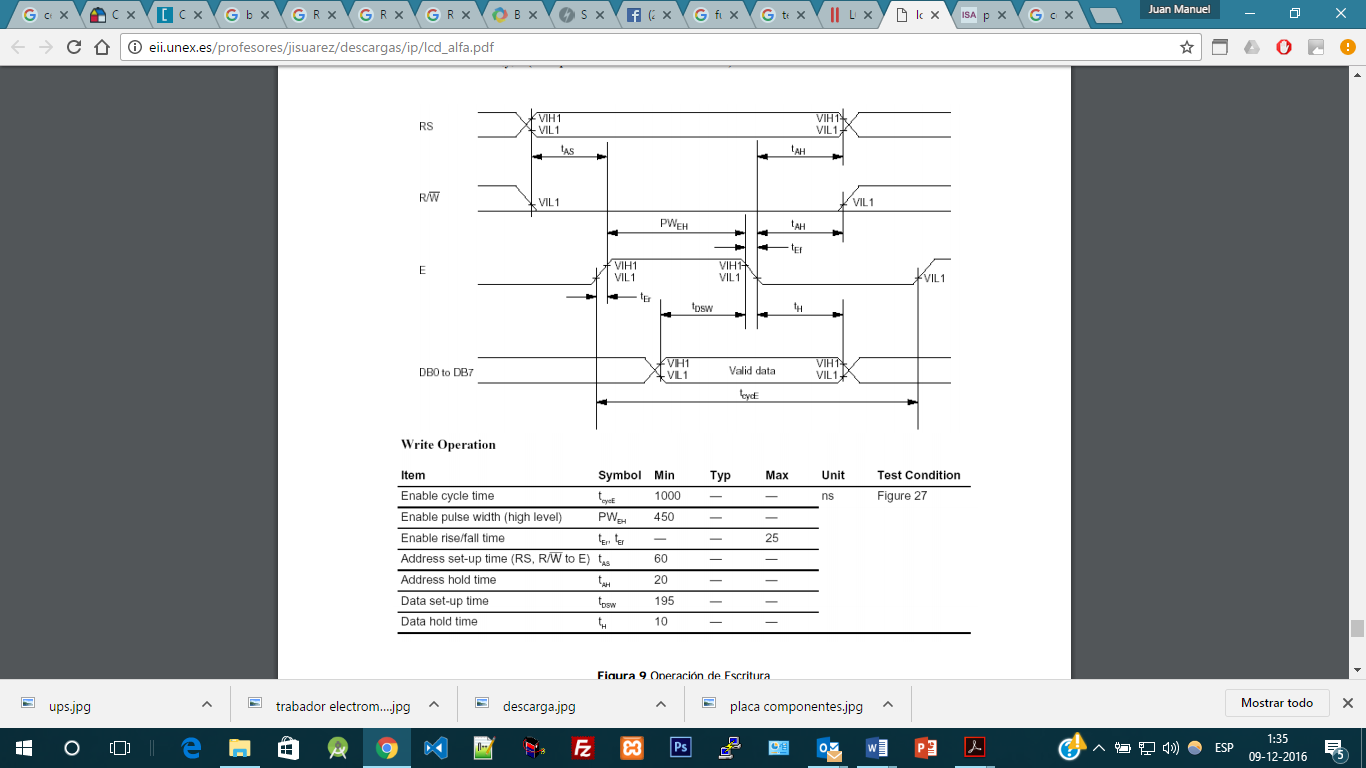


Figura A.1 Operación de escritura

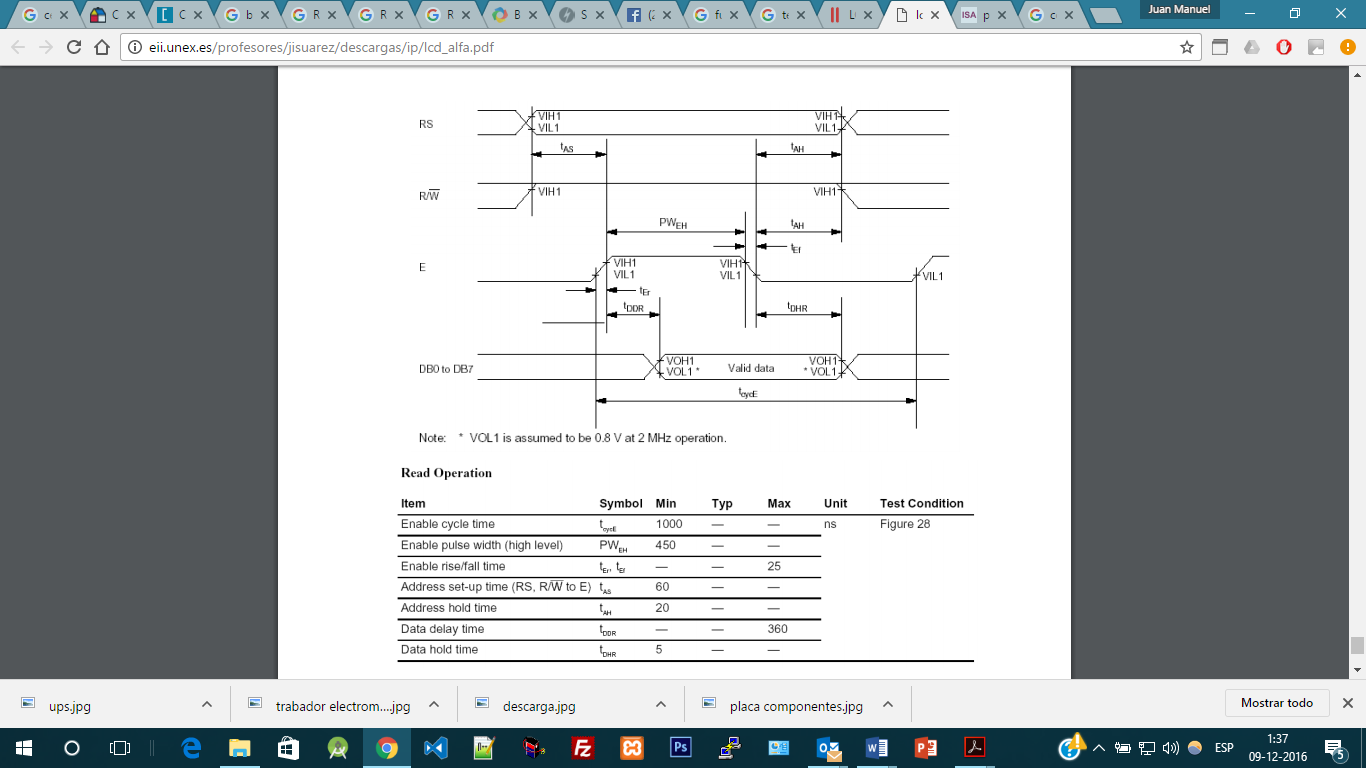


Figura A.2 Operación de lectura

## A.2 MFRC522

### A.2.1 Características de sincronización

Tabla A.2 