ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES

"DISEÑO DE UN PROTOTIPO DE CERRADURA ELECTRÓNICA CONECTADA A UNA RED WIFI Y CONTROLADA MEDIANTE UNA APLICACIÓN MÓVIL, PARA EL CONTROL AUTOMÁTICO DE LAS PUERTAS DE LOS LABORATORIOS DEL EDIFICIO DE LA FIE."

TRABAJO DE TITULACIÓN: DISPOSITIVO TECNOLÓGICO

Para optar al Grado Académico de:

INGENIERO EN ELECTRÓNICA, CONTROL Y REDES INDUSTRIALES

AUTORES: CUENCA SARANGO CLAUDIO SEBASTIAN

MANOTOA JORDÁN ALEX JAVIER

TUTOR: ING. HENRY ERNESTO VALLEJO VIZUETE

Riobamba – Ecuador
2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES

El Tribunal del Trabajo de Titulación certifica que: El trabajo de titulación: "DISEÑO DE UN PROTOTIPO DE CERRADURA ELECTRÓNICA CONECTADA A UNA RED WIFI, Y CONTROLADA MEDIANTE UNA APLICACIÓN MÓVIL PARA EL CONTROL AUTOMÁTICO DE LAS PUERTAS DE LOS LABORATORIOS DEL EDIFICIO DE LA FIE", de responsabilidad de los señores, CLAUDIO SEBASTIÁN CUENCA SARANGO Y ALEX JAVIER MANOTOA JORDÁN, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
Ing. Washington Gilberto Luna E. **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA.**	**……...**	**…….**
Ing. Freddy Chávez V. **DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES.**	**……...**	**…….**
Ing. Henry Ernesto Vallejo V. **DIRECTOR DEL TRABAJO DE TITULACIÓN**	**……...**	**…….**
Dr. Hugo Moreno A. **MIEMBRO DEL TRIBUNAL**	**……...**	**…….**

Nosotros, Claudio Sebastián Cuenca Sarango y Alex Javier Manotoa Jordán, somos responsables de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación, y el patrimonio intelectual de la misma pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Claudio Sebastián Cuenca Sarango
Alex Javier Manotoa Jordán

DEDICATORIA

Dedico este trabajo de titulación al creador de todas las cosas, dándome la vida, fortaleza y sabiduría, con el único fin de saber afrontar cada difícil situación que se ha presentado en mi vida, por ello, en primero lugar dedico mi trabajo a Dios.

Dedico de igual manera este trabajo a dos personas muy importantes que han sido los pilares fundamentales para llegar a donde estoy, mis padres: Víctor Cuenca y Lucía Sarango, quienes, me han visto crecer cada día y que, con su ejemplo, con sus enseñanzas, los valores, y palabras de aliento que me han brindado, han logrado de mí, ser un hombre de bien y que a lo largo de mi vida, me han sabido guiar para ser una mejor persona que puede aportar un pequeño granito de arena en todo este basto mundo.

A mis hermanos Mario, Alonso, Santiago, Jimena que me han dado todo su apoyo incondicional, su amabilidad, depositando en mí su esperanza, a ellos, que me inspiran a conseguir grandes cosas, a quienes admiro y sobre todo respeto mucho.

A mi familia en general, por los buenos y malos momentos, de los cuales quedarán recuerdos y enseñanzas maravillosas.

Y a los amigos que nunca faltan, con ocurrencias, bromas y demás, han convertido los días grises, en alegres e inolvidables.

Sebastian

El presente trabajo de titulación lo dedico a Dios, por darme la vida, el conocimiento y permitirme llegar a este momento tan especial de mi vida.

A mis padres EMILIO MANOTOA y GUADALUPE JORDÁN quienes siempre me brindaron su apoyo incondicional, quienes creyeron en mí, encontrando en mi madre todo su cariño y consejos que me brido durante toda mi vida académica, a mi padre ejemplo de superación y constancia personal. A mi hermano por apoyarme en cada momento, y en especial a mi tía Celinda que ha sido un pilar fundamental en este trayecto, por esta razón este triunfo es para ustedes por ser mi motivación de superación.

Alex

AGRADECIMIENTO

Nuestro más sincero agradecimiento a la Escuela Superior Politécnica de Chimborazo por abrirnos las puertas en esta Institución Educativa, en especial a la Facultad de Informática y Electrónica por permitirnos formar ingenieros Electrónicos en Control y Redes Industriales. A los docentes de la Facultad quienes con sus conocimientos, enseñanzas y sabiduría han logrado encaminarnos para llegar a ser grandes profesionales.

A nuestras familias, por su apoyo incondicional y su infinito amor en todo este largo y arduo trayecto, han estado siempre ahí, para nosotros.

Y a todas y cada una de las personas que nos han permitido culminar este trabajo de titulación y cumplir nuestros objetivos.

Sebastián

Alex

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

INDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

INDICE DE ECUACIONES

ÍNDICE DE ABREVIATURAS

ADSL	Asymmetric Digital Subscriber Line
AES	Estándar de Encriptación Avanzada
AP	Punto de Acceso
DC	Corriente Directa
DHCP	Protocolo de Configuración Dinámica de Host
HTML	HyperText Markup Language
HZ	Hercios
IDE	Entorno de Desarrollo Integrado
IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
IoT	Internet de las cosas
JSON	JavaScript Object Notation
LAN	Red de Área Local
LUA	Lenguaje de programación Estructurado
mA	Miliamperio
MAC	Media Access Control
Mbps	Megabit por Segundo
Mm	Milímetro
OS	Sistema Operativo
OSI	Interconexión de Sistemas Abiertos
PCB	Placa de Circuito Impreso
RSA	Rivest, Shamir y Adleman
RTC	Reloj en tiempo real
SCL	Serial Clock
SD	Secure Digital

SDA	Serial Data
SDK	Kit de Desarrollo de Software
SPI	Interfáz Periférica Serial
SSID	Service Set Identifier
TCP/IP	Protocolo de Control de Transmisión/ protocolo de Internet
URL	Uniform Resource Locator
USB	Bus Universal en Serie
UTP	Par trenzado no Blindado
WAN	Red de Área Amplia
WLAN	Red de Área Local Inalámbrica

ÍNDICE DE ANEXOS

RESUMEN

El objetivo de la investigación fue diseñar un prototipo de cerradura electrónica conectada a una red WiFi y controlada mediante una aplicación móvil, para el control automático de las puertas de los laboratorios del Edificio de la Facultad de Informática y Electrónica (FIE) de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Mediante métodos de experimentación y observación, se desarrolló un sistema de control de acceso electrónico. Se compone de mecanismos diseñados, que permiten abrir y/o cerrar una puerta de forma automática utilizando la placa de desarrollo NodeMCU como dispositivo de control y comunicación WiFi. Cuenta con un sistema de protección en el envío y recepción de información mediante el algoritmo de cifrado AES-128 bits. La aplicación móvil que maneja el usuario se desarrolló en el software Android Studio. Además, el sistema cuenta con el servicio de Google de base de datos en tiempo real Firebase, que permite la autenticación de usuarios en la aplicación. El prototipo dispone de sistemas de contingencia; ante cortes eléctricos, una batería de 12V a 7Ah y para fallas de comunicación inalámbrica, se dispone de un sistema de control de acceso con tecnología de comunicación de campo cercano (NFC). Por los resultados obtenidos, por medio de un software de captura de tráfico de red, se verificó que existe el correcto cifrado de mensajes al enviar o recibir información entre interfaces, garantizando un sistema seguro inalámbricamente. El sistema de respaldo de energía dura aproximadamente tres horas a plena carga, y en estado de reposo, un tiempo de 58 horas. El prototipo creado podrá reducir el tiempo de acceso de estudiantes y docentes para el uso de los laboratorios y, convertirse en un elemento funcional y moderno de bajo costo que puede complementarse con otros dispositivos. Se recomienda asignar al dispositivo una dirección IP fija dentro de la red, para enviar peticiones desde la aplicación móvil.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>**,** <TECNOLOGÍA DE CONTROL AUTOMÁTICO>, <DOMÓTICA>, <COMUNICACIONES INALÁMBRICAS>, <NODEMCU (HARDWARE)>, <BASE DE DATOS FIREBASE>, <COMUNICACIÓN DE CAMPO CERCANO (NFC)>, <ENCRIPTACIÓN ESTÁNDAR AVANZADA (AES)>.

ABSTRACT

The aim of the research was to design an electronic lock prototype connected to a wifi network and controlled through a mobile application, for the automatic control of the doors in the laboratories of the Faculty of Computer Science and Electronics (FIE) building at Escuela Superior Politécnica de Chimborazo (ESPOCH). Using methods of experimentation and observation, a system of electronic access control was developed. It is made up of designed mechanisms, that allow you to open and / or close a door automatically using the development board NodeMCU as control device and wireless communication. It has a system of protection in the sending and receiving of information through the encryption algorithm AES-128. The mobile application that handles the user was developed in the Android software. Also, the system has the service of Google real-time database (Firebase) that enables the authentication of users in the application. The prototype has contingency systems against electrical outages, a battery from 12V to 7ª, for wireless communication failures, there is an access control system with Near Field Communication (NFC). From the results obtained, by means of a software to capture network traffic, it was verified that there is a correct encryption of messages to send and receive information between interfaces, ensuring a secure system wirelessly. The system power backup works approximately three hours at full load, and in a state of rest, 58 hours. The prototype created may reduce the access time of students and teachers for the use of laboratories, and become a modern and functional element of low cost that can be supplemented with other devices. It is recommended to assign a fixed IP address to the device within the network, to send requests from the mobile application.

KEYWORDS: <TECHNOLOGY AND ENGINEERING SCIENCE>, <AUTOMATIC CONTROL TECHNOLOGY>, <AUTOMATION>, <WIRELESS COMMUNICATIONS>, <NODEMCU (HARDWARE)>, <DATA BASE FIREBASE>, <NEAR FIELD COMMUNICATION (NFC) >, <ADVANCED STANDARD ENCRYPTION (AES)>.

INTRODUCCIÓN

En un mundo en donde la tecnología avanza a pasos agigantados cada día, y la necesidad de tener conectados entre sí gran parte de los dispositivos electrónicos compartiendo información significativa. Aparece como parte de un ecosistema tecnológico, el medio de comunicación denominado, *internet de las cosas (IoT),* conjuntamente con el desarrollo de las aplicaciones que usan todos los dispositivos móviles, permitiendo hacer más fácil la vida cotidiana y además contando con toda la seguridad necesaria para proteger los datos personales ante ataques informáticos.

Sin duda, los sistemas de control de acceso también han ido evolucionando, debido a que son los principales instrumentos que sirven para bloquear o dar acceso a personas al interior de edificaciones. Estos sistemas en su mayoría son aún manuales, es decir se necesita insertar la llave físicamente dentro de la cerradura para que el mecanismo interno funcione, lo cual es incómodo cuando se encuentra en zonas lejanas.

En la Escuela Superior Politécnica de Chimborazo, en la Facultad de Informática y Electrónica, se encuentran instaladas cerraduras de tipo tubular en las puertas de los laboratorios. Para lo cual se ve en la necesidad del desarrollo de un proyecto que pretende mejorar este tipo de sistemas mecánicos mediante el complemento de sistemas electrónicos para que realicen estos procesos de apertura o cierre de forma automática, ahorrando una considerable cantidad de tiempo y facilitando su control de forma remota.

En el presente documento, se detalla la parte teórica que permite un mejor entendimiento de conceptos fundamentales, seguido de la construcción y elementos necesarios para el desarrollo del prototipo electrónico que tiene como objetivo crear un sistema de control de acceso innovador y seguro.

Finalmente, se exponen los resultados obtenidos luego de la implementación y verificación del funcionamiento del dispositivo que, sin duda, puede servir como un complemento eficaz y de bajo costo dentro del mundo de la domótica como de la inmótica.

ANTECEDENTES

Desde la antigüedad, el hombre sintió aquella necesidad de protegerse del medio exterior, por ello solía cerrar con una enorme piedra la entrada de su caverna. De esta forma sentía más seguridad en el lugar donde vivía. Al aumentar sus pertenencias, también aumentó el riesgo de que intrusos llegaran a su hogar. El rudimentario sistema de seguridad de aquel entonces en la entrada de su hogar fue sometido a un proceso de perfeccionamiento continuo que no se detuvo por siglos, con el único fin de elaborar ingeniosos mecanismos que evitaran a personas extrañas ingresar a sus casas o puedan roban sus pertenencias. Llegando así, al desarrollo de la cerradura, que funciona con una única llave que protege y asegura con mayor confiabilidad todo lo que se encuentre del otro lado tan sólo con un ligero movimiento.

A pesar de los años transcurridos, el diseño mecánico de esas primeras cerraduras se mantiene todavía. La evolución ha logrado mejorar el sistema de seguridad y protección de las pertenecías de cada persona, pues la ingeniería logrado crear mecanismos verdaderamente sofisticados. Hoy se puede contar con algunos pocos mecanismos electrónicos dentro del área sistemas de control de acceso, pero que aún dejan mucho que desear debido a su nivel básico de seguridad, y la necesidad de optar por mecanismos electrónicos complementarios, que ofrezcan un nivel de seguridad aceptable han lleva a industrias a innovar y mejorar estos sistemas existentes.

Es así se pudo percatar que las cerraduras instaladas en los laboratorios del edificio central de la FIE son ya obsoletas e innecesarias. Puesto que, se requiere un uso excesivo de llaves y peor aún, si son muchas las áreas que se tienen que cubrir, lo que requiere un tiempo considerable y esencial para el personal encargado del cuidado de los laboratorios el abrir o cerrar cada puerta. Además, este tipo de chapas no brindan la seguridad y confiabilidad necesaria.

Por tal motivo el presente trabajo de investigación, se tiene como objetivo fundamental desarrollar un prototipo electrónico que permita optimizar la apertura y cierre de las puertas de los laboratorios de la Facultad, tan solo usando una aplicación móvil instalada en un teléfono inteligente.

FORMULACIÓN DEL PROBLEMA

¿Se podrá solucionar los inconvenientes que presenta el personal encargado del cuidado de los laboratorios del edificio central de la facultad de informática y electrónica de la ESPOCH, al

momento de la apertura y cierre de puertas, sobre todo para ahorrarles el uso extenso de llaveros, para también de esta forma poder economizar su valioso tiempo y cómo se podría implementar un control de acceso inteligente y remoto para aumentar la seguridad y accesibilidad de los laboratorios?

SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cómo será el diseño de dichas cerraduras electrónicas?
- ¿Cómo será el funcionamiento de dichas cerraduras electrónicas?
- ¿Cómo se diseñará la aplicación móvil para el cliente final (interfaz gráfica)?
- ¿Cómo se dará la conectividad y la apertura de las puertas en el caso de redes Wifi caídas?
- ¿Con qué medios se dará la apertura y cierre de la puerta automáticamente?
- ¿Cómo se detectará el estado actual de las puertas de los laboratorios (abierto o cerrado)?
- ¿Cómo se dará la conectividad y la apertura de las puertas en el caso de fallos eléctricos?

OBJETIVOS

Objetivo General:

- Diseñar un prototipo de cerradura electrónica conectada a una red Wifi y controlada mediante una aplicación móvil, para el control automático de las puertas de los laboratorios del Edificio de la FIE.

Objetivos Específicos:

- Diseñar un sistema electrónico para acoplar a la cerradura convencional que permita la apertura o cierre de la puerta, y que, a la vez, permita conectarse a la red WiFi.
- Desarrollar una aplicación móvil basada en Android que cuente con una protección de seguridad de datos inalámbricos.
- Elaborar un sistema auxiliar ante la caída de la red WiFi y ante cortes eléctricos.
- Comprobar el funcionamiento y conectividad del dispositivo.

CAPITULO I

1 MARCO TEÓRICO REFERENCIAL

El presente capítulo constituye el estudio teórico para el desarrollo del proyecto de investigación. Para ello se detallará conceptos fundamentales, así como las características de los elementos empleados para la construcción del prototipo base.

1.1 Cerraduras

Las cerraduras son mecanismos de metal que se incorporan principalmente en puertas para resguardar la integridad de pertenecías. Este mecanismo de seguridad funciona con una llave que logra bloquear e impedir que personas que no las posean puedan acceder a ciertos lugares. La cerradura, se logra accionar con el uso de una llave, la cual por lo general es de bronce. Estas cerraduras actualmente se dividen en dos grupos, mecánicas y electrónicas, para el caso de las cerraduras electrónicas la llave puede ser un código por teclado, reconocimiento dactilar, etc. (Tipos de cerraduras, 2016)

1.1.1 Tipos de cerraduras

En la actualidad, existen diversos tipos de cerraduras. a elección de una de ellas depende del lugar o área donde se va a colocar, y la función qua ha de tener conjuntamente con el nivel de seguridad, y un control que se necesite, logrando que las pertenencias se encuentran a salvo.

Dentro de la gama de cerraduras tenemos las siguientes:

1.1.1.1 Cerraduras Tubulares

Su sistema de apertura es similar al de un picaporte, se pueden cerrar desde el interior accionando un botón. Normalmente se utiliza en las puertas de los cuartos de baño, habitaciones y estancias que necesitemos cerrar desde el interior. Su instalación es más requerida en hogares como en los establecimientos públicos. (Muñoz).

Figura 1-1: Cerradura Tubular
Fuente:http://ferreteriagolpeyllave.com/media/catalog/category/MCM_705-3_PLATA__2.jpg

1.1.1.2 Cerradura de sobreponer

La cerradura de sobreponer es un mecanismo que siempre queda al descubierto, por uno de los lados de la puerta, quedando vulnerable a ser forzada por la parte que esta visible ya sea mediante palanca, u otros elementos que usa para romper la seguridad del mecanismo (Muñoz).

Figura 2-1: Cerradura de Sobreponer
Fuente: http://www.yalelatinoamerica.com/es/yale/yale-latinoamerica/productos/

1.1.1.3 Cerraduras embutidas o empotradas

Se encuentran empotradas en la parte lateral de las puertas. Normalmente se utilizan en puertas de exterior tanto metálicas como de madera. El sistema consiste en un pestillo que se acciona girando la llave y que bloquea su apertura. Existen algunas que incluyen un sistema de auto-bloqueo con el fin de evitar que los dueños de lo ajeno no puedan hacerse de las suyas (Muñoz). Este tipo de cerraduras se encuentran en una categoría de seguridad media.

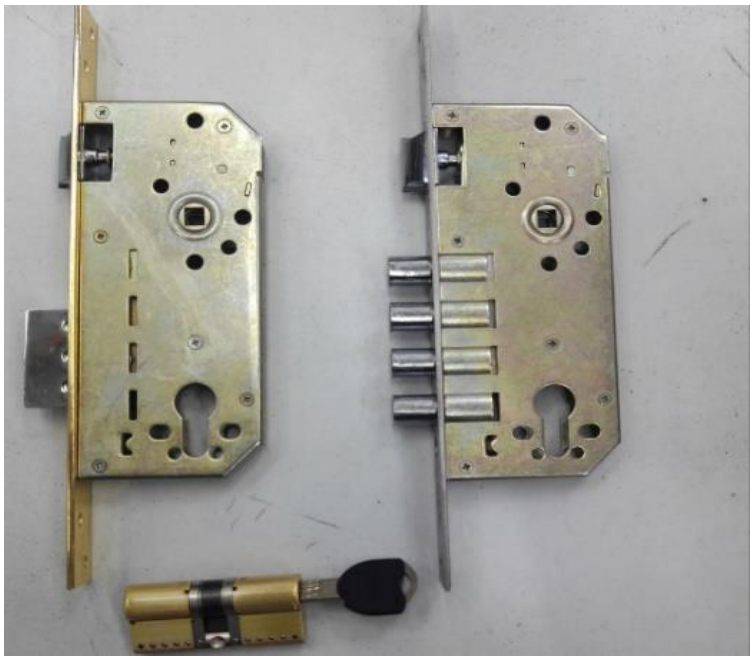


Figura 3-1: Cerradura de empotrar o embutir
Fuente: https://comunidad.leroymerlin.es/t5/Bricopedia-Reparaci%C3%B3n-y/Qu%C3%A9- tipos-de-cerraduras-existen/ta-p/79408

1.1.1.4 Cerraduras digitales

Actualmente la tecnología está en todo, incluido el mundo de las cerraduras, hoy se cuenta con algunas chapas eléctricas que se abren y cierran mediante un código por teclado, normalmente se encuentran instaladas en hoteles garajes o edificio públicos. También mencionar que este tipo de cerraduras son bastante costosas. (Muñoz)

Figura 4-1: Cerradura Digital
Fuente:http://www.yalelatinoamerica.com/es/yale/yale-latinoamerica/productos-digitales-yale/cerraduras-digitales-seguridad/cerraduras-digitales-huella/cerraudra-digital-ymf40/

1.2 Placa de desarrollo

1.2.1 Placa de desarrollo NodeMCU

NodeMCU es una placa de desarrollo de código abierto, el mismo que cuenta con el chip integrado ESP8266 a nivel de hardware y software. Consta de conexión USB, pines de entradas y salidas, y gracias a este dispositivo hace posible la comunicación Wifi. Además, el costo del controlador es sumamente económico y accesible para la mayoría de usuarios. (Gonzalez, 2017).

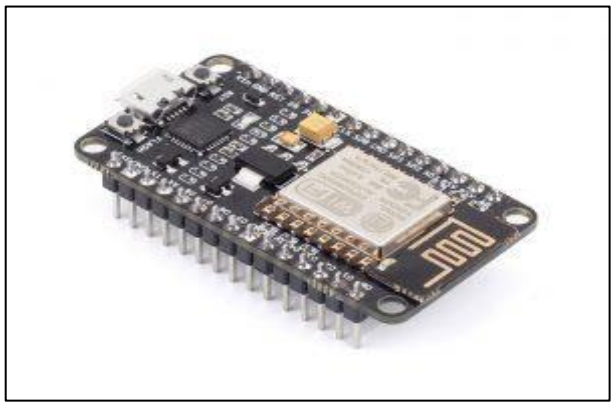


Figura 5-1: Placa de desarrollo NodeMCU
Fuente:https://statics3.seeedstudio.com/seeed/img/2017- 03/QluwTVU7FQIvaC8dZy6x2JaM.jpg

La programación se realiza mediante el lenguaje de programación LUA, un lenguaje imperativo y estructurado en el que se puede cargar scripts. Se puede programar mediante consola con comandos en tiempo real. Por otra parte, esta placa también puede ser programada mediante el software Arduino IDE como si se tratara de una placa Arduino cualquiera. (Gonzalez, 2017).

Tabla 1-1: Especificaciones técnicas de NodeMCU.

Tarjeta de desarrollo NodeMCU	Características
Procesador	ESP8266
Protocoló Inalámbrico	802.11 b/g/n
Protocolo de Internet	TCP/IP
Sensor	Temperatura
Tensión de entrada	5 V DC
Tensión de entradas/salidas	3.3 V DC
Corriente por pin	12mA.
Frecuencia del procesador mínima	80MH y (80mA)
Frecuencia del procesador máxima	160MH y (90mA)
Memoria Flash	4MB
Consumo de corriente al utilizar HTTP	100 a 110 mA

Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Fuente: http://danielmartingonzalez.azurewebsites.net/conociendo-esp8266-nodemcu-el-modulo-wifi-para-iot/

En la figura 6-1 se puede ver claramente cada uno de los pines de la placa de desarrollo.

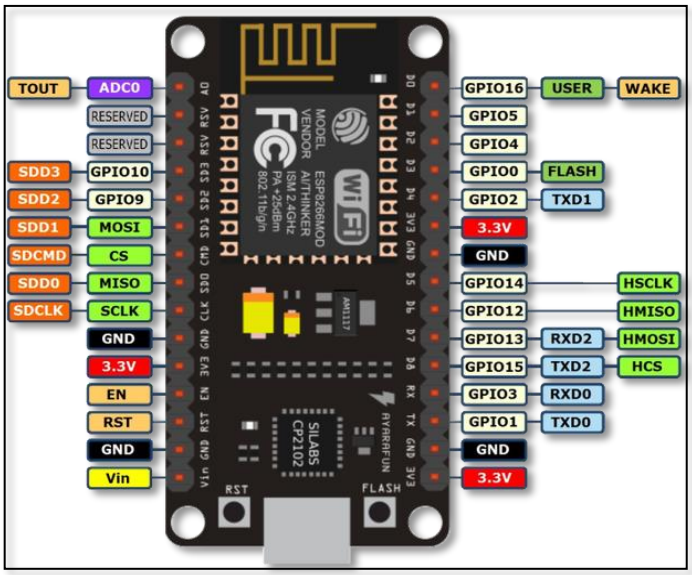


Figura 6-1: Pines de la placa de desarrollo NodeMCU
Fuente: http://panamahitek.com/esp8266-y-nodemcu-la-nueva-generacion/

1.3 Sensores

Un sensor es un dispositivo que permite captar información de forma física y convertirla en señales eléctricas como: temperatura, presión, luz, aceleración, distancia etc. Esto proporcionan una salida útil para realiza acciones de control.

Los sensores utilizados en la construcción del prototipo son los siguientes:

1.3.1 Sensor Magnético

Los sensores magnéticos se accionan por presencia de un campo magnético. Son dos encapsulados en donde Los contactos se cerrarán bajo la influencia de los imanes del cual están hechos provocado por un dispositivo imantado alojado en el objeto a detectar, dando como resultado un elemento de conmutación on-off. En otras palabras, abierto o cerrado (Sensores Fundamentos, 2014).

Estos sensores detectan el campo magnético que es provocado por los imanes que vienen insertados en cada uno de los encapsulados, su modo de funcionamiento es muy simple ya que cuando se acercan los dos contactos, cierran el circuito, y cuando se alejan, el circuito se abre.

Figura 7-1: Sensor magnético
Fuente: http://dfast.cl/sensores/113-sensor-magnetico-reed-switch.html

1.3.2 Sensor de barrera óptico

También conocido como sensor de herradura. Este tipo de sensor está compuesto por un diodo emisor de luz, por lo general es un led infrarrojo, y también de un fototransistor. La detección ocurre cuando un objeto interrumpe el haz de luz entre el emisor y receptor. Generando así una señal de cero o uno. (Sensores Fundamentos, 2014)

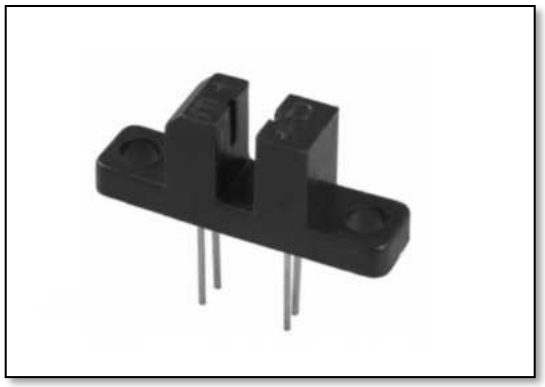


Figura 8-1: Sensor de barrera
Fuente: http://sgsdistribuciones.com/sgs/wp-content/uploads/2015/02/H21A1.png

1.3.3 Sensor LDR

Es una resistencia que varía su valor dependiendo de la cantidad de luz, esto quiere decir que el foto resistor disminuye su resistencia, si hay un aumento en la intensidad de luz, y por el contrario si la intensidad de luz disminuye, la resistencia aumenta. (Fotorresistencia, 2017). Los valores de resistencia varían dependiendo de la cantidad de luminosidad, estos valores varían entre 1 MΩ o más en la oscuridad y 100 Ω con luz brillante.

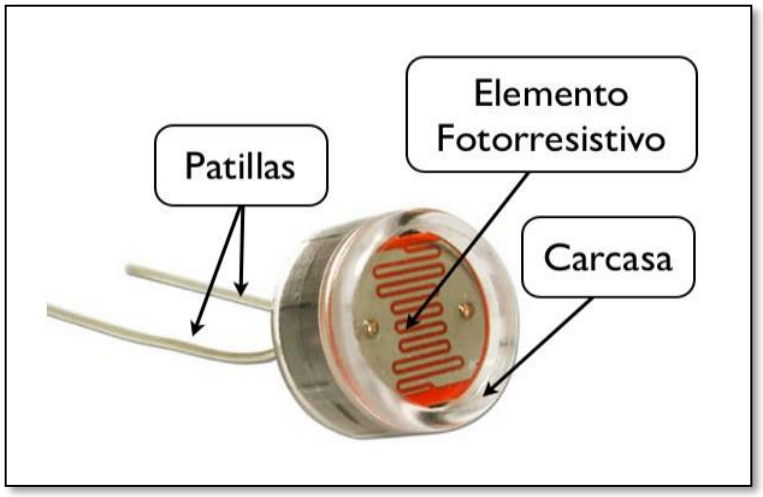


Figura 9-1: Partes de una fotocélula
Fuente: https://ingenieriaelectronica.org/fotorresistencia-definicion-caracteristicas-y-tipos/

1.4 Actuadores Eléctricos

1.4.1 Definición

Un actuador es un dispositivo inherentemente mecánico que brinda la posibilidad de transformar diferentes tipos de energía para generar algún funcionamiento dentro de un sistema automatizado determinado, su función es proporcionar fuerza para mover o "actuar" otro dispositivo mecánico. (Gonzáles, 2016).

Usualmente, los actuadores generan una fuerza mecánica a partir de distintos tipos de energía, como puede ser eléctrica, neumática, o hidráulica.

1.4.2 Servomotor

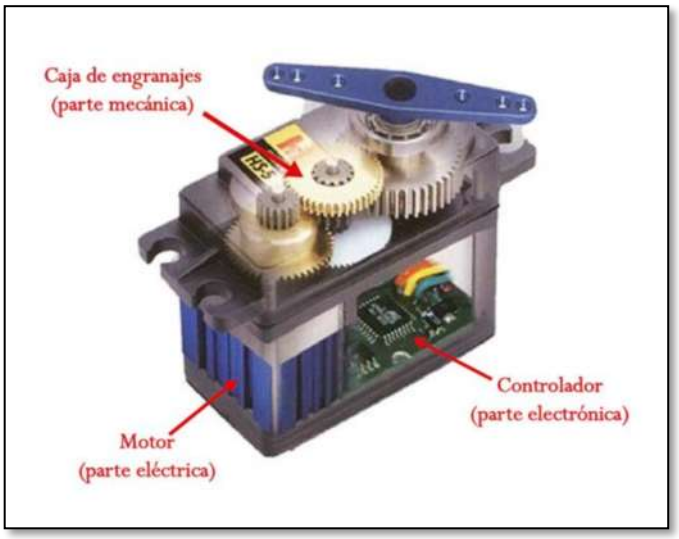


Figura 10-1: Partes de Servomotor
Fuente: http://panamahitek.com/wp-content/uploads/2016/11/servomotor.png

Un servomotor es un motor eléctrico especial en el que se puede controlar tanto la velocidad, como la posición del eje en un momento dado, están diseñados para moverse determinados grados y mantener la posición de manera fija. El servomotor no gira su eje 360º, pero actualmente existen algunos que, si pueden hacerlo, pero son poco comunes. Los servomotores normales, giran 180º hacia la izquierda o hacia la derecha es decir ida y retorno. (Servomotores).

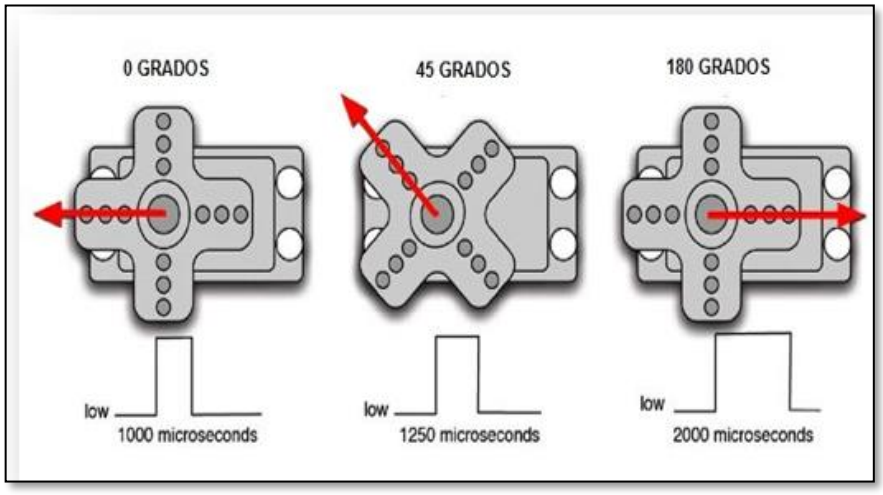


Figura 11-1: Funcionamiento de un Servomotor
Fuente:http://www.areatecnologia.com/electricidad/servomotor.html

1.4.2.1 Características principales

El interior, de un servomotor es un motor DC común. El eje del motor se acopla a una caja de engranajes similar a un sistema de transmisión. Esto se hace para potenciar el torque del motor y permitir mantener una posición fija cuando se requiera. De forma similar a un automóvil, a menor mayor velocidad, menor torque. El circuito electrónico es el encargado de manejar el movimiento y la posición del motor. (Gonzáles, 2016)

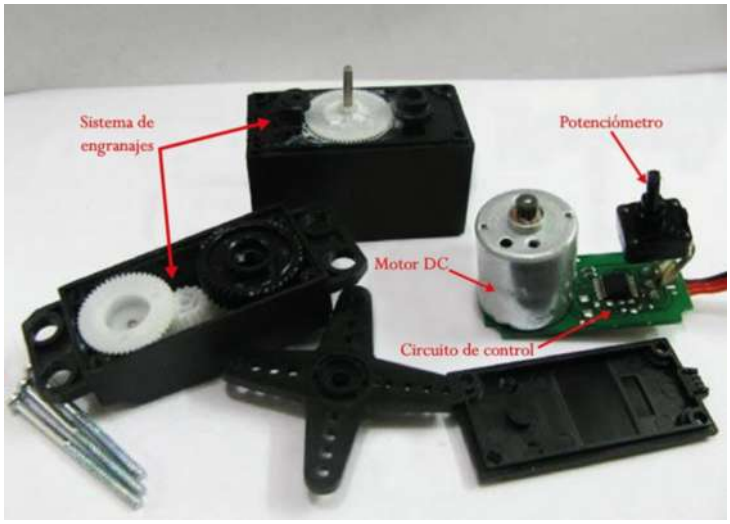


Figura 12-1: Partes de un servomotor
Fuente: http://panamahitek.com/wp-content/uploads/2016/12/partes_servomotor.jpg

1.4.2.2 Partes de un Servomotor

Un servomotor es un sistema compuesto por:

- Un motor eléctrico el cual se encargado de generar el movimiento, a través de su eje.
- Un sistema de regulación formado por engranajes, que actúan sobre el motor para regular su velocidad y el par. Mediante estos engranajes, podemos aumentar la velocidad o disminuirlas
- Un circuito electrónico y un sensor interno que controla el movimiento del motor mediante el envío de pulsos eléctricos.
- Un potenciómetro conectado al eje central del motor, que nos permite saber en todo momento su ángulo, pues un potenciómetro lo utilizamos como un sensor variable.

1.5 Comunicación Inalámbrica

En 1887 Heinrich Rudolph Hertz, un físico alemán, demostró que existían las ondas electromagnéticas y que éstas podrían ser usadas para mover información a grandes distancias, la unidad de medidas de las frecuencias del espectro llevan su apellido (Hertz o Hz). (Tecnologías de Comunicación Inalámbrica, 2002)

Un breve ejemplo básico de un tipo de comunicación inalámbrico es la comunicación verbal entre dos personas el medio que se utiliza es el aire como un canal para el intercambio de información.

1.5.1 Comunicación WiFi

La red WIFI (Wireless Fidelity) se refiere a una de las tecnologías de comunicación inalámbrica más utilizadas actualmente, el traspaso de información se la realiza mediante ondas electromagnéticas. WIFI, también llamada WLAN (red inalámbrica) o estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11.

El estándar 802.11 es un tipo de estándar de comunicación inalámbrica la cual permite un ancho de banda de 1 a 2 Mbps, actualmente tenemos estándares físicos (802.11a, 802.11b y 802.11g) esto con el fin de garantizar mayor seguridad y compatibilidad a continuación se presenta los diferentes estándares físicos Wifi. (La comunicación inalámbrica, 2005)

Tabla 2-1: Especificaciones técnicas del estándar WiFi

Estándar	Características
Wifi (802.11a)	El flujo de datos es de 54 Mbps, cinco veces más del 802.11b. Su rango de alcance es de 30 m , su tecnología se basa en OFDM (multiplicación por división de frecuencias ortogonales). Transmite en un rango de frecuencias de 5GHz y utiliza 8 canales no superpuestos.
Wifi (802.11b)	Transferencia de datos de 11Mbps.

	Tiene un alcance de 100m en ambiente cerrados y más de 200m al aire libre.
Wifi (802.11g)	Transferencia máxima de datos de datos es de 54Mbps. Tiene un alcance de 100 a 150 m. Frecuencia de operación es de 2.4 a 2.5 GHz.
Wifi (802.11n)	Tiene una transferencia de datos de 200Mbps. La transferencia de datos es de 540Mbps. Su alcance es de 50m hasta un máximo de 160m.

Fuente: http://ieeestandards.galeon.com/aficiones1573579.html

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

La velocidad que ofrecen estos distintos tipos de estándares se convierte en un método perfecto para el acceso a internet sin la necesidad de usar cables para su conexión. (La comunicación inalámbrica, 2015)

1.5.2 Funcionamiento

Una red Wireless (sin cables), utiliza las ondas de radio de la misma forma que lo hacen los teléfonos móviles, de hecho**,** la comunicación a través de una red Wireless es muy parecida a las dos vías de comunicación por radio.

- El adaptador inalámbrico (Wireless) de un ordenador traduce los datos en forma de señal de radio y los transmite por medio de una antena.
- Un router inalámbrico recibe la señal y la decodifica. El router envía la información a Internet utilizando una conexión física, cableada, de Ethernet.

El proceso funciona también a la inversa, cuando el router recibe información de Internet la traduce a una señal de radio que es enviada al adaptador inalámbrico del ordenador. (¿CÓMO FUNCIONA LO INALÁMBRICO?, 2013)

Ventajas

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse dentro de un rango suficientemente amplio.

- Una vez configuradas, las redes WiFi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura. (Tecnología WiFi)

1.5.3 Red de datos

Una red de datos o red informática, es un conjunto de computadores y software conectados entre sí por medio de un conjunto de dispositivos físicos que envían y reciben señales eléctricas, ondas electromagnéticas, haces de luz o cualquier otro medio que permita el transporte de datos, para compartir información, recursos y ofrecer servicios.