SPI características de sincronización

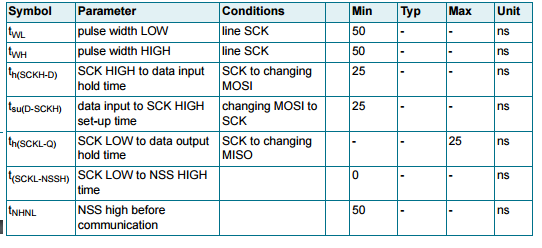




Figura A.3 Diagrama de sincronización SPI

### A.2.2 Configuración de bytes para lectura y escritura SPI

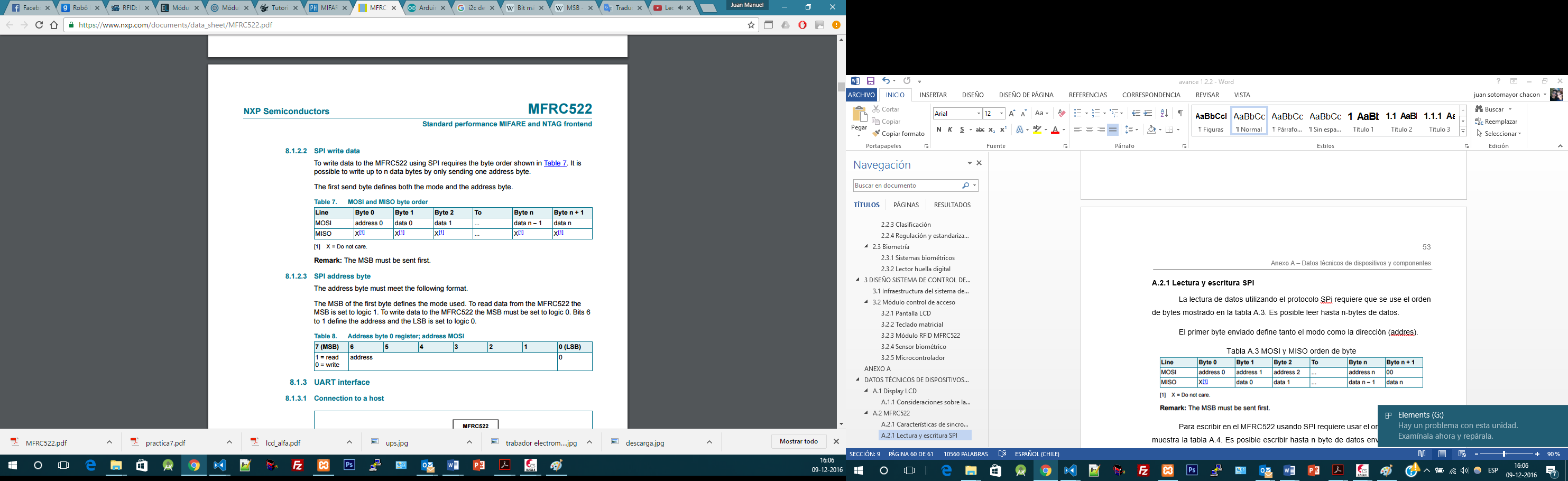
La lectura de datos utilizando el protocolo SPi requiere que se use el orden de bytes mostrado en la tabla A.3. Es posible leer hasta n-bytes de datos. El primer byte enviado define tanto el modo como la dirección (addres).