Las redes de datos se pueden clasificar dependiendo ciertas características, siendo una de ellas el alcance que tiene la misma. La siguiente es una clasificación con base, en el alcance geográfico.

- **Red Local:** una red de área local, (**LAN**. Local Área Network) es una red de dispositivos que abarca un área reducida como una casa, un departamento, un edificio, o cualquier área donde no existe conexión con otra red, es decir todas las computadoras pertenecen al mismo dominio.

- **Red Remota:** una red de área amplia, (**WAN**. Wide Área Network), es una red de dispositivos que abarca varias ubicaciones físicas, permitiendo la conexión de una zona más extensa como un campus universitario, todo el terreno de una empresa, un municipio, un país, incluso varios continentes. Es una red que posibilita a varias redes locales (LAN) estar unidas permitiendo que todos los equipos estén conectados a pesar de no estar en la misma ubicación física.

1.5.3.1 Canales de datos

Para poder realizar el envío y recepción de datos se necesita un medio por el cual puedan viajar los mismos, las redes actuales utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar una ruta por la cual pueden transmitirse los datos.

- **Hilos metálicos:** cable de cobre como UTP o coaxial.
- **Fibra óptica:** fibras de vidrio o plástico.
- **Ondas de radio:** Wifi, Bluetooth, NFC.

Algunas características que se deben considerar en la selección del medio son, por ejemplo, la distancia por la que los medios pueden transportar una señal correctamente, el entorno en el que

se instalarán los medios, la cantidad de datos y la velocidad a la que se deben transmitir, el costo del medio y de la instalación.

1.5.4 Modelos de Referencia

Un modelo de referencia permite la comprensión de los protocolos de comunicación y la arquitectura de los sistemas utilizados para interrelacionar distintos programas y equipos, los modelos están formados por capas o normas. Así se tiene los dos tipos de modelos como son:

1.5.4.1 Modelo OSI

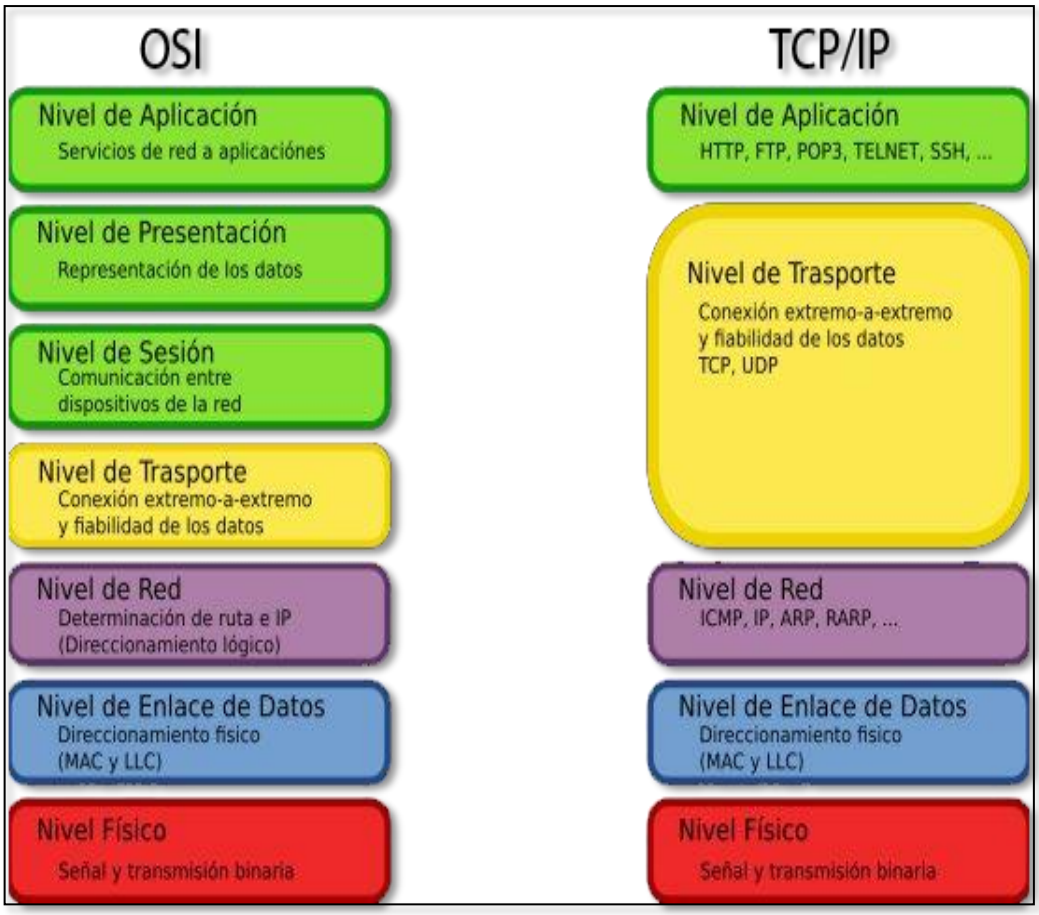


Figura 13-1: Modelo OSI vs TCP/IP
Fuente: http://mikrotikxperts.com/images/informacion/conocimientos_basicos/ositcp01.png

Capas del modelo OSI

- **La capa de aplicación:** proporciona los servicios que usan las aplicaciones para que el usuario pueda comunicarse con la red.
- **La capa de presentación:** es un formato que se usa para intercambiar datos entre las aplicaciones, y a la vez permite la transferencia de los datos.

- **La capa de sesión:** tiene herramientas para controlar el diálogo entre las aplicaciones de los sistemas, como abrir y cerrar sesión.
- **La capa de transporte:** permite intercambiar datos entre sistemas finales, dividiendo el mensaje en varios fragmentos. El servicio de transporte puede ser orientado o no orientado a conexión.
- **La capa de red:** es el camino por donde se trasladará los datos desde el origen hasta su destino a través de una o más redes conectadas mediante dispositivos de enrutamiento (router).
- **La capa de enlace de datos:** realiza el direccionamiento físico dentro de cualquier topología de red, esta capa nos permite activar, mantener y deshabilitar la conexión, así como la notificación de errores.
- **La capa física:** controla las señales por donde viajaran los datos (cable de par trenzado, fibra óptica, radio frecuencia). (Rodríguez, Jose Maria; San Martín, Maimon)

1.5.4.2 Modelo TCP/IP

En casos prácticos se tiene el modelo TCP/IP que representa todas las reglas de comunicación para Internet y se basa en la noción de direcciones IP dotada a cada equipo de la red para poder enviar paquetes de datos. Está diseñado para cumplir con una cierta cantidad de criterios, entre ellos, dividir mensajes en paquetes, usar un sistema de direcciones, enrutar datos por la red y detectar errores en las transmisiones de datos. (Vialfa, 2017)

El modelo TCP/IP se ve influenciado por el modelo OSI que de igual forma usa el enfoque modular (utiliza módulos o capas), pero sólo contiene cuatro:

Capas del modelo TCP/IP

- **Capa de acceso a la red**: especifica la forma en la que los datos deben enrutar, sea cual sea el tipo de red utilizado.

- **Capa de Internet**: es responsable de proporcionar el paquete de datos (datagrama).
- **Capa de transporte**: brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión. Comprende a los protocolos TCP y UDP.
- **Capa de aplicación**: incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.). (Vialfa, 2017)

1.5.5 Router

Llamado también enrutador. Es un dispositivo que permite dirige la información recolectada por el módem hacia los aparatos que estén dentro de una red a la vez entregan selectivamente paquetes de información a múltiples destinos. (Definición de Router)

Figura 14-1: Router HG 110 ADSL
Fuente:http://static.mercadoshops.com/modem-fiberhome-hg110-router-adsl-wifi-nuevo-speedy_iZ1XvZcXpZ3XfZ128404736-439768736-3.jpgXsZ128404736xIM.jpg

1.6 NFC

La tecnología Near Field Comnunication (NFC) permite la transmisión de datos de una manera simple entre diferentes dispositivos mediante un enlace de radiofrecuencia en la banda de radio ISM, lo que quiere decir que está orientada para fines industriales científicos y médicos (Industrial, Scientific and Medical).

Se trata de una tecnología inalámbrica que funciona en la banda de los 13.56 MHz. Se deriva de las etiquetas RFID. NFC es una plataforma abierta pensada desde el inicio para teléfonos y dispositivos móviles. Su tasa de transferencia puede alcanzar los 424 kbit/s por lo que su enfoque más que para la transmisión de grandes cantidades de datos es para comunicación instantánea, es decir, identificación y validación de equipos y o personas. (Simons, 2012)

La tecnología NFC puede funcionar en dos modos:

- **Activo**, en el que ambos equipos con chip NFC generan un campo electromagnético e intercambian datos.
- **Pasivo**, en el que solo hay un dispositivo activo y el otro aprovecha ese campo para intercambiar la información.

1.7 Aplicación Móvil

Una aplicación móvil es un programa que se puede descargar e instalar en el dispositivo móvil de un usuario y al que se puede acceder directamente desde su teléfono, tiene una función de ayudar al usuario en la realización de un trabajo concreto. Toda persona que tenga en posesión un Smartphone, Tablet u otro tipo de dispositivo móvil, utiliza a diario algunos tipos de aplicaciones móviles. La mayoría de ellas vienen instaladas por defecto, en cada uno de los móviles. (Desarrollo de apps, 2017).

1.7.1 Ciclo de vida de una aplicación en Android

Toda aplicación en Android cumple con un ciclo de vida administrada por el sistema operativo, basándose en las necesidades del usuario, los recursos disponibles, etc. Si se tiene una aplicación que está consumiendo muchos recursos y se arranca otra nueva, el S.O. probablemente le diga a la aplicación que se queda en segundo plano que libere todo lo que pueda. (Ciclo de vida de una aplicación Android, 2011). Si es necesario la cerrará. En Android los recursos son normalmente muy limitados y por eso el sistema operativo tiene más control sobre sus aplicaciones.

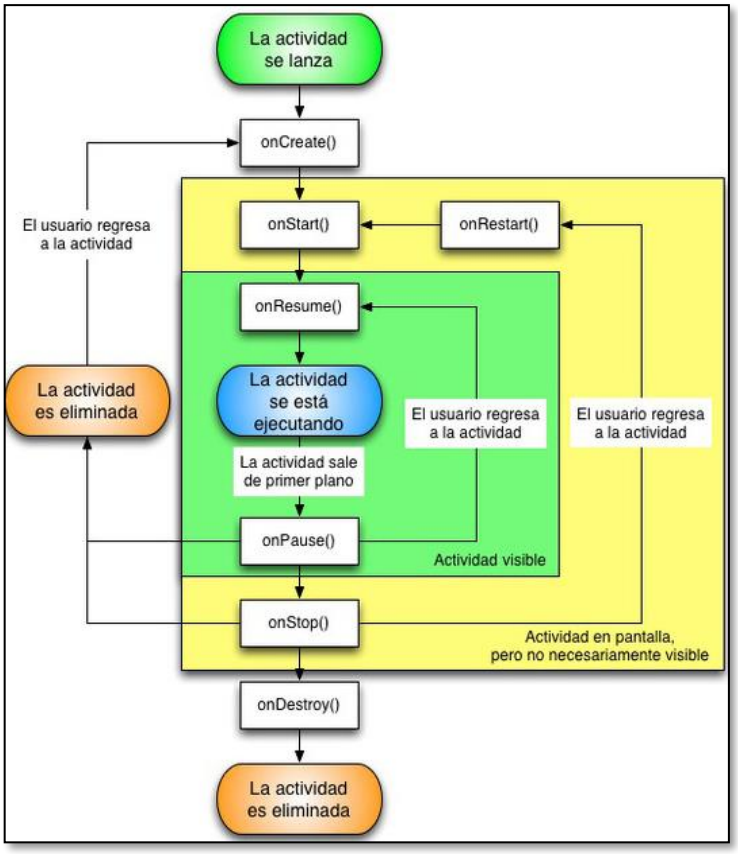


Figura 15-1: Ciclo de vida de una Aplicación
Fuente: http://aplicmovil101desmovil.blogspot.com/2015/06/politica-de-eliminacion-y-el-ciclo-de.html

Todas las aplicaciones móviles actualmente tienen que poseer un parámetro que permita realizar las respectivas actualizaciones y por consiguiente se tiene los siguientes métodos que intervienen en cada activity de Android (Victor, 2013)

- **onCreate():** Representa el momento en el que la actividad se crea. Este método normalmente lo generará el asistente al crear una nueva actividad en Android, y es donde crearemos todo lo que vaya a necesitar la actividad. (2015).
- **onStart():** La actividad va a pasar a estar en pantalla, aunque no necesariamente visible. Si venimos de una parada, pasaremos antes por onRestart ().
- **onRestart():** Una actividad parada vuelve a ser acivada.
- **onResume():** La actividad va a empezar a responder a la interacción del usuario.
- **onPause():** La actividad va a dejar de responder a la interacción del usuario.
- **onStop():** La actividad ha pasado completamente a segundo plano.
- **onDestroy():** La actividad va a ser destruida y sus recursos liberados.

1.7.2 Service en Android

Un servicio es un componente necesario para realizar una tarea en segundo plano sin que exista interfaz gráfica que interactúe con el usuario, la función de un servicio es permitir hacer repetitiva una actividad o que necesiten usar operaciones que requieren de bastante tiempo, como puede ser una descarga de archivos, sincronización de datos con la Apps, etc. (Programación en Android,2014)

Ventajas de usar un servicio

- Facilita que la aplicación pueda indicar al sistema, realizar una tarea en el background, e incluso si el usuario no está interactuando con la aplicación, esto se lo realiza con el método startService (Intent serv) la misma que hace una petición al sistema para ejecutar el servicio. Hasta que el servicio finalice por si sólo o el usuario lo haga.

- Comparte funcionalidades con otras aplicaciones, mediante el método bindService (Intent ser, ServiceConnetion conn, int flags).

- Facilita la interfaz cliente servidor, ayuda también con la interfaz gráfica y realiza peticiones al servicio obteniendo los resultados esperados.

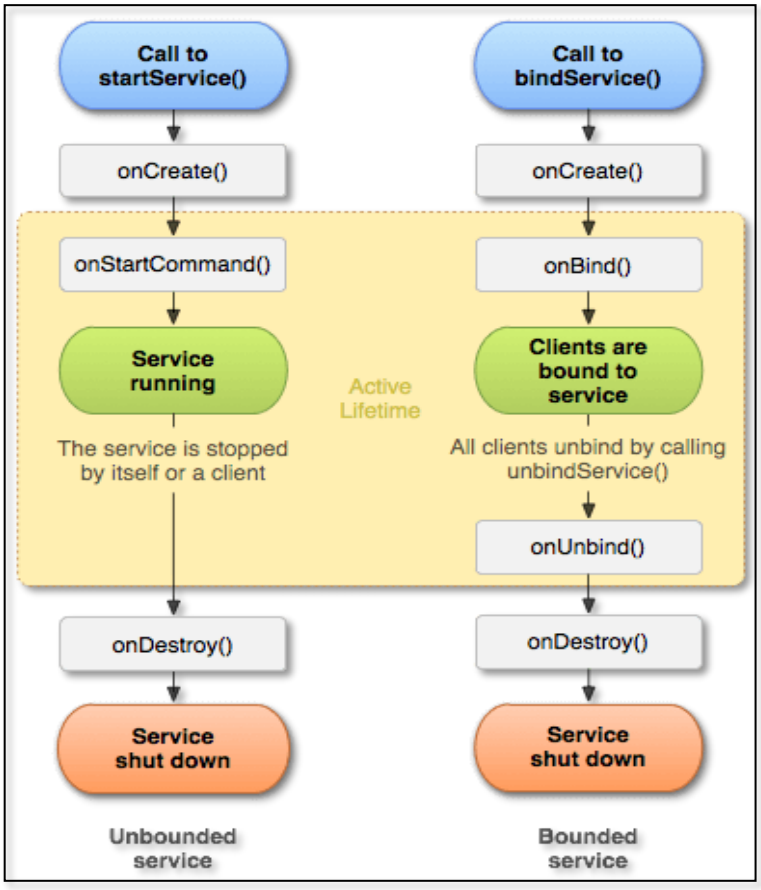


Figura 16-1: Ciclo de vida de un Servicio
Fuente: http://www.proyectosimio.com/wp-content/uploads/2014/02/service_lifecycle.png

1.8 Criptografía

1.8.1 Definición

"La criptografía es la ciencia de usar las matemáticas para encriptar y desencriptar datos (cifrar y descifrar datos). Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aun así permanecer secreta. " (Technologies, 2016)

El algoritmo criptográfico trabaja en combinación con una clave ya sea un número, una palabra, frase, o contraseña para encriptar y desencriptar la información. El objetivo es hacer tan difícil, como sea posible la desencriptación de datos.

Con la encriptación de datos se logra tener tres aspectos fundamentales sobre la información que se desea enviar a través de la red de comunicaciones:

- **Confidencialidad:** Que sólo pueda acceder a la información el verdadero destinatario.
- **Autentificación:** Que tanto el emisor como el receptor de la información puedan confirmar la identidad de la otra parte.
- **Integridad:** Que la información no pueda ser alterada sin ser esto detectado.

Un buen sistema de cifrado es cuando la seguridad tiene mayor peso en su clave y no en el algoritmo, siendo el tamaño de la clave una medida de seguridad del sistema.

1.8.2 Tipos de Criptografía

1.8.2.1 Criptografía de clave privada o simétrica

La Criptografía simétrica permite una comunicación segura entre las dos partes siempre que, con anterioridad, se intercambie la misma clave correspondiente, la cual se denomina clave simétrica, la simetría se refiere a que tanto para cifrar como para encriptar tengan la misma contraseña.

Además, existen dos modos de operación:

- **Cifrado por bloques:** La información a cifrar se divide en bloques de longitud fija (8,16 bytes) y luego se aplica el algoritmo de cifrado a cada bloque utilizando una clave secreta. **Ejemplos:** DES, AES. (Pousa, 2011)

- **Cifrado de flujo:** Mayormente usado para el cifrado de conversaciones telefónicas o chats porque los datos se producen en tiempo real en pequeños fragmentos. Las muestras de datos pueden ser tan pequeñas como 8 bits o incluso de 1 bit.

  El algoritmo genera una secuencia pseudoaleatoria (secuencia cifrada o keystream) de bits que se emplea como clave. Esto quiere decir que mientras va ingresando los bits, inmediatamente son cifrados. Un ejemplo es el RC4. (Pousa, 2011)

1.8.2.2 Criptografía de clave pública o asimétrica

La Criptografía asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, Este tipo de sistema utiliza dos claves diferentes para cada

usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. (Marrero, 2003)

1.8.3 Algoritmo de Encriptación AES

AES (Advanced Encryption Standard), conocida como el Estándar de Encriptación Avanzada, es una técnica de cifrado de clave simétrica. Fue desarrollado por dos criptologistas belgas, Vincent Rijmen y Joan Daemen. Proporciona una encriptación segura lo suficientemente confiable para proteger la información clasificada de alto nivel. Por ser simétrico, se utiliza la misma clave para encriptar como para desencriptar, la longitud de la clave puede ser de 128, 192 o 256 bits según especifica el estándar, esto permite tres implementaciones conocidas como AES-128, AES-192 y AES-256

1.8.3.1 Funcionamiento

AES es un algoritmo de cifrado por bloques, inicialmente fue diseñado para tener longitud de bloque variable pero el estándar define un tamaño de bloque de 128 bits, por lo tanto los datos a ser encriptados se dividen en segmentos de 16 bytes (128 bits) y cada segmento se lo puede ver como un bloque o matriz de 4x4 bytes al que se lo llama estado, este se organiza como se ve en la figura 17-1. (Pousa, 2011)

Figura 17-1: Bloque AES
Fuente:http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf.

Partiendo de una clave inicial de 16 bytes (128 bits), que también se la puede ver como un bloque o matriz de 4x4 bytes, se generan 10 claves, estas claves resultantes junto con la clave inicial son denominadas subclaves.

El proceso de cifrado del algoritmo consiste en aplicar a cada estado un conjunto de operaciones agrupadas en lo que se denominan rondas, el algoritmo realiza 11 rondas, en donde a cada ronda se aplica una subclave diferente. Las 11 rondas se pueden clasificar en 3 tipos: (Pousa, 2011)

- 1 ronda inicial (se aplica la subclave inicial).
- 9 rondas estándar (se aplican las 9 subclaves siguientes, una en cada ronda).
- 1 ronda final (se aplica la última subclave).

Las operaciones que realiza el algoritmo dentro de las rondas se reducen a 4 operaciones básicas:

- SubBytes.
- ShiftRows
- MixColumns.
- AddRoundKey

Y como se aprecia en la figura 18-1 se muestra todo el proceso hasta obtener un bloque cifrado

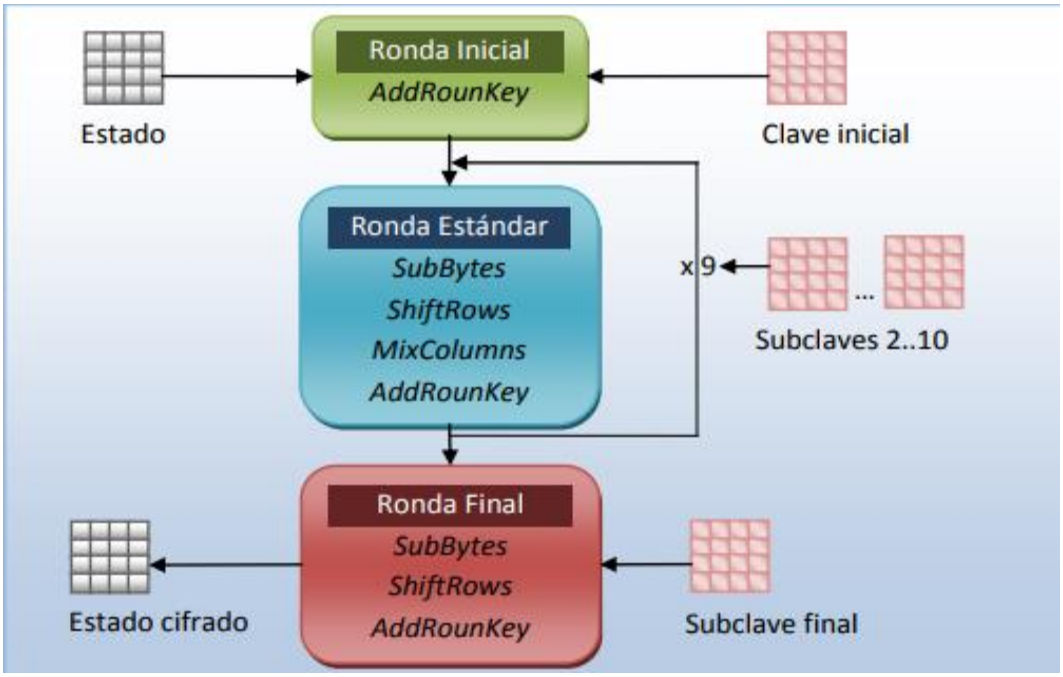


Figura 18-1: Diagrama de operaciones y claves del algoritmo AES
Fuente:http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf

1.9 Firebase

Firebase es la nueva y mejorada plataforma de desarrollo móvil en la nube de Google. Se trata de un servicio compatible para diferentes plataformas como son Android, iOS o web, de esta forma presentan una alternativa seria a otras opciones para ahorro de tiempo en el desarrollo, facilitando el poder tener una aplicación conectada con datos en la nube para proveer una API que se pueda guardarlos y sincronizarlos en tiempo real. (Zamora, 2016)

Las características que presenta son:

- **Analítica**: Provee una solución gratuita para tener todo tipo de medidas (hasta 500 tipos de eventos), para gestionarlo todo desde un único panel.
- **Desarrollo**: Permite construir mejores apps, permitiendo delegar determinadas operaciones en Firebase, para poder ahorrar tiempo, evitar bugs y obtener un aceptable nivel de calidad. Entre sus características destacan el almacenamiento, testeo, configuración remota, mensajería en la nube o autenticación, entre otras.
- **Crecimiento:** Permite gestionar los usuarios de las aplicaciones, pudiendo además captar nuevos. Para ello dispondremos de funcionalidades como las de invitaciones, indexación o notificaciones.
- **Poder de crecimiento**: Permite gestionar de manera fácil todos los usuarios de las aplicaciones, con el añadido de que se pueden captar nuevos usuarios, mediante invitaciones o notificaciones.
- **Monetización**: Mediante AdMob, Firebase permite ganar dinero.
- **Rapidez:** Implementar Firebase puede ser fácil y rápido, gracias a su API que es muy intuitiva, sostenida en un solo SDK. Se puede centrar el esfuerzo del desarrollador en resolver los problemas de los clientes y así poder evitar la pérdida de tiempo en la creación de una infraestructura compleja.
- **Agilidad**: Firebase ofrece apps multiplataforma con aplicaciones integradas a SDK individuales para iOS, Android y Javascript, de tal forma que se puede gestionar diferentes apps sin necesidad de salir de la propia plataforma. (Zamora, 2016)

Uno de los servicios que ofrece Firebase es la autentificación, una herramienta que ayuda a realizar el Login en el sistema y crear aplicaciones multiusuario sin tener que programar mucho. En la autenticación, se debe mencionar que al realizar el Login con un usuario y clave, se lo puede realizar también con distintos conectores sociales como Facebook, Twitter, Google, etc. Este servicio ofrece la posibilidad de realizar aplicaciones funcionalidades avanzadas (Zamora, 2016)

1.10 Sistema de alimentación

1.10.1 Convertidor DC-DC Step-Down (Mp1584)

Este módulo permite convertir una tensión DC/DC, los rangos de tensión máximos están entre 4.5 V y 28 V, también opera con rangos de salida que están entre 0.8V y 18V. Este módulo está basado en un regulador DC-DC Step Down LM2596, que es un circuito integrado monolítico, maneja una corriente de 3A, denominada también como una fuente de alimentación conmutada, así que su eficiencia es significativamente mayor en comparación con los populares reguladores lineales de tres terminales, se debe recalcar que la tensión de entrada por lo menos debe ser de 1.5V mayor que el voltaje de salida para que el módulo pueda funcionar correctamente.

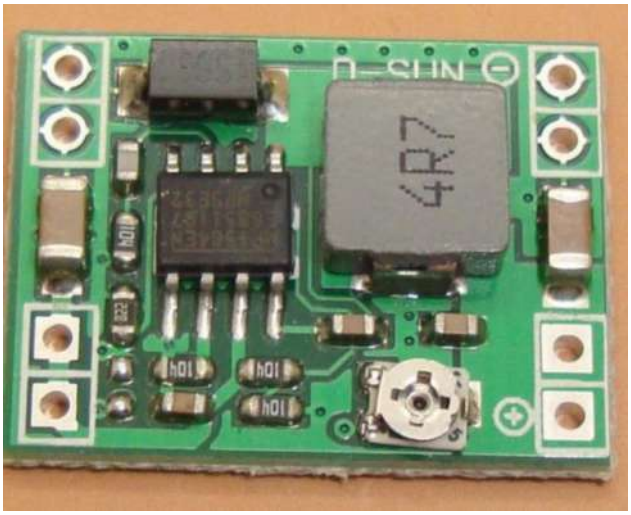


Figura 19-1: Módulo Step-Down MP1584
Fuente: http://jghttrading.com/static/p/959/959_800.jpg

Especificaciones:

- Amplio rango de operación, desde 4.5V hasta 28V.
- Un 92% de eficiencia.
- Temperatura de funcionamiento es de -40° Celsius a 80° Celsius.
- Frecuencia de conmutación programable de 100kHz a 1.5 MHz.
- Modo de omisión de pulsos de alta eficiencia para capacitores cerámicos estables.
- Protección de sobre corriente ciclo a ciclo.
- Bloqueo de sobre voltaje de entrada.

En la figura 20-1 se puede apreciar cómo se debe conectar los pines del módulo.

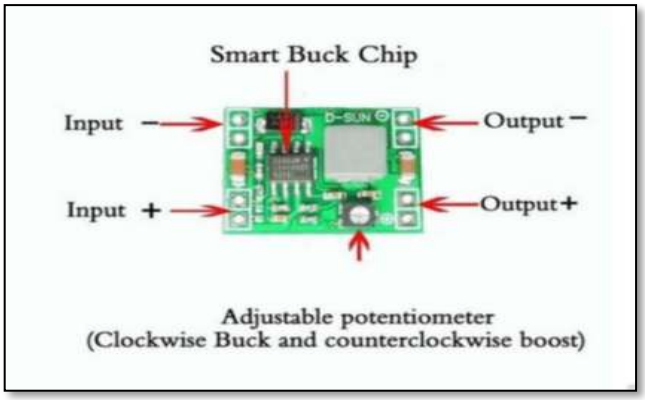


Figura 20-1: Pines de conexión del convertidor DC/DC
Fuente:https://ae01.alicdn.com/kf/HTB1RBEJJXXXXXbAXFXXq6xXFXXXC/MP1584EN-super-font-b-small-b-font-DC-DC-3A-Adjustable-power-step-down-module-exceed.jpg

1.10.2 Batería

Es un acumulador de energía es decir un dispositivo que está fabricado con celdas electroquímicas que pueden convertir la energía química acumulada en electricidad (BATERIAS Y ACUMULADORES)

1.10.2.1 Ciclo de carga de una batería

Con el tiempo empieza a degradarse las baterías químicamente, que a la larga se verá afectado el desempeño, y la vida útil de las mismas.

Proceso de carga: La tensión de una batería de acumulación es cc, para realizar la carga de la batería se necesita de un transformador, y una placa para la regulación de tensión, y para poder forzar una corriente de carga la tensión deberá ser mayor al de la batería, ya que esta corriente provoca reacciones químicas en los electrodos y que el transformador sea capaz de mantener esa corriente. Este proceso es reversible es decir si se conecta un transformador y se le conecta una carga eléctrica a la batería, la corriente circulará en dirección opuesta a la carga provocando reacciones químicas. (Etapas de carga de una batería, 2016)

Ciclo de carga – descarga

En principio existen limitaciones donde el tiempo de vida útil del batería se ven afectadas por este fenómeno. Cuando un tipo de energía es convertido la eficiencia del sistema nunca alcanza el

100% ya que existen perdidas por el calor, aquí existe doble conversión energética que da lugar a las pérdidas durante el proceso de carga y descarga.

1.11 SolidWorks

1.11.1 Definición

SolidWorks es una solución de diseño tridimensional completa que integra un gran número de funciones avanzadas, creada para facilitar el modelado de piezas, crear grandes ensamblajes, generar planos y otras funcionalidades que le permiten validar, gestionar y comunicar proyectos de forma rápida, precisa y fiable. (Introducción a SolidWorks)

Aplicaciones de SolidWorks

- Está presente principalmente en el diseño mecánico.
- Sistemas dentro de la Ingeniería Mecatrónica.
- Ensamble de Robots.
- Diseño Automotriz y aeroespacial.
- Biomecánica.
- Diseños de dispositivos médicos.

1.12 Componentes Electrónicos

1.12.1 DFplayer Mini

El DFPlayer Mini es un reproductor de audio a través de ficheros almacenados en una tarjeta SD.

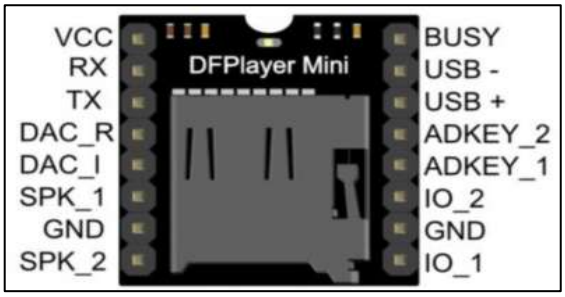


Figura 21-1: Reproductor MP3
Fuente:https://www.dfrobot.com/wiki/images/thumb/a/ab/Miniplayer_pin_map.png/550px-Miniplayer_pin_map.png

Características

- Capaz de reproducir formatos de fichero MP3, WMA y WAV.
- Trabaja a 3.3 y 5 V.
- Dispone de un lector micro SD compatible con FAT16 y FAT32, con una capacidad máxima de 32GB. Soporta hasta 100 carpetas y puede acceder hasta 255 canciones.
- Proporciona velocidades de muestreo de 8, 11.025 12 16 22.05 24 32 44.1 y 48 kHz, y salida con DAC de 24 bits. Dispone de 30 niveles de volumen ajustable, ecualizador de 6 niveles, y una relación señal ruido (SNR) de 85dB
- EL DFPlayer Mini recibe comandos desde NodeMCU por puerto serie. Dispone de funciones para reproducir, detener, pausar, avanzar, retroceder entre canciones. La salida se realiza directamente al altavoz, a través de los pines SPK_1 y SPK_2. (Llamas)

1.12.2 RTC DS3231

El módulo RTC es un reloj en tiempo real que permite llevar un registro detallado del transcurso del tiempo, cuando se está ejecutando una petición, desde la tarjeta de desarrollo NodeMCU. La ventaja de este dispositivo es mantener el tiempo, aun cuando se desconecte el mismo del sistema. (Ganzáles, 2014)

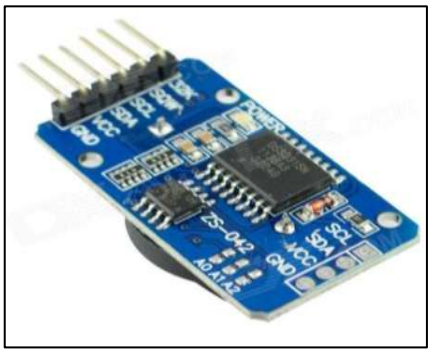


Figura 22-1: Reloj RTC
Fuente: http://pana mahitek.com/el-modulo-ds3231-un-reloj-para-arduino/

Características

- Posee un regulador de tensión.
- Incorporan una pequeña memoria EEPROM AT24C32, que puede ser empleada para almacenar registros y mediciones.

- Consta de una batería de 3.6 voltios, tiene otros usos adicionales como medir la temperatura.
- Se comunica con Arduino utilizando el protocolo I2C.
- Los pines de conexión son: VCC, GND, SCL y SDA.

1.12.3 Display oled SSD1306

Estas son pantallas pequeñas, pero muy legibles debido al alto contraste de una pantalla OLED. Esta pantalla está hecha de 128x64 individuales de blanco OLED píxeles, cada uno es encendido o apagado por el chip del controlador, la pantalla hace su propia luz, no se necesita luz de fondo. De esta manera se reduce potencia necesaria para ejecutar el OLED o pantalla además de su contraste tan alto. (Mini pantalla OLED)

Figura 23-1: Display Oled
Fuente: https://images-na.ssl-images-amazon.com/images/I/41nxGCQnvVL.jpg

Tabla 3-1: Características de Display Oled.

Display OLED	
Características	**Dimensiones**
Interfaz SPI o I2C.	PCB: 38mm x 29 mm (1.5 “x 1”)
Alimentación de 5 V.	Pantalla de 25mm x 14mm.
Posee un regulador de tensión	Espesor:4mm.
Requiere de un microcontrolador que por lo menos tenga 1K de memoria RAM.(Utiliza un buffer intermedio).	Un peso de 8.5g
Consume una corriente de 20 mA.	

Fuente: http://tienda.bricogeek.com/descatalogado/483-mini-pantalla-oled-128x64.html
Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

CAPITULO II

2. MARCO METODOLÓGICO

En éste capítulo se detalla cada uno de los bloques que conforman el prototipo de cerradura electrónica conectada a una red WiFi. Por medio de esquemas se describe claramente el diseño e implementación del sistema mecánico y electrónico, el desarrollo de la aplicación móvil desarrollada en Android Studio.

Además, se describe una base de datos del registro de usuarios que tendrán acceso a la aplicación, así como la respectiva comunicación WiFi y la protección de envío y recepción de datos mediante un algoritmo de encriptación, y, por último, se presenta un sistema de respaldo de energía ante cortes eléctricos, así como también un respaldo ante la falla de la comunicación inalámbrica.

2.1 Esquema de diseño y construcción del dispositivo

El diseño del prototipo de cerradura electrónica conectada a una red WiFi cumple con los objetivos planteados en el proyecto de investigación, es por ello que, para su desarrollo se usa los métodos de observación y experimentación, es decir estrategias basadas en la experiencia, la práctica y el análisis de los hechos, con el fin de llegar a la solución eficaz del problema planteado.

El problema se divide en varios bloques muy bien estructurados, es decir pequeños problemas más sencillos, esto con la finalidad de lograr la completa resolución del problema principal de manera óptima y teniendo en cuenta que cada bloque lleva su tiempo de construcción.

En la figura 1-2 se muestra el esquema de las diferentes etapas en las que se basa el desarrollo del prototipo electrónico.

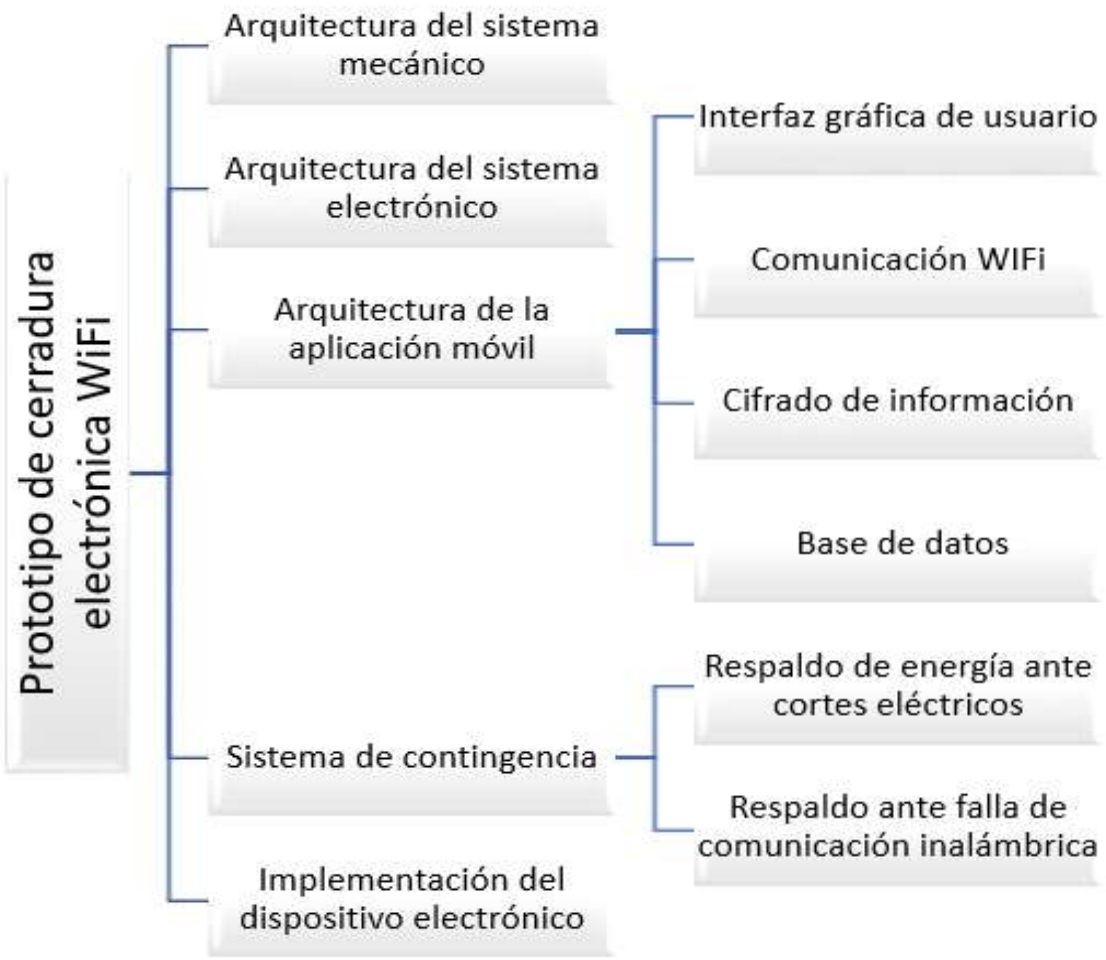


Figura 1-2: Etapas de desarrollo del prototipo
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

2.2 Arquitectura del sistema mecánico

En este bloque se detalla la elección de la cerradura colocada en la puerta y dos mecanismos fundamentales; los elementos necesarios que constituyen el mecanismo tanto para sacar los pestillos y seguros de la cerradura, y también para abrir o cerrar la puerta de forma automática.