Tabla A.3 MOSI y MISO orden de byte para la lectura



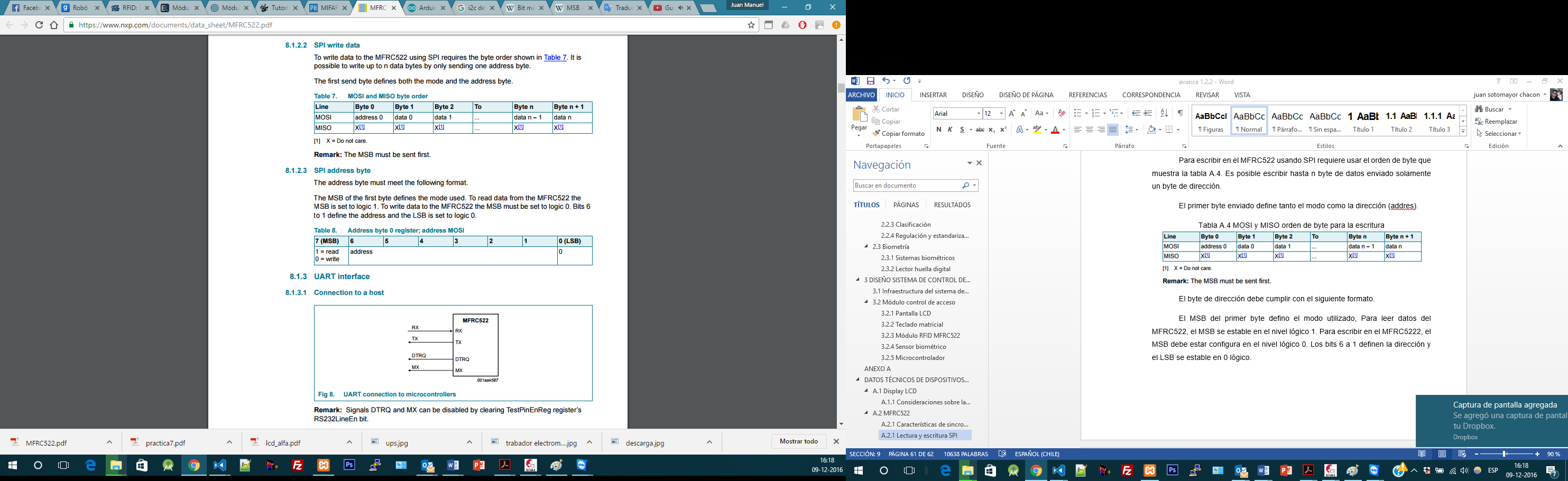
Para escribir en el MFRC522 usando SPI requiere usar el orden de byte que muestra la tabla A.4. Es posible escribir hasta n byte de datos enviado solamente un byte de dirección. El primer byte enviado define tanto el modo como la dirección (addres).

Tabla A.4 MOSI y MISO orden de byte para la escritura



El byte de dirección debe cumplir con el siguiente formato. El MSB del primer byte define el modo utilizado, Para leer datos se estable en el nivel lógico 1 y para escribir en el nivel lógico 0. Los bits 6 a 1 definen la dirección y el LSB se estable en 0 lógico.

Tabla A.5 Byte de dirección MOSI.



## A.3 ZFM-20

### A.3.1 Protocolo de comunicación

El protocolo define el formato de intercambio de datos cuando el ZFM-20 se comunica con el ordenador superior. El protocolo de comunicación por los cuales envía la instrucciones pueden ser UART y USB, el interfaz del USB se recomienda encarecidamente para mejorar la velocidad que intercambia, especialmente en dispositivo de la exploración de la huella digital.

Al comunicarse, la transferencia y recepción de comando / datos / resultado están envueltos en formato de paquete de datos.

Tabla A.6 Formato de paquete de datos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Header** | **Adder** | **Package**  **Identifier** | **Package**  **Lenght** | **Package content**  **(instuction/data/Parameter)** | **Checksum** |

Tabla A.7 Definiciones del paquete de datos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Name** | **Length** | **Description** | |
| Header | Start | 2 bytes | Fixed value of EF01H; High byte transferred first. | |
| Adder | ADDER | 4 bytes | Default value is 0xFFFFFFFF, which can be modified by  command. High byte transferred first and at wrong adder value,  module will reject to transfer. | |
| Package  identifier | PID | 1 byte | 01H | Command packet; |
| 02H | Data packet; Data packet shall not appear alone in executing processs, must follow command packet or acknowledge packet. |
| 07H | Acknowledge packet. |
| 08H | End of Data packet. |
| Package  length | LENGTH | 2 bytes | Refers to the length of package content (command packets and  data packets) plus the length of Checksum( 2 bytes). Unit is  byte. Max length is 256 bytes. And high byte is transferred first. | |
| Package  contents | DATA | - | It can be commands, data, command¡ s parameters,  acknowledge result, etc. (fingerprint character value, template  are all deemed as data); | |
| Checksum | SUM | 2 bytes | The arithmetic sum of package identifier, package length and  all package contens. Overflowing bits are omitted. high byte is  transferred first. | |