2.2.1 Selección de la cerradura

Para seleccionar la cerradura se toma en cuenta principalmente el tipo de bombín que viene con la cerradura, el mismo que cuenta con un mecanismo interno que facilita realizar un giro de 360 grados, esto permite acoplar un sistema mecánico para controlar el giro completo de la cerradura con ayuda de un servomotor, además posee un sistema funcional óptimo, y el nivel de seguridad

alto debido al material que está construido. Para el desarrollo del proyecto se utiliza una puerta de madera. Y para mayor seguridad de elección, se realiza mediante una comparación de las mejores características que ofrecen entre tres tipos de cerraduras, entre ellas; de empotrar, de sobreponer y tubulares. En la tabla 1-2 se puede ver las características por las cuales de elige la cerradura de embutir.

Tabla 1-2: Elección de la cerradura de acuerdo a sus características.

Tipo de cerradura	Características
Cerradura de Sobreponer	- El mecanismo queda expuesto en uno de los lados de la puerta - Útiles en su mayoría para puertas exteriores de hierro y necesitan ser soldadas. - Es necesario encajar la llave para abrir desde el exterior y posee un tirador para abrir desde el interior
Cerradura Tubular	- El mecanismo queda expuesto en ambos lados de la puerta - Útiles en su mayoría para puertas interiores de madera o aluminio - Su seguridad radica en la pulsación de un botón incorporado - Son parecidas al uso de un picaporte - El cilindro para la llave se ubica dentro del pomo lo que la hace dependiente.
Cerradura de Embutir	- Todo el mecanismo se instala dentro de la puerta obteniendo una mayor protección fiabilidad y seguridad - No pueden ser forzadas fácilmente. -Pueden colocarse tanto para puertas interiores como exteriores independientemente del material de que estén construidas - Existen cilindros que se adaptan a las necesidades y son fácilmente intercambiables, incluso en algunos se puede abrir la puerta,

	aunque por accidente se deje la llave puesta por el interior. - El mecanismo interno del cilindro de la cerradura puede giran 360º para abrir o cerrar su pestillo y seguros adicionales. - Hay variaciones de esta cerradura en la que como principal característica es su seguridad como cerraduras multipunto y sistemas de bloqueo automático. - Su modelo posee manijas colocados en ambos lados de la puerta y son independientes del mecanismo del bombín de la cerradura.

Realizado por: Cuenca Sebastián, Manotoa Alex, 2017

2.2.2 Mecanismo para girar automáticamente el bombín de la cerradura

Una vez elegida la cerradura se procede al diseño del mecanismo que hace que el cilindro interior pueda girar completamente en un sentido u otro para abrir o cerrar, accionando el pestillo y retener o liberar los seguros de la cerradura. El mecanismo previamente se lo desarrolla en el software SolidWorks con se muestra en la figura 2.2, con la finalidad de visualizar claramente la mejor ubicación, componentes necesarios y movimiento del diseño simulado, para luego facilitar la construcción y finalmente convertirlo en un diseño real.

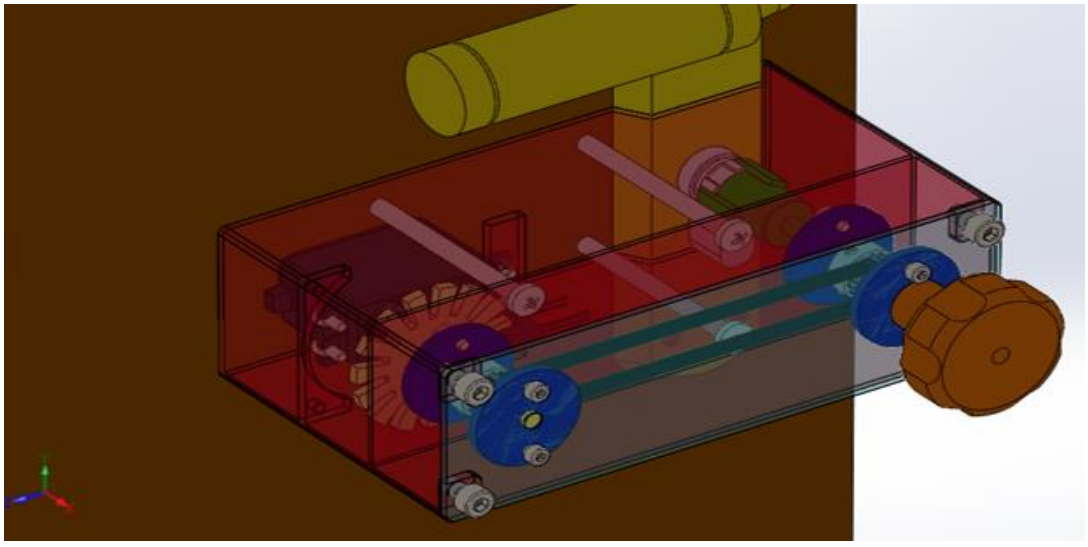


Figura 2-2: Diseño del mecanismo para el bombín de la cerradura en SolidWorks.
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Este diseño se compone de: un sistema de transmisión mecánica, un servomotor, un sensor de herradura, una rueda dentada, un acople para el bombín y una perilla como se muestra en la figura 3-2. Todos estos componentes se encuentran encapsulados en una caja de acero inoxidable para la instalación sobre la puerta.

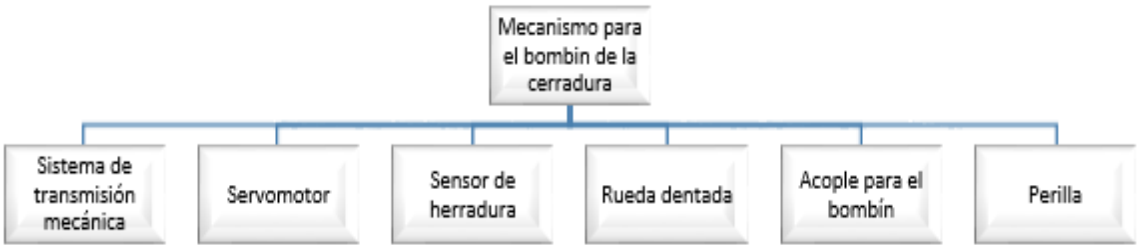


Figura 3-2: Elementos del mecanismo para el bombín de la cerradura
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

2.2.2.1 Sistema de transmisión mecánica

El proceso de construcción y parte del diseño del sistema mecánico del prototipo, se lo realizó mediante el principio de transmisión mecánica, es decir un conjunto de dos poleas ubicadas de forma paralela a una cierta distancia, acopladas por medio de una correa dentada con el fin de transmitir potencia desde un punto a otro, esta fuerza se transmite por el giro del motor sobre la polea ubicado en un extremo, ejerciendo un movimiento sobre la correa y finalmente transmitiendo la potencia generada sobre la polea del otro extremo.

Se debe recalcar que para el desarrollo se optó por la trasmisión por engrane pues este sistema hace uso de poleas dentadas y posee un acople de enlace flexible llamada banda dentada.

Componentes del sistema de transmisión

- **Polea motriz:** también llamada polea conductora, esta polea está sujeta al eje del servomotor el mismo que permite hacer girar la polea adquiriendo un movimiento propio.
- **Polea conducida:** esta polea es la que se encuentra anclada un eje al que deseamos generar el movimiento, en este caso al bombín de la cerradura empotrada.
- **Correa de transmisión:** son cintas cerradas de cuero y otros materiales que se emplea para transmitir el movimiento de rotación entre los dos ejes.

Calculo de la longitud de la correa de transmisión

Para saber que la longitud de la correa que se ajustará entre las dos poleas se aplica la fórmula:

Ecuación 1-2: Cálculo de longitud de la correa dentada

$$\boldsymbol{L = \frac{\pi}{2}(D + d) + 2C + \frac{(D - d)^2}{4C}}$$

Donde:

L= Longitud de la correa en mm.

D = Diámetro de la polea mayor.

d = Diámetro de la polea menor.

C = Distancia entre centros.

Entonces, con los datos conocidos se procede a obtener el dato numérico de la longitud de la correa. Se toma en cuenta el uso de un par de poleas dentadas iguales de modelo GT2-20T-5

Datos:

D = 1.3 cm, **d** = 1.3 cm, **C** = 11 cm

Aplicando la ecuación 1-2 se obtiene:

$$\boldsymbol{L = \frac{\pi}{2}(1.3cm + 1.3cm) + 2(11cm) + \frac{(1.3cm - 1.3cm)^2}{4(11cm)}}$$

$$\boldsymbol{L = 26.1\ cm}$$

La longitud de la correa dentada es de 26,1 cm.

Relación de las velocidades de transmisión por correa

Luego de obtener la banda, se verifica la velocidad que tendrá la transmisión mecánica con la siguiente ecuación:

Ecuación 2-2: Relación de velocidades entre poleas

$$\boldsymbol{D1 * N1 = D2 * N2}$$

Quedando así la relación de velocidades:

Ecuación 3-2: Variación de la relación de Velocidad entre poleas.

$$\boldsymbol{I = \frac{N1}{N2} = \frac{D1}{D2}}$$

Donde:

I= índice de velocidades.

D1: es el diámetro de la polea conductora.

D2: es el diámetro de la polea conducida.

N1: Velocidad de giro de la polea conductora.

N2: Velocidad de giro de la polea conducida.

Y aplicando la ecuación 3-2 se obtiene el índice de velocidades.

$$\boldsymbol{I = \frac{D1}{D2}} = \frac{1.3cm}{1.3cm} = \mathbf{1}$$

Como se puede apreciar, luego del cálculo, el resultado de la relación de velocidad da el valor de uno. Esto quiere decir que la velocidad trasmitida es idéntica en ambas poleas.

En la figura 4-2 se observa el mecanismo real con la instalación de las poleas y correa dentada

Figura 4-2: Componentes del sistema de transmisión mecánica
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

2.2.2.2 Servomotor

Para determinar el tipo de servomotor que se necesita para mover el mecanismo del bombín de la cerradura, que va junto con el sistema de trasmisión mecánica, se requiere el cálculo del torque necesario. Para lo cual colocó una palanca sobre el sistema mecánico como se puede ver en la figura 5-2, y para el cálculo de los parámetros en la ecuación 4-2.

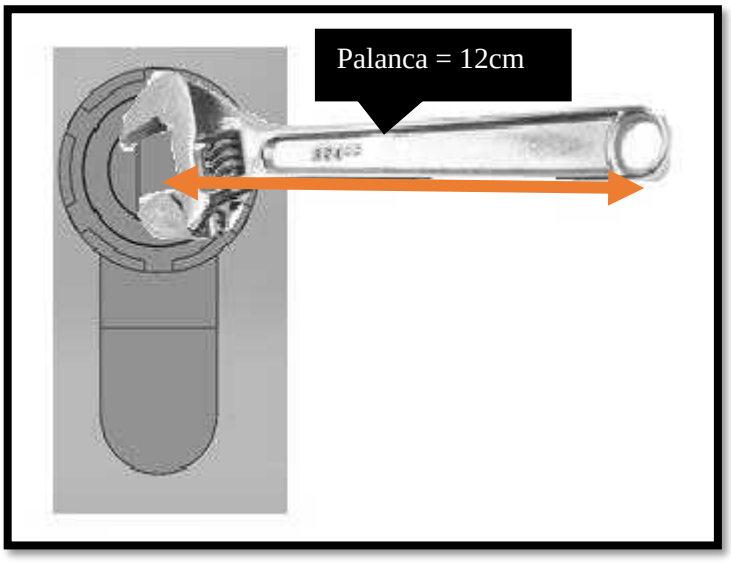


Figura 5-2: Palanca necesaria para calcular el torque de la cerradura.
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Ecuación 4-2: Torque

$$\boldsymbol{T = F * r}$$

Donde:

T= es el torque.

F= es la fuerza necesaria para mover el sistema.

r= es la medida que va desde el centro de giro, al punto donde se aplica la fuerza.

Para obtener el dato de la fuerza que se necesita para girar el bombín y que el pestillos y seguros salgan o se retengan en la cerradura, se usa una balanza portable que se sujeta a la palanca acoplada al bombín, entonces de estira la balanza obteniendo de esta manera el valor de 3 libras fuerza con un radio de 12cm.

Como en la hoja de datos de servomotores usualmente se tiene el dato de torque en $\boldsymbol{kg.cm}$ se procede a convertir las libras fuerza obtenida a kilogramos fuerza con la ecuación 5-2

Ecuación 5-2: Conversión de libras fuerza a kilogramos fuerza.

$$\boldsymbol{F = 1\ lbf * \frac{1\ kgf}{2.2\ lbf}}$$

$$\boldsymbol{F = 3\ lbf * \frac{1\ kgf}{2.2\ lbf}}$$

$$\boldsymbol{F = 1,36\ kgf}$$

y aplicando la ecuación 4-2 se tiene:

$$\boldsymbol{T = 1,36 kgf * 12 cm}$$

$$\boldsymbol{T = 16,32\ kgf.cm}$$

Dando un torque de $\boldsymbol{16,32\ kgf.cm}$ que es el necesario para mover el mecanismo.

De acuerdo a los cálculos mencionados anteriormente, se elige un servomotor que cumpla con los requerimientos que necesita el mecanismo. En la tabla 2-2 se aprecia las características del servomotor adquirido.

Tabla 2-2: Características del servomotor para el sistema de transmisión.

Características	Datos
Modelo	LD-3015MG
Torque	15 kg-cm con 6V 17 kg-cm con 7.4V
Tensión de alimentación	6V ~ 7.4V DC
Rango de operación	0º - 270º

Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Después de obtener el servomotor es necesario realizar una modificación o *trucar* al servomotor, para que de esta manera éste pueda realizar un giro continuo de 360º.

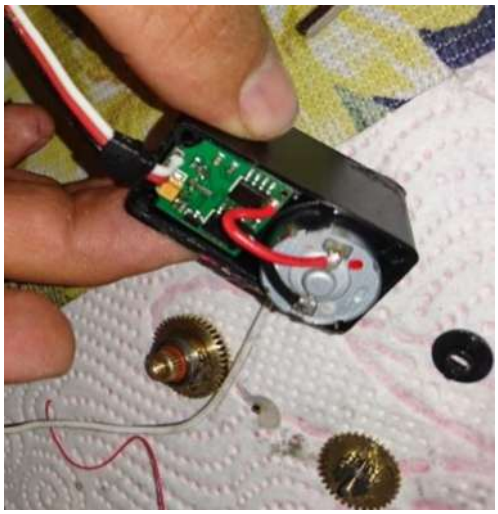


Figura 6-2: Trucado del servomotor de 17 Kg.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Una vez hecho esto, el servomotor a través del sistema de transmisión mecánica girará de manera continua el bombín y dependiendo del número de vueltas trasmitirá el torque para abrir o cerrar el pestillo y seguros de la cerradura implementada.

2.2.2.3 Sensor de herradura y rueda dentada

Es el sensor encargado ayudar a contabilizar las vueltas que dará el servomotor colocado sobre la chapa y también su correcta posición angular ya sea en un sentido u otro. Se coloca en medio de la rueda dentada dentro del mecanismo de la chapa de la cerradura. De esta forma contabiliza cada corte de la rueda de 15 dientes, lo que significa que se tiene 15 conteos en el sensor lo que equivale a una vuelta sobre la chapa.

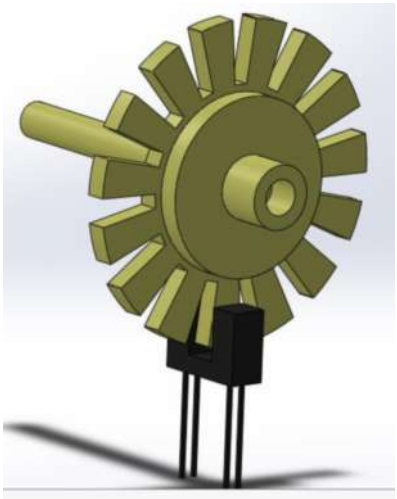


Figura 7-2: Rueda dentada y sensor
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.2.2.4 Acople para el bombín y perrilla

Para que exista un anclaje debido a la transmisión de movimiento, se coloca un acople en el bombín de 9 cm de longitud con tres terminales como se ve en la figura 7-2.

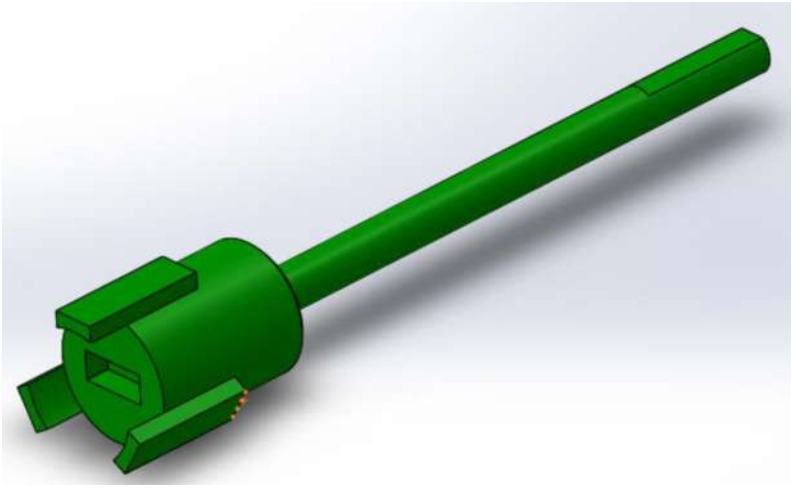


Figura 8-2: Acople para el bombín
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Este agarre activa el mecanismo de la cerradura y por el otro lado se sujeta una perilla, la que puede ser girada manualmente por el usuario según se requiera como se observa en la figura 8-2.

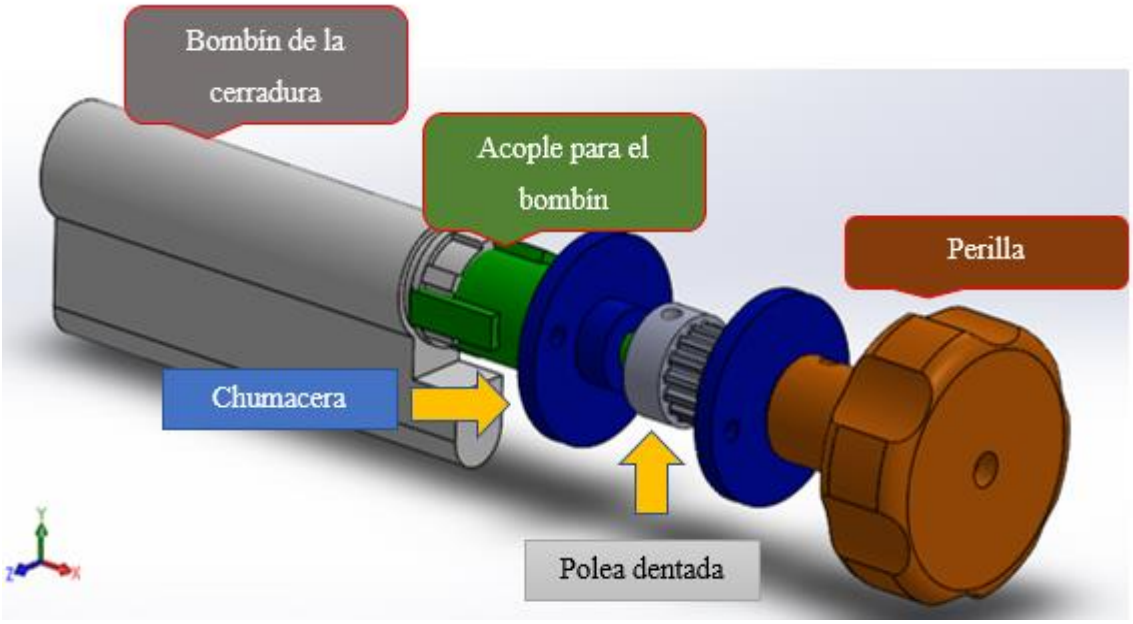


Figura 9-2: Acople para el bombín y perilla simulado
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Como se aprecia en la figura 9-2 constituye el mecanismo interno real construido.

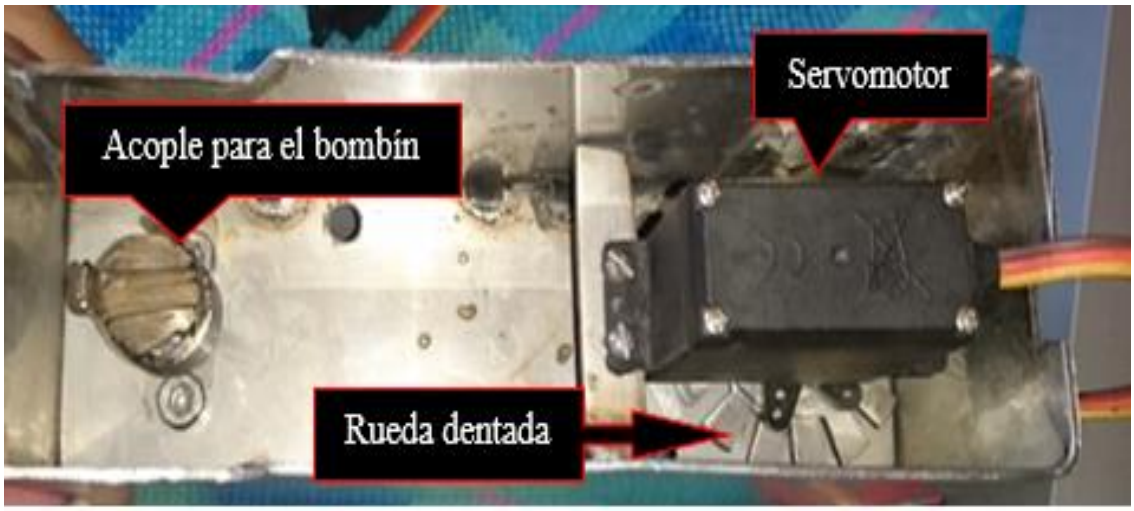


Figura 10-2: Estructura interna real del mecanismo que se acopla al bombín
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Y finalmente se instala la caja completa con todos los elementos del mecanismo sobre el bombín de la cerradura.

Figura 11-2: Mecanismo real instalado sobre el bombín de la cerradura
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

2.2.3 Mecanismo para la apertura y cierre automático de la puerta

El prototipo también tiene la finalidad de abrir y cerrar completamente la puerta de forma automática, es por ello que se realiza un modelo previo en el software SolidWorks como se observa en la figura 12-2 para visualizar el rango de operación, movimiento del diseño simulado, para luego facilitar la construcción y finalmente construirlo y convertirlo en un diseño real.

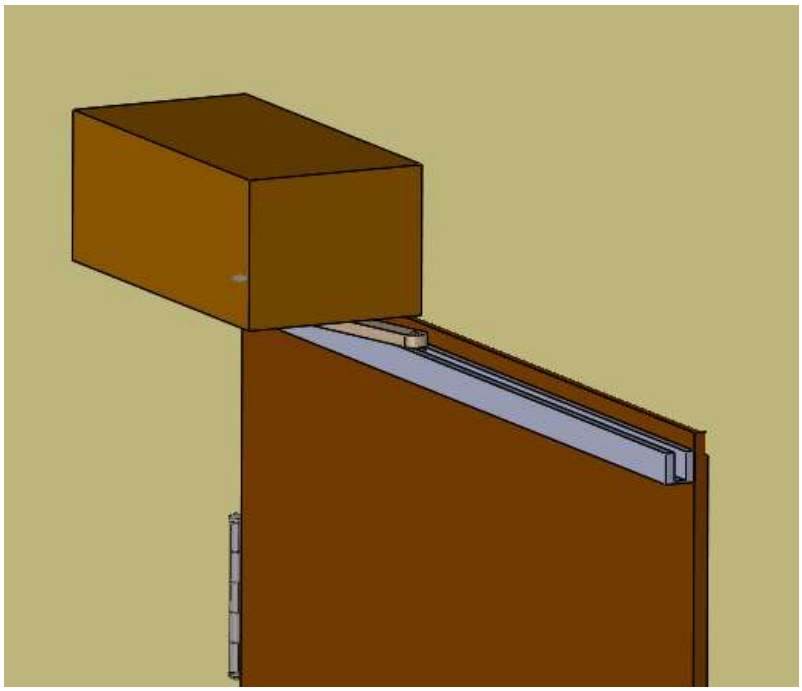


Figura 12-2: Diseño del mecanismo automático para la puerta en SolidWorks.
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Este diseño se compone de: un brazo mecánico, un rodamiento, un riel, y un servomotor como se muestra en la figura 12-2. Todos estos componentes se encuentran instalados en la parte superior de la puerta.

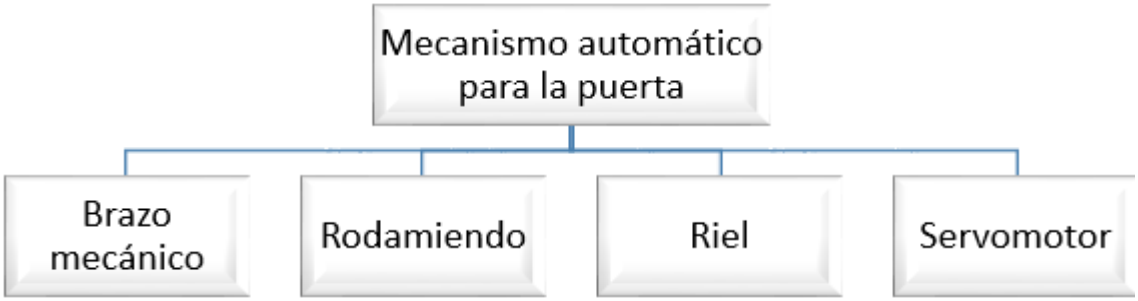


Figura 13-2: Elementos del mecanismo automático para la puerta.
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Para la construcción del mecanismo real, se usa un brazo mecánico de madera de un grado de libertad con una longitud de 20 cm. En un extremo circular se acopla al eje del servomotor, y por el otro extremo se coloca al eje de un rodamiento de puerta corrediza como se visualiza en la figura 14-2.

Figura 14-2: Rodamiento de puerta corrediza.
Fuente: http://www.grupoancor.es/ficheros/productos/317.jpg

Este rodamiento que se desliza en el interior y a lo largo de un riel que mide 50 cm de longitud facilitando que el brazo se extienda y así poder abrir o cerrar la puerta de forma autónoma. Todo el mecanismo real previo a la instalación se puede ver en la figura 15-2.

Figura 15-2: Parte del mecanismo automático para la puerta.
Fuente: http://www.grupoancor.es/ficheros/productos/317.jpg

2.2.3.1 Dimensionamiento del servomotor

Una vez obtenido los elementos necesarios, se debe dimensionar el servomotor a utilizar, ya que es el actuador encargado de abrir o cerrar completamente la puerta de forma automática, y es por ello que se requiere calcular el torque necesario para mover toda la puerta.
Se partió del principio de la ley de la inercia, la cual establece que "un cuerpo permanecerá en un estado de reposo (velocidad cero) o de movimiento rectilíneo a velocidad constante, siempre y cuando una fuerza externa neta no actúe sobre él." Con esta afirmación en la física, se puede asumir que la puerta siempre se mantiene en reposo a menos que exista algo que la mueva. (2010).

Entonces, para calcular la fuerza que se requiere para romper la inercia, se optó por una balanza portable que se colocó en el centro de la puerta. Las medidas de la puerta de madera empleada se detallan en la tabla 3-2.

Tabla 3-2: Dimensiones de la puerta

Parámetros	Altura	Ancho	Espesor
Valor	196 cm	81 cm	4 cm

Fuente: http://tienda.bricogeek.com/descatalogado/483-mini-pantalla-oled-128x64.html

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Una vez sujeta la balanza en el centro de masa de la puerta, se procede a estirar la balanza hasta que rompa la inercia y se abra completamente como se puede observar en la figura 16-2. Se obtiene el valor de ***1,2 Ibf*** que marca en la balanza**.**

Figura 16-2: Tomando el dato de la fuerza con una balanza
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Para saber la distancia de la palanca, se toma en cuenta desde el extremo de la puerta, hasta su centro como se muestra en la figura 17-2.

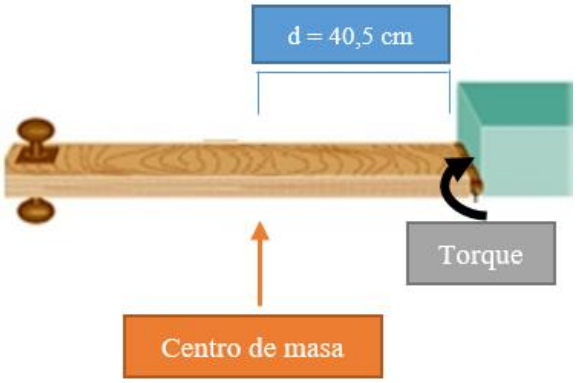


Figura 17-2: Distancia del centro de masa
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Luego aplicando la ecuación 4-2 para calcular el torque necesario para abrir toda la puerta.

$$\boldsymbol{T = F * d}$$

$$\boldsymbol{T = 1,2\ lbf * 40,5\ cm}$$

$$\boldsymbol{T = 48,6\ lbf.cm}$$

Se tiene el torque aplicado al extremo de la puerta para abrirla de $\boldsymbol{48,6\ lbf.cm}$

Una vez obtenido el valor del torque necesario para mover la puerta, se realiza el análisis del torque necesario que debe realizar el servomotor con el brazo para abrir o cerrar la puerta. El sistema instalado se visualiza en la figura 18-2.

Figura 18-2: Brazo mecánico real instalado
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Volviendo a redibujar el sistema visto desde la parte superior se tiene la figura 19-2.

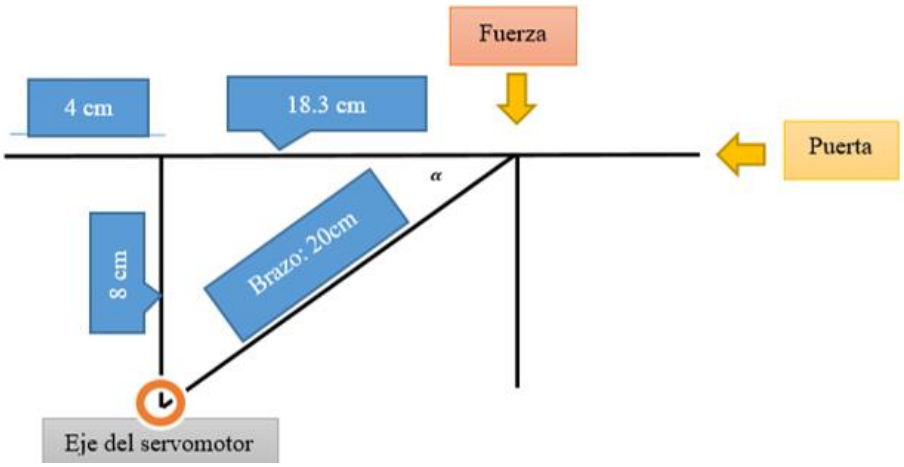


Figura 19-2: Componentes del brazo mecánico
Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

Teniendo todos los lados se procede a calcular el Angulo generado en el punto donde se genera la fuerza con la ecuación 6-2.

Ecuación 6-2: Calculo del ángulo generado.

$$\boldsymbol{\alpha = \tan^{-1}(\frac{cateto\ opuesto}{cateto\ adyacente})}$$

$$\boldsymbol{\alpha = \tan^{-1}(\frac{8\ cm}{18.3\ cm})}$$

$$\boldsymbol{\alpha = 23.6^{o}}$$

Y con los datos se procede calcular el torque que necesita el actuador para realizar la apertura y cierre de la puerta. Para el cálculo se aplica la definición de torque nuevamente con la ecuación 4-2 conociendo el torque que necesita la puerta en el anterior cálculo y se toma en cuenta la distancia total desde el extremo de la puerta para obtener la fuerza ejercida en el brazo.

$$\boldsymbol{T = F * r}$$
$$\boldsymbol{48.6\ lbf = F * (18.3\ cm + 4cm)}$$
$$\boldsymbol{F = \frac{48.6\ lb * cm}{22.3\ cm}}$$
$$\boldsymbol{F = 2.18\ lbf}$$

Pero, por la definición de torque en la que indica que la fuerza aplicada siempre debe ser perpendicular a la distancia, se realiza una descomposición en coordenadas de la fuerza obtenida con la ecuación 7-2.

Ecuación 7-2: Descomposición de la fuerza en el eje x

$$\boldsymbol{Fx = F * cos\ (\alpha)}$$

$$\boldsymbol{Fx = 2.18\ lbf * cos(23.6)}$$

$$\boldsymbol{Fx = 1.997\ lbf}$$

Como en la hoja de datos de servomotores usualmente se tiene el dato de torque en $\boldsymbol{kg.cm}$ se procede a convertir las libras fuerza obtenida a kilogramos fuerza con la ecuación 5-2

$$\boldsymbol{F = 1\ lbf * \frac{1\ kgf}{2.2\ lbf}}$$

$$\boldsymbol{F = 1.997\ lbf * \frac{1\ kgf}{2.2\ lbf}}$$

$$\boldsymbol{F = 0.91\ kgf}$$

Calculando el torque necesario en el eje del servomotor.

$$\boldsymbol{T = Fx * r}$$

$$\boldsymbol{T = 0.91\ Kgf * 20\ cm}$$

$$\boldsymbol{F = \ 18.2\ kgf.cm}$$

Dando un torque de $\boldsymbol{18,2\ kgf.cm}$ que es el necesario para mover toda la puerta.

De acuerdo a los cálculos mencionados anteriormente, se elige un servomotor que cumpla con los requerimientos que necesita el mecanismo. Tal es el caso del servomotor adquirido como se aprecia en la figura 20-2.

Figura 20-2: Servomotor de 20 kg.
Fuente: http://www.chd.hk/Product_Detail.aspx?id=142

En la tabla 4-2 se aprecia las características del servomotor adquirido.

Tabla 4-2: Servomotor para la apertura y cierre automático de la puerta.

Características	Datos
Modelo	LF-20MG HD
Torque	16,5 kg-cm con 4V 20 kg-cm con 6V
Tensión de alimentación	4,8V ~ 6,6V DC
Rango de operación	0º - 180º

Realizado por: Sebastián, Cuenca; Alex, Manotoa; 2017

2.3 Arquitectura del Sistema Electrónico

El prototipo de cerradura electrónica WiFi, dispone de un sistema de control que se realiza por medio del módulo NodeMCU, en el cual se conectan el resto de elementos electrónicos ya sea de entrada como de salida, para la realización de funciones específicas. Este microcontrolador es el encargado de recibir las instrucciones que provienen de la aplicación móvil y las procesa.

En la figura 20-2, se muestra el diagrama de la respectiva conexión del sistema electrónico.

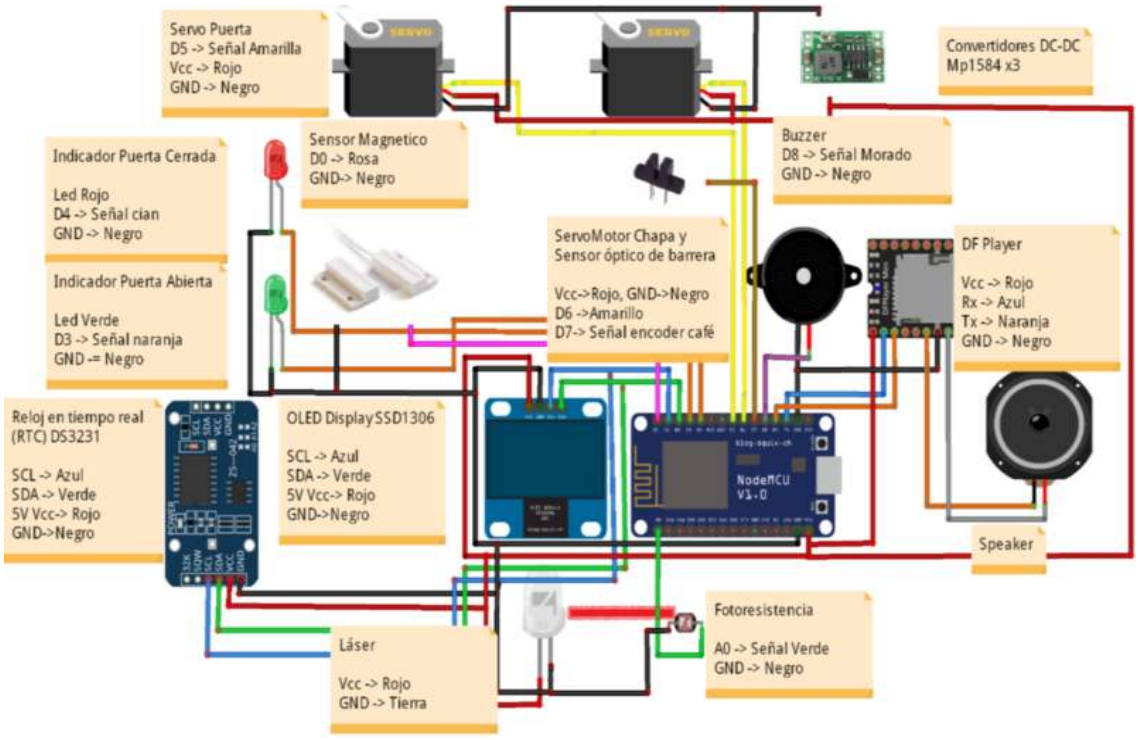


Figura 21-2: Esquema del sistema electrónico de control
Realizado por Sebastián, Cuenca; Alex, Manotoa; 2017

2.3.1 NodeMCU como dispositivo de control y comunicación WiFi

Como se ha mencionado antes, para el diseño del sistema se ha elegido un módulo *NodeMCU 1.0* como el "cerebro" de la cerradura electrónica. Está basado en el procesador ESP8266-12E, puesto que con este pequeño microcontrolador se puede realizar cualquier sistema para el Internet de las cosas (IoT) en cuestión de horas. Puede ser reprogramado según las necesidades del usuario mediante un conector micro USB, se lo encuentra a bajo costo en el mercado y sobre todo es *open-source*.