## A.4 Arduino Mega 2560

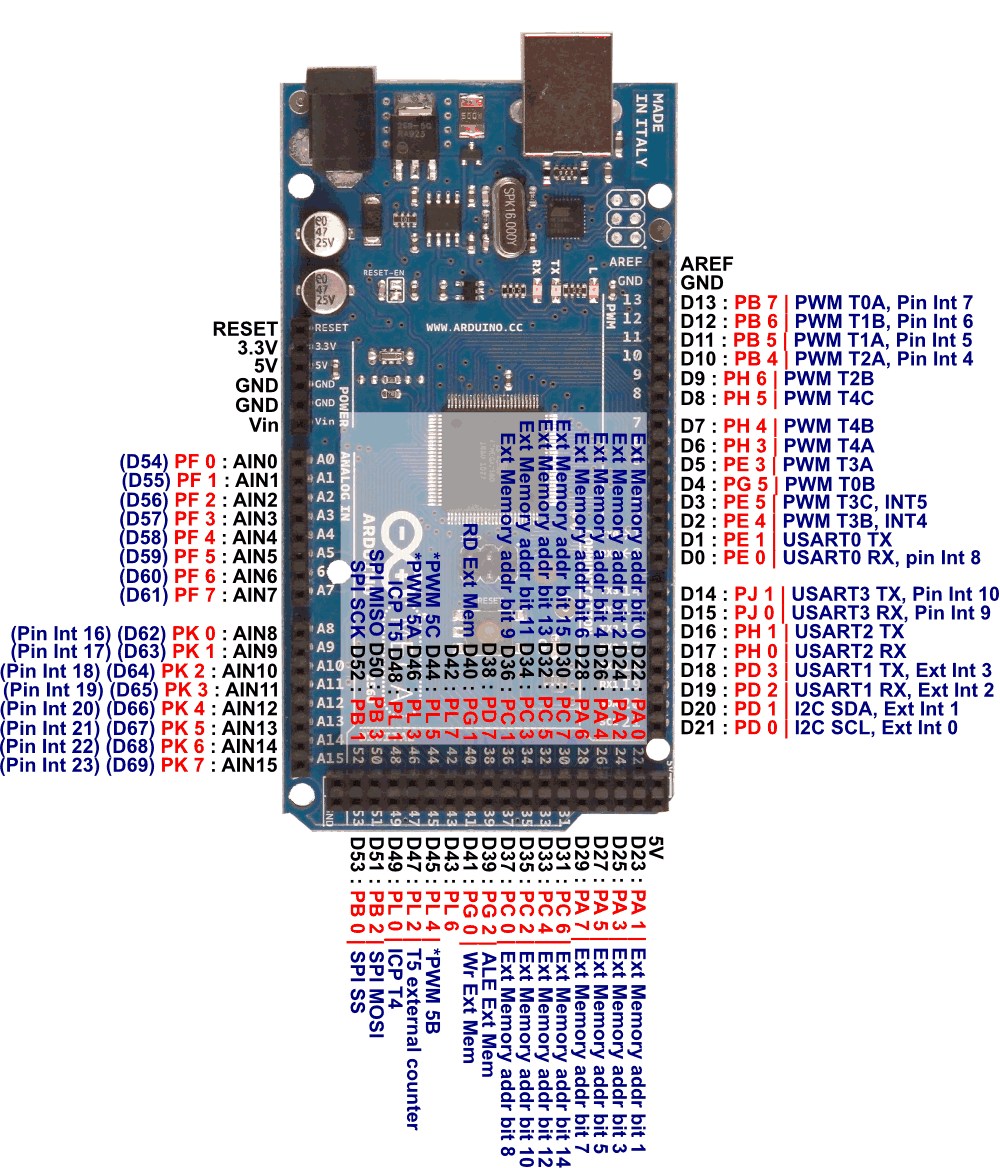