2.3.1.1 Instalación del módulo NodeMCU

La placa NodeMCU incorpora un chip necesario para la comunicación USB hacia cualquier PC. Entonces es necesario instalar el controlador dentro del computador para que de esta forma el sistema operativo pueda reconocer a la placa cada vez que sea conectada.

Cuando se conecta la tarjeta por primera vez al equipo en algunos de los casos y dependiendo del sistema operativo en el que se trabaje, los drivers se instalan automáticamente y no es necesario ningún procedimiento adicional puesto que la conexión se realiza dentro de una PC con Windows 10 Pro de 64bits.

Figura 22-2: Información del sistema operativo.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.1.2 Instalación de drivers necesarios

En el caso de que no se instalara correctamente el paquete de software, el driver necesario de la placa NodeMCU se puede descargar en el siguiente link oficial:

https://github.com/nodemcu/nodemcu-devkit

Seguidamente, se descomprime se ubica una ruta y en el administrador de dispositivos se da clic en actualizar el controlador.

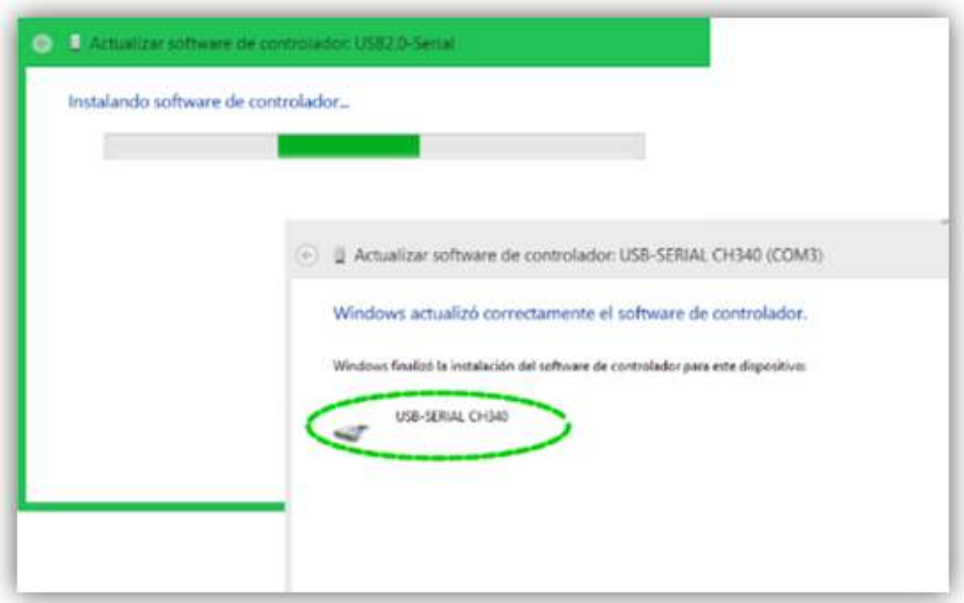


Figura 23-2: Instalación del driver
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.1.3 Instalación del firmware

En muchos de los casos el firmware (equivalente a la bios de cualquier PC), que es una clase de software de más bajo nivel que permite controlar el hardware (comunicaciones, pines de entrada y salida del NodeMCU), no viene cargado correctamente o se encuentra desactualizado, es por ello que se recomienda realizar un proceso de *flashing* que vendría a ser la programación del procesador interno del módulo ESP8266. Es necesario descargar los elementos almacenados en los siguientes enlaces:

- **NodeMCU Flasher (Software):** https://github.com/nodemcu/nodemcu-flasher

- **NodeMCU Firmware** (nodemcu_float_0.9.6 dev_20150704.bin)

https://github.com/nodemcu/nodemcu-firmware/releases

Acto seguido se abre el programa *ESP8266Flasher.exe*, dentro de la pestaña *Config*. Clic sobre el botón de engrane. Y se coloca el archivo *nodemcu_float_0.9.6-dev_20150704.bin*

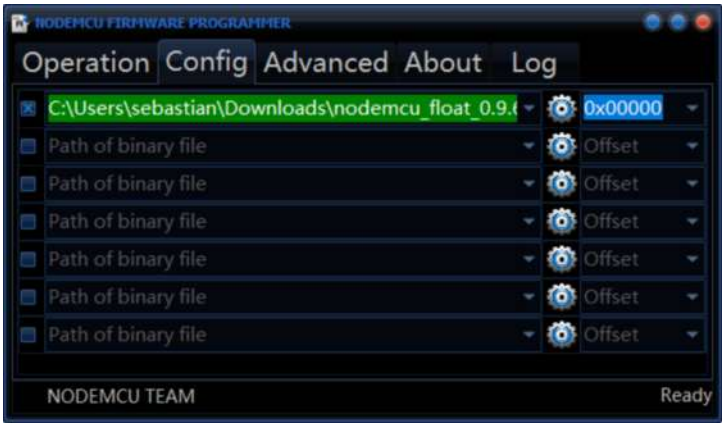


Figura 24-2: ESP8266Flasher.exe
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Se regresa a la pestaña *Operation*, donde se ubica el puerto COM correspondiente del NodeMCU. Se da clic en el botón *Flash(F)*, y se espera a que se complete la operación.

Figura 25-2: Proceso de Flashing NodeMCU
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Con esto, al programar en la interfaz de Arduino, la tarjeta responderá muy bien a cada línea de instrucción que se le asigne, así como también a una buena compatibilidad con los módulos conectados en la placa de desarrollo.

2.3.1.4 Compatibilidad con Arduino IDE

Para realizar la programación dentro del software de Arduino es recomendable tener la última versión del programa que puede ser descargado en su página web oficial. Puede ser descargado en el siguiente link https://www.arduino.cc/en/main/software, puesto que siempre está en constante actualización de versiones, pudiendo elegir tanto una versión de instalación o portable.

Luego, para instalar la placa NodeMCU conjuntamente con sus librerías para la respectiva comunicación WiFi es necesario dirigirse a la siguiente dirección web,

https://github.com/arduino/Arduino/wiki/Unofficial-list-of-3rd-party-boards-support-urls en el cual se encuentran las placas basadas en el ESP8266.

Figura 26-2: Descarga de placas basadas en ESP8266.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Copiar el link, ingresar al Arduino IDE, en la barra de herramientas seleccionar la pestaña *Archivo*, luego en *Preferencias*, y pegar el enlace en donde se indica en la figura 27-2.

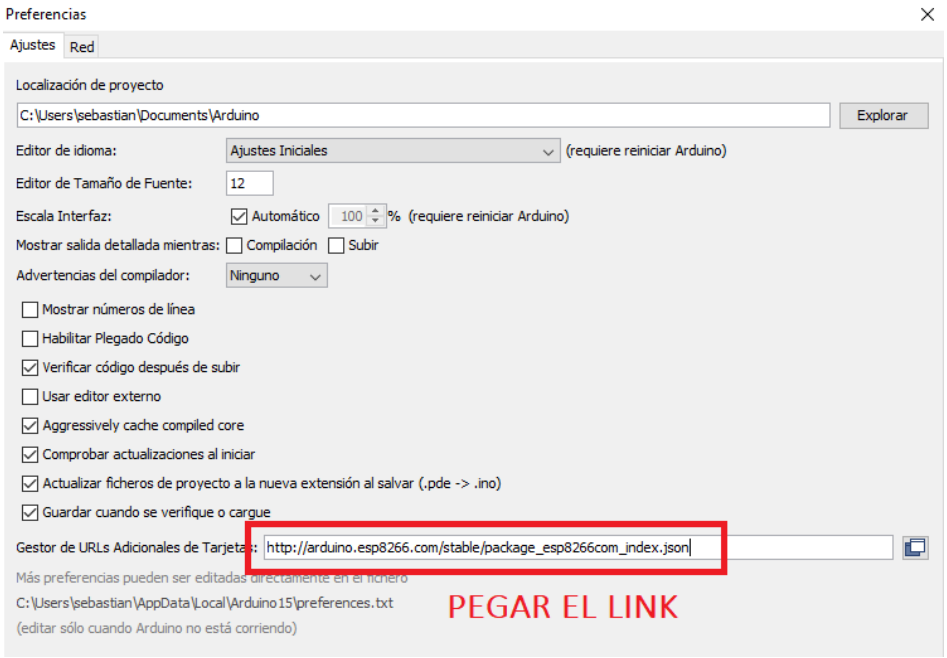


Figura 27-2: Link necesario para realizar la comunicación
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Una vez hecho esto, dirigirse a la pestaña *Herramientas*, luego en Gestor de tarjetas y dentro del buscador, escribir *"esp8266*" e instalar

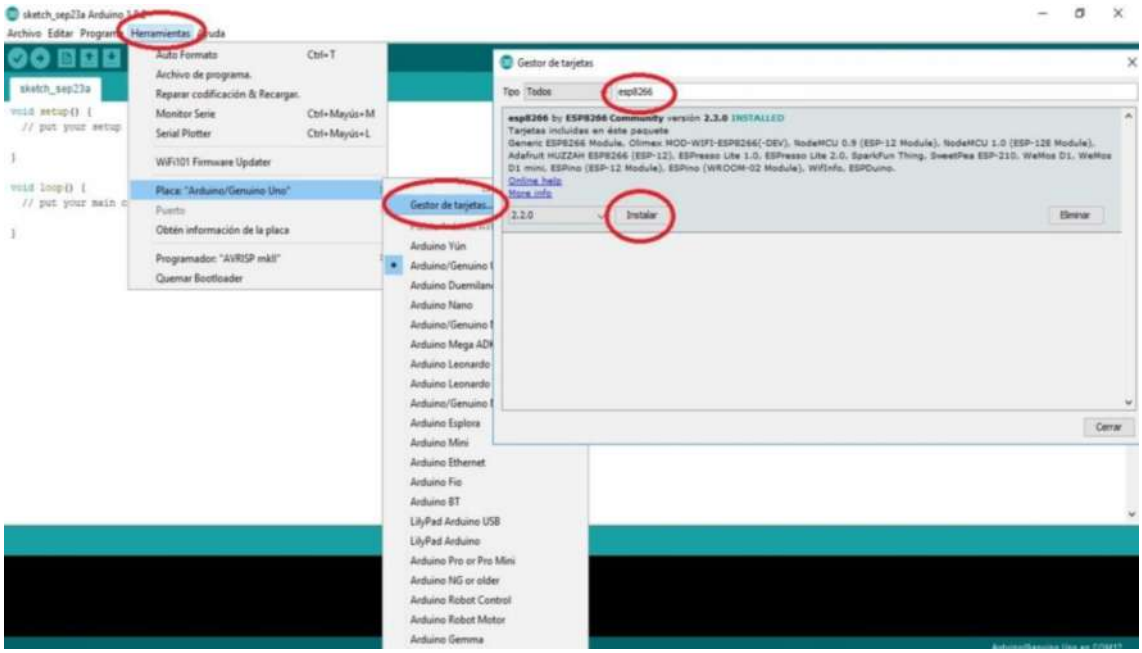


Figura 28-2: Pasos para la instalación
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Luego de esto, reiniciar el Arduino IDE. Se selecciona la tarjeta NodeMCU en el selector de tarjetas sobre *NodeMCU 1.0 (ESP-12E Module)* que es compatible con la tarjeta *V2* que es la utilizada para el proyecto. Luego seleccionar el puerto al que está conectado el módulo y entonces con todos los pasos realizados antes, el software quedará listo para realizar la programación del módulo NodeMCU dentro de esta interfaz.

2.3.2 Servomotores para el movimiento de los mecanismos

Son los actuadores que producen la fuerza necesaria para permitir que tanto la chapa como la puerta se abran o cierren dependiendo de los requerimientos del usuario como se explica en la construcción del sistema mecánico.

2.3.3 Funcionamiento del display OLED SSD1306

Este módulo se encarga de presentar en pantalla el detalle de la fecha y hora en tiempo real, verificando el horario de apertura y cierre en los días de la semana programados, cuando se configure desde la aplicación móvil. Muestra en forma de texto el estado actual de la puerta ya sea abierta o cerrada. Como se muestra en la figura 29-2. También se encarga de mostrar el código ID de un dispositivo NFC al momento del registro.

Figura 29-2: Funcionamiento de pantalla OLED SSD1306
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.4 Funcionamiento del RTC DS3231

El DS3231 es un reloj de tiempo real de baja potencia, caracterizado por la comunicación I2C, se puede incorporar una pila de litio de 3.6V para que cuando se desenergice el sistema, y mantenga correctamente configurada la hora y fecha.

Su función dentro del prototipo es el de llevar la cuenta de tiempo en segundo en el que se tiene que mantener la puerta abierta debido a que desde la aplicación móvil se presiona el botón de *Apertura Temporal*, o también cuando se presente una llave electrónica *NFC* en la puerta, ésta proceda a su cierre automático luego del tiempo programado (30 segundos).

Otra de las principales funciones es llevar la hora en tiempo real del día para que el microcontrolador haga una comparación de la hora y fecha actual, con la hora y fecha recibida desde la aplicación móvil para que, al instante en el que el usuario programe un horario de apertura y cierre, la puerta pueda realizar las acciones respectivas.

2.3.5 DFplayer mini para dotar de voces al sistema

Este módulo reproductor de audio mp3, permite reproducir voces pregrabadas con el fin de informar las acciones que se están ejecutando sobre la puerta de inmediato. Dentro de las funciones que informa son cuando existe señales de: *error, registro de llaves electrónicas, la activación y desactivación de la programación de apertura y cierre de la puerta, indicador de encendido del sistema, y las acciones cuando la puerta cambie de estado de abierta a cerrada* y viceversa. Permitiendo de este modo tener un mayor grado de interactividad con el usuario.

2.3.6 Buzzer como elemento de notificación

Es un componente utilizado como notificación de audio sobre: *la alerta de activación, desactivación de la programación de apertura y cierre, la pulsación de botones desde la aplicación móvil en las acciones que se realicen sobre la cerradura electrónica*, además como un indicador de: *encendido del sistema, y las peticiones requeridas al momento de que la puerta cambie de estado de abierta a cerrada o viceversa.*

2.3.7 Calibración de sensores

2.3.7.1 Instalación del sensor magnético

El sensor magnético colocado en la parte superior de la puerta, es en encargado de verificar el estado de la puerta, si se encuentra abierta o cerrada y enviar esa información a la aplicación móvil desde el módulo WiFi. Puesto que este sensor se le puso una resistencia *pull down*, entonces cuando el sensor este separado, el microcontrolador detectará un estado *LOW* o *cero,* sobre el pin de entrada, y, por el contrario, cuando el sensor esté unido, el microcontrolador detectará un nivel *HIGH* o uno sobre el pin de entrada.

Figura 30-2: Sensor magnético colocado en la puerta
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.8 Instalación de fotorresistencia y láser

Este sensor colocado en el marco inferior lateral de la puerta, está ubicado a 50cm desde el suelo. Se encarga de verificar la cantidad de luz emitida por un rayo láser que proviene desde el otro extremo, lo que permite saber si alguien corta el haz de luz al momento de que la puerta se esté cerrando, permita detener la acción de cierre y procederá a abrir la puerta nuevamente.

Figura 31-2: Ubicación del Láser (izquierdo) y fotorresistencia (derecha) en la puerta
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.9 Instalación de los indicadores Led del sistema

- **Led rojo:** Advierte que la puerta está cerrada por completo.

Figura 32-2: Indicador de puerta cerrada
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

- **Led verde:** Advierte que la puerta está abierta.

Figura 33-2: Indicador de puerta abierta.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.3.10 Alimentación del circuito electrónico con fuentes conmutadas (Mp1584)

Para llevar una correcta alimentación del sistema se usaron convertidores DC-DC, una fuente switching de reducido tamaño y bajo costo capaz de dotar al sistema los voltajes y corrientes estables necesarios para el correcto funcionamiento de los componentes electrónicos.

Para el proyecto se usaron un total de tres fuentes conmutadas:

- Para la alimentación del NodeMCU y demás componentes. La fuente está regulada en $V_{out}=5V_{cc}$

- Para la alimentación del servomotor que gira el bombín de la cerradura. La fuente está regulada en $V_{out} = 7.3V_{cc}$
- Para la alimentación del servomotor que abrirá y cerrará por completo la puerta de forma automática. La fuente está regulada en $V_{out} = 6.4V_{cc}$

2.4 Diseño de la aplicación móvil

La aplicación móvil constituye también un pilar fundamental del prototipo, puesto que el objetivo de la aplicación es la de ofrecer al usuario una interfaz gráfica llamativa y multifuncional que pueda ser manejada de una manera sencilla y didáctica para realizar las funciones de apertura y cierre de la puerta de forma automática.

El proceso de diseño y desarrollo del software, se lo realizó en Android Studio, que puede ser instalada en dispositivos móviles que cuenten con sistemas operativos del mismo tipo.

En la figura 34-2 se presenta los bloques principales y funciones que realiza la aplicación sobre el control del dispositivo electrónico

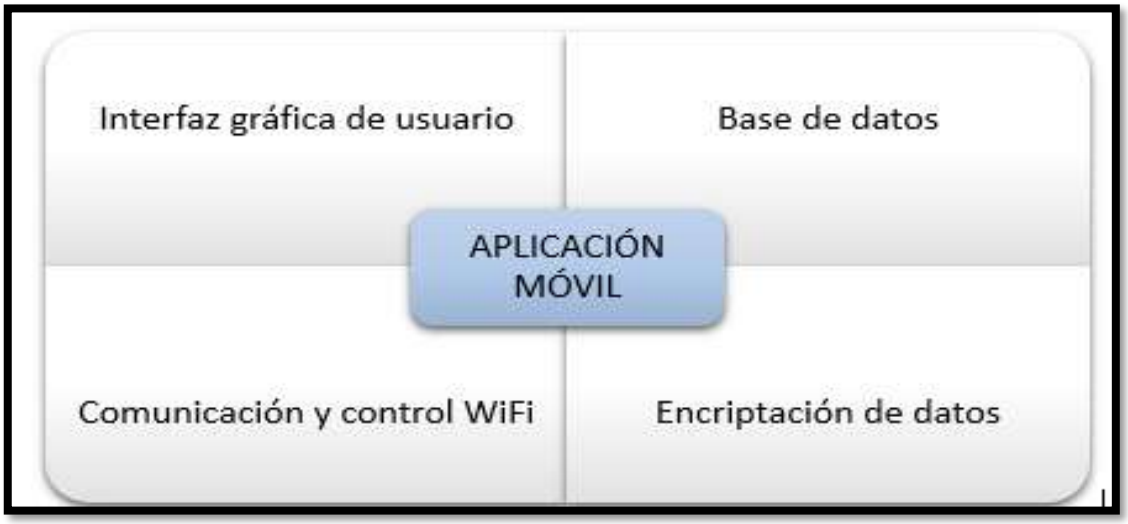


Figura 34-2: Bloques que conforman la aplicación móvil
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.1 Desarrollo de la interfaz gráfica de usuario

En este bloque se presenta la forma como están diseñadas las diferentes pantallas que interactúan con el usuario y la función de cada una de ellas. La aplicación se desarrolló en la versión API 5.0 Lollipop.