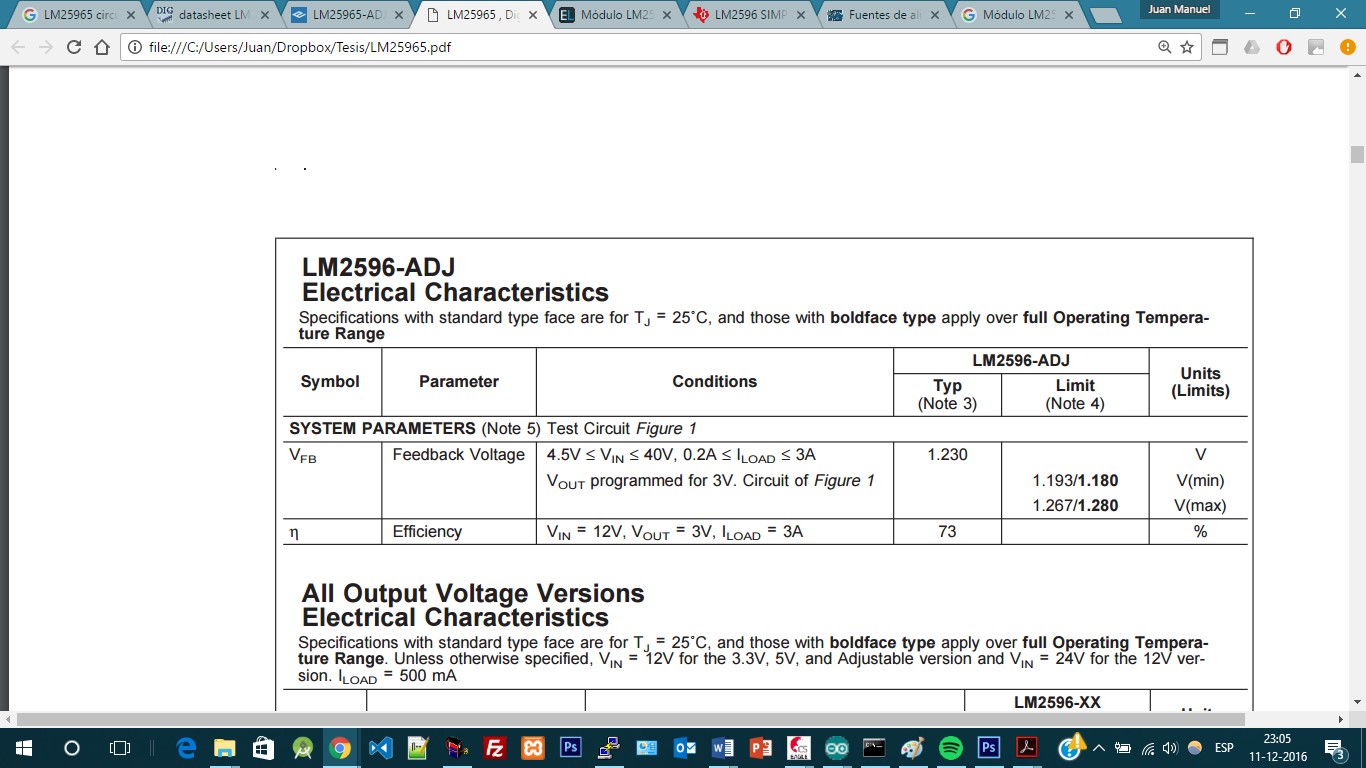


Figura A.4 Arduino Mega y disponibilidad de pines

## A.5 Módulo LM2596

En la tabla A.8 se observan las condiciones de funcionamiento del módulo.

Tabla A.8 Especificaciones eléctricas módulo LM2596



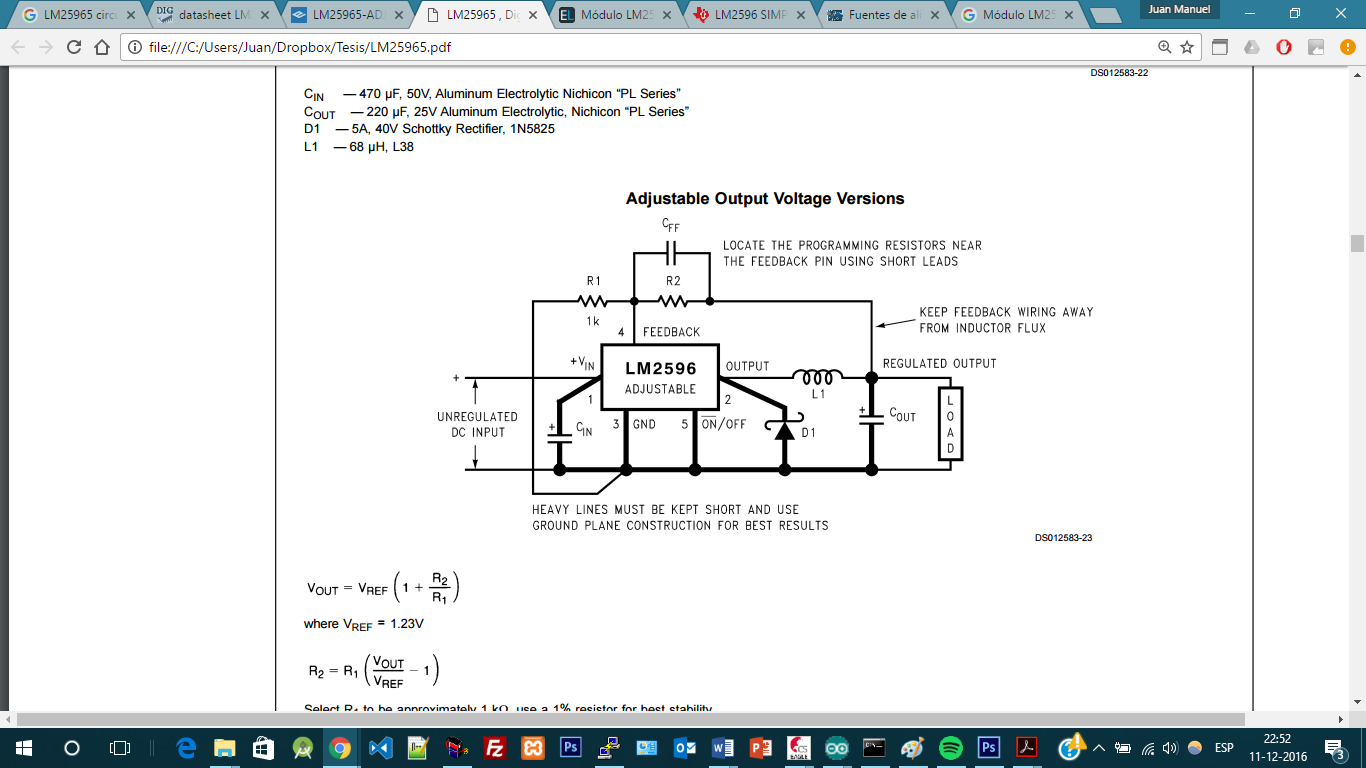


Figura A.5 Circuito módulo LM2596

Ecuación A.1

Donde *VREF* = 1.23 [V]

Ecuación A.2

Seleccionar R1  próximo a 1 [KΩ] y con una tolerancia de 1% para mejor estabilidad.

## A.6 Transistor BC548

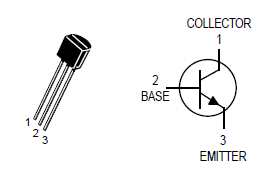


Figura A.6 Circuito módulo LM2596

Tabla A.9 Especificaciones eléctricas transistor BC548

|  |  |  |  |
| --- | --- | --- | --- |
| Descripción | Símbolo | Valor | Unidad |
| Voltaje colector-emisor | VCEO | 30 | Vdc |
| Voltaje colector-base | VCBO | 30 | Vdc |
| Voltaje emisor-base | VEBO | 6.0 | Vdc |
| Corriente colector | IC | 100 | mAdc |
| Voltaje saturación base-emisor | VBE(sat) | 0.7 | Vdc |
| Ganancia de corriente | β | 110 | - |

## A.7 Relé

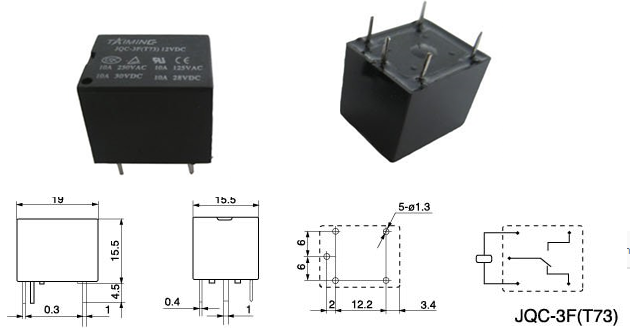


Figura A.7 Relé JQC-3F(T73)

Tabla A.10 Especificaciones eléctricas relé

|  |  |
| --- | --- |
| Descripción | Valor |
| Voltaje de operación | 5 [V] |
| Resistencia entre contactos | 60 [Ω] |
| Voltaje DC max en la bobina | 24 [V] |
| Corriente DC max en la bobina | 5 [A] |
| Voltaje AC max en la bobina | 250 [V] |
| Corriente AC max en la bobina | 10 [A] |

1. Es una red que conecta los ordenadores en un área relativamente pequeña. [↑](#footnote-ref-1)
2. Es una red de gran cobertura en la cual pueden transmitirse datos a larga distancia. [↑](#footnote-ref-2)
3. Circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria. [↑](#footnote-ref-3)
4. Enrollment, en la bibliografía inglesa. [↑](#footnote-ref-4)
5. En inglés, Sample. [↑](#footnote-ref-5)
6. En inglés, Identification register. [↑](#footnote-ref-6)
7. En inglés, Feature set. [↑](#footnote-ref-7)
8. En inglés, Template. [↑](#footnote-ref-8)
9. En inglés, smart cards. [↑](#footnote-ref-9)
10. **ROM** (acrónimo en inglés de ***read-only memory***), es un medio de almacenamiento utilizado en ordenadores y dispositivos electrónicos, que permite sólo la lectura de la información y no su escritura. [↑](#footnote-ref-10)
11. **RAM** (acrónimo en inglés de ***Random Access Memory***), Memoria principal de la computadora, donde residen programas y datos, sobre la que se pueden efectuar operaciones de lectura y escritura. [↑](#footnote-ref-11)
12. La resistencia de pull-down hace que la entrada lógica sea cero mientras éste está en reposo (LOW). [↑](#footnote-ref-12)
13. SPI, del inglés Serial Peripheral Interface, es un estándar de comunicaciones, usado para la transferencia de información entre circuitos integrados en equipos electrónicos. [↑](#footnote-ref-13)
14. I2C, del inglés Inter Integrated Circuito, es un bus de datos para múltiples dispositivos. [↑](#footnote-ref-14)
15. DSP, del inglés de Digital Signal Processor, es un sistema basado en un procesador o microprocesador que posee un conjunto de instrucciones, un hardware y un software optimizado. [↑](#footnote-ref-15)
16. TTL, del inglés Transistor-Transistor Logic. [↑](#footnote-ref-16)
17. Un Hash se utiliza en lo que se llaman funciones hash criptográficas o funciones unidireccionales en el área de la criptografía. [↑](#footnote-ref-17)
18. RGB, sigla en inglés de red, green, blue, en español rojo, verde y azul. [↑](#footnote-ref-18)
19. NPN es uno de los tipos de transistores bipolares, la letra “N” se refiere a negativo y la “P” a positivo, esto significa que la corriente entra por el colector y sale por el emisor. [↑](#footnote-ref-19)
20. Entorno de Desarrollo Integrado (IDE), es un entorno de programación que ha sido empaquetado como un programa de aplicación, consiste en un editor de código, un compilador y un depurador. [↑](#footnote-ref-20)
21. Un Array es una estructura de datos que nos permite almacenar una gran cantidad de datos de un mismo tipo. [↑](#footnote-ref-21)