2.4.1.1 Interfaz Login

De acuerdo a la figura 35-2, se muestra la pantalla principal de la aplicación móvil en donde aparecen dos campos a llenar. Como medio de seguridad se tienen: *Correo Electrónico* y *Contraseña*, esto quiere decir que el usuario deberá previamente tener una cuenta registrada en la base de datos de la nube para poder acceder al control principal de la cerradura electrónica.

Figura 35-2: Pantalla Login de la app
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.1.2 Interfaz menú principal

Completados los pasos anteriores, la aplicación redirige al nuevo usuario automáticamente hacia la pantalla principal de la aplicación móvil en donde según la figura 36-2 se pueden visualizar diferentes secciones de control que influirán sobre el comportamiento de la cerradura electrónica, deslizando el menú lateral de izquierda a derecha.

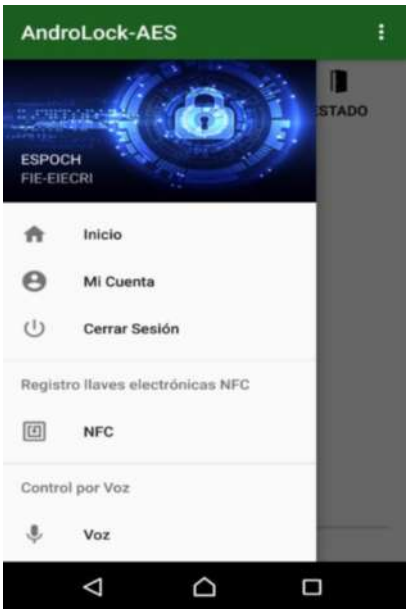


Figura 36-2: Barra lateral de la app
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.1.3 Interfaz pantalla inicio

Al pulsar sobre el menú lateral el botón *Inicio*, se presenta una pantalla de control, la cual se divide en tres diferentes pestañas o *Fragments* que a continuación de detalla cada una de sus funciones.

2.4.1.3.1 Modo manual

En esta pestaña llamada Apertura Manual como se indica en la figura 37-2, se tiene una imagen de un candado que representa a la cerradura electrónica en estado Cerrado. Cuando se pulse sobre la imagen, el candado se abre y a continuación empieza la secuencia respectiva hasta que la puerta se abra de forma automática, permitiendo así, dar acceso a los usuarios hacia el interior del laboratorio.

Cabe mencionar que la puerta se mantiene abierta de forma permanente, a menos que, si se mantiene pulsada la imagen nuevamente, está cambia de estado y de este modo enviará una señal de instrucción al módulo Wifi para realizar la secuencia respectiva que hace que la puerta se cierre completamente y de forma permanente.

Figura 37-2: Pestaña Control Manual
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.1.3.2 Modo automático

Deslizando la pantalla de derecha a izquierda, se cambiará a la pestaña siguiente en donde de acuerdo a la figura 38-2 se tendrán dos secciones: *Apertura Temporal* y *Apertura Programada*.

En la primera sección, se dispone de un botón, entonces si se mantiene presionado dicho botón, dará una instrucción al NodeMCU, la cual consiste en que realizará una secuencia hasta que la puerta quede abierta completamente. Luego, internamente gracias el módulo RTC DS3231 mencionado en la sección anterior, se iniciará un contador de *30 segundos*, en los cuales, terminado esa cuenta, el dispositivo electrónico nuevamente realizará la secuencia respectiva, permitiendo de este modo volver a cerrar la puerta completamente.

Se aclara que, por motivos de seguridad y gracias a una barrera óptica ubicada en los laterales del marco de la puerta, conformada principalmente por un láser y una fotorresistencia (LDR). Al momento de que la puerta se está cerrando, si fuera el caso en que una persona al querer pasar dentro de la habitación, corta dicha barrera láser. La puerta interrumpirá la acción de cerrado y procede en la posición que está, a volver abrirse por *15 segundos* más, y luego de terminada la cuenta, volverá a iniciar el proceso de cerrado.

Figura 38-2: Pantalla de apertura automática.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.1.3.3 Estado de la puerta

En este *Fragment*, se recibe constantemente la señal que el módulo wifi envía mediante la lectura de un sensor magnético colocado en la puerta para comprobar el estado de la misma. Se tienen tres posibles casos.

- **Indicador Blanco:** Señala que no existe comunicación entre el Smartphone y la cerradura electrónica, o a su vez indica que el dispositivo se encuentra apagado.

Figura 39-2: Pestaña del estado de la puerta
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

- **Indicador Rojo:** Señala que la puerta se encuentra cerrada completamente.

Figura 40-2: Indicador puerta Cerrada
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

- **Indicador Verde:** Señala es estado de la puerta que está abierta.

Figura 41-2: Indicador puerta Abierta
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

2.4.2 Comunicación WiFi entre dispositivos.

2.4.2.1 Modo de operación WiFi

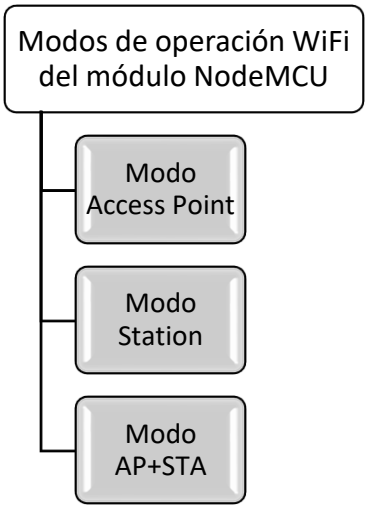


Figura 42-2: Etapas de la comunicación wifi
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

La tarjeta de desarrollo NodeMCU posee tres modos de operación WiFi y de acuerdo a las necesidades de la aplicación que se requiera, se debe configurar correctamente para que actúe de una forma u otra. Entre los modos de operación se tiene:

- **Access Point (AP)**

  El módulo NodeMCU se configura en modo *Punto de Acceso* en la cual se crea una red WiFi de área local (WLAN). En este modo, la tarjeta crea una clave de acceso (password) y un SSID (service set identifier), es decir un nombre de red que se visualiza sobre los dispositivos WiFi clientes. En este modo el módulo se comporta como un router virtual gracias a una cierta configuración que se realiza por software interna.

  Por defecto, los parámetros de fábrica de la dirección IP funcionando en este modo es 192.168.4.1. la cual sirve para conectarse con cualquier dispositivo cliente. Se asigna direcciones IP por DHCP (Dynamic Host Configuration Protocol) a los dispositivos conectados a partir de la dirección IP 192.168.4.2.

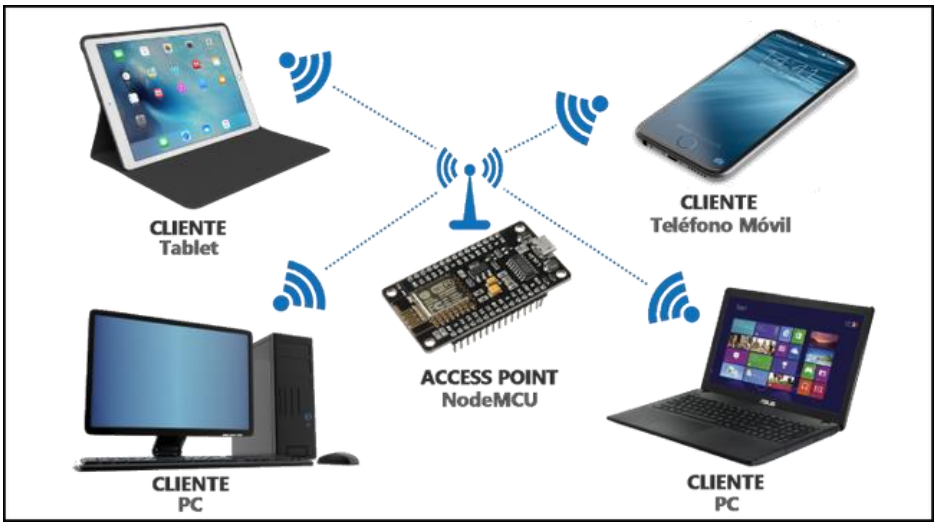


Figura 43-2: Sistema de comunicación punto de acceso.
Fuente: http://www.esploradores.com/access-point-servidor-web-nodemcu/

- **Mode Station (STA):** El módulo NodeMCU se configura en modo *Estación***,** es decir se conecta a un punto de acceso que puede ser: un router, módulos ESP8266, etc. De esta forma, el dispositivo queda integrado en la red WiFi como cliente, pudiendo así interactuar directamente con el resto de dispositivos conectados.

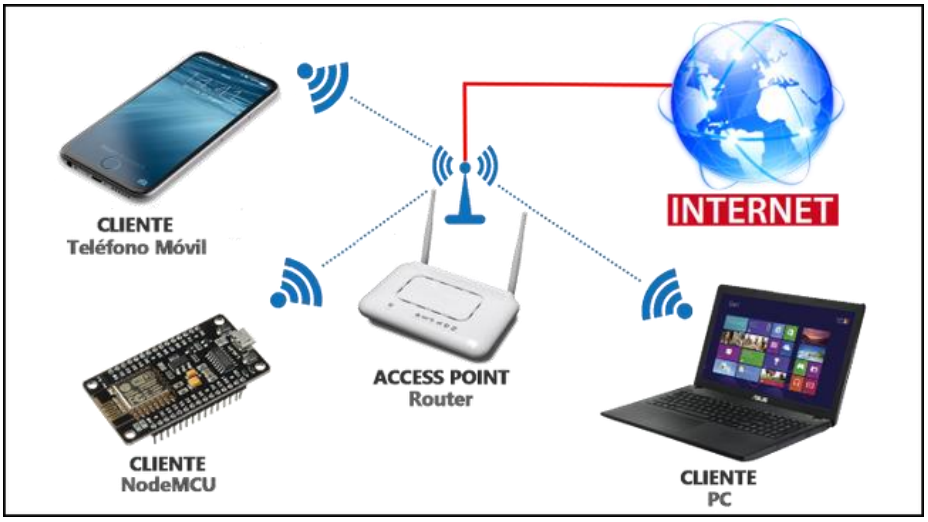


Figura 44-2: Comunicación en modo estación.
Fuente: http://www.esploradores.com/practica-3-station-conexion-con-access-point/

- **Modo AP+STA:** El módulo NodeMCU se comporta como una combinación de los dos casos anteriores.

Para el desarrollo del prototipo, el NodeMCU trabaja en modo estación, ya que, de esta manera cualquier dispositivo conectado a Internet puede acceder a la tarjeta de desarrollo a través del router.

2.4.2.2 Comunicación WiFi entre Aplicación Móvil y NodeMCU

Para lograr que el dispositivo electrónico tenga una comunicación inalámbrica, es necesario la intervención principalmente de las capas II, III, y IV del modelo OSI, se usa este modelo para mejor entendimiento teórico de cómo se realiza la conexión de red y la relación con los respectivos protocolos. Gran parte del trabajo para la configuración de red necesaria lo realiza el router dado por el proveedor de internet (ISP).

2.4.2.2.1 Mapeo de puertos

El mapeado de puertos (Port Forwarding), consiste en permitir que una petición que proviene de Internet llega a la dirección IP pública del router y por un puerto específico, sea encaminada a un equipo en concreto de la red LAN, en este caso el dispositivo es el módulo NodeMCU. Es necesario mapear puertos solo cuando se ejecuten aplicaciones con funciones de servidor.

Como se ve en la figura 44-2 se explica de forma gráfica como un cliente realiza una petición y llega hasta el dispositivo en particular a través de un router y un puerto asignado.

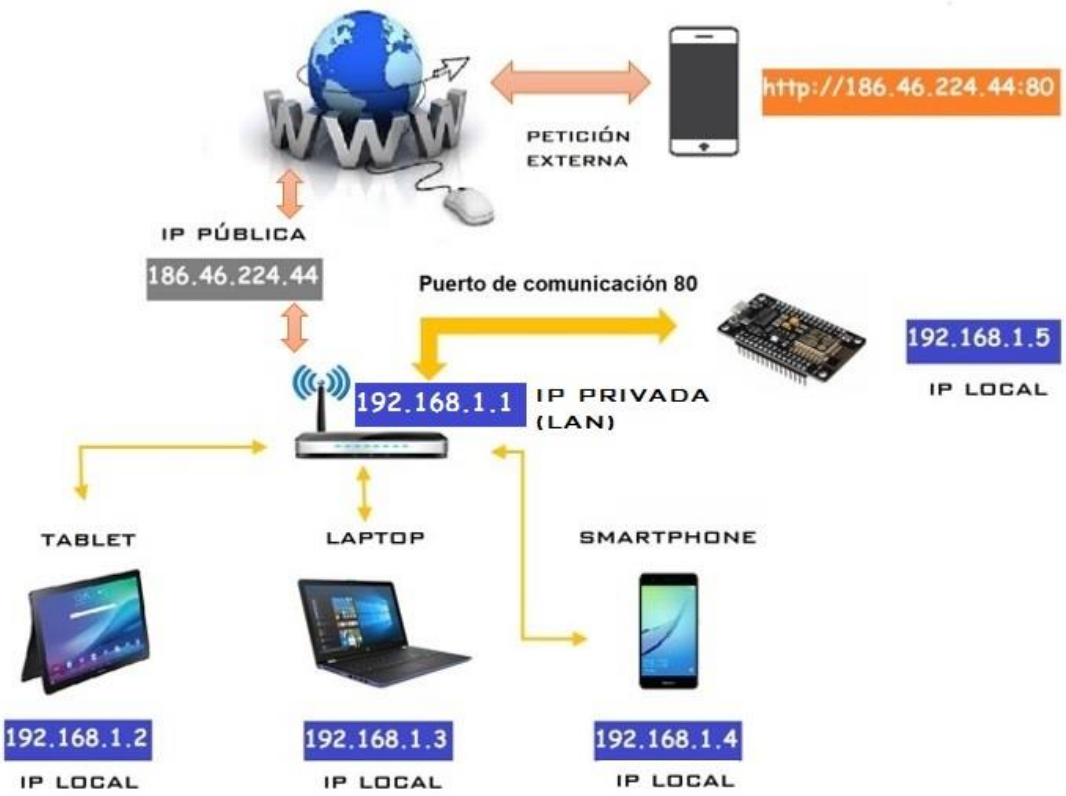


Figura 45-2: Peticiones desde internet a través del puerto de comunicaciones
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

La petición hecha por un cliente desde internet, se dirige por la IP publica 186.46.224.44 perteneciente al router y se dirige por la red local a través del puerto de comunicaciones 80 relacionado con el protocolo *HTTP* de páginas web. Entonces la petición finalmente llega a la dirección IP 192.168.1.5 a la que está asignado el módulo NodeMCU.

Para el mapeado de puertos, cada modelo de router de acuerdo a su fabricante, tiene un procedimiento específico, por lo que hay que buscar la documentación específica para poder realizar este procedimiento.

Para el desarrollo del proyecto se usa un router HG110 ADSL proporcionado por la compañía CNT de Ecuador que dota el servicio de internet y que actúa como punto de acceso para conectar el prototipo a la red local.

Pasos abrir puertos en el router

- Acceder al router a través de un navegador Web de un dispositivo conectado a la *red local*. La dirección de acceso por defecto es 192.168.1.1. En la pantalla inicial se debe introducir el nombre de usuario y contraseña que proporciona el proveedor del servicio de Internet.

Para tener acceso como administrador se coloca en el campo

Account: *instalador*

Password: *corporacion*

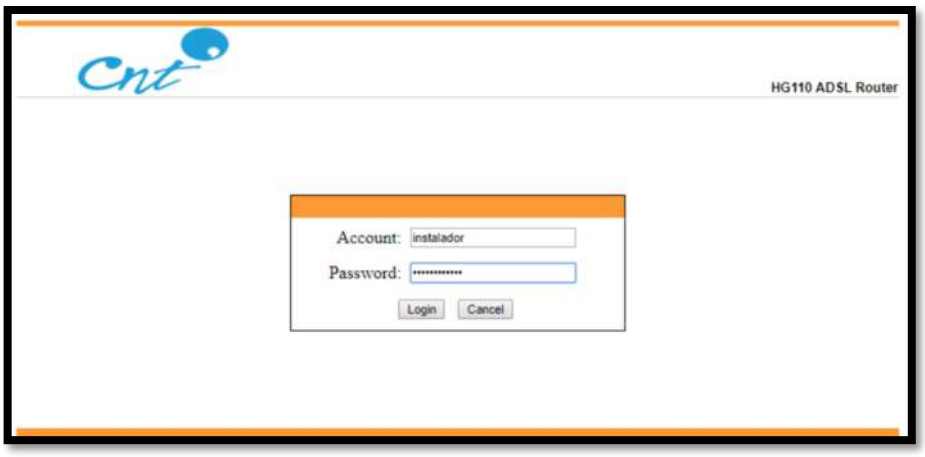


Figura 46-2: Acceso a la configuración del router
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

- Dirigirse a la pestaña *Advanced Setup*, seleccionar la subpestaña *NAT* y clic sobre *Virtual Server* como se muestra en la figura 46-2.

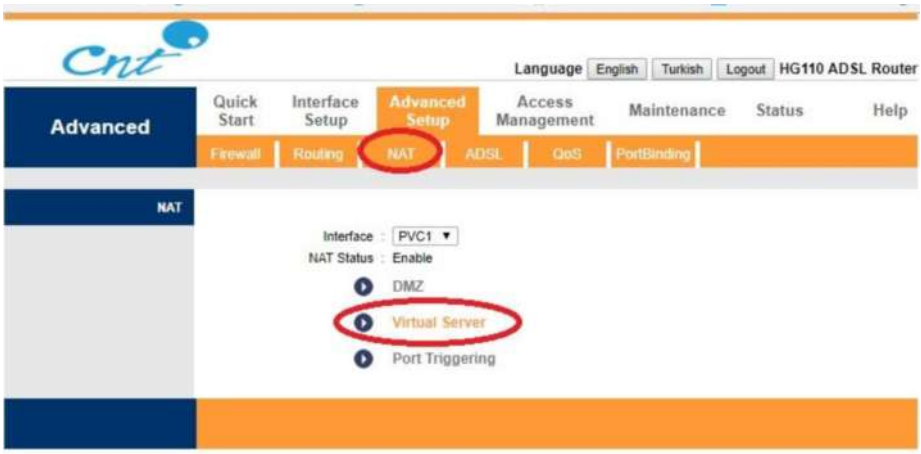


Figura 47-2: Pestaña de abertura de puerto
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

- Como se muestra en la figura 47-2, se coloca el puerto de comunicaciones y la dirección IP local que el router reservada para el módulo WiFi que es la dirección 192.168.1.5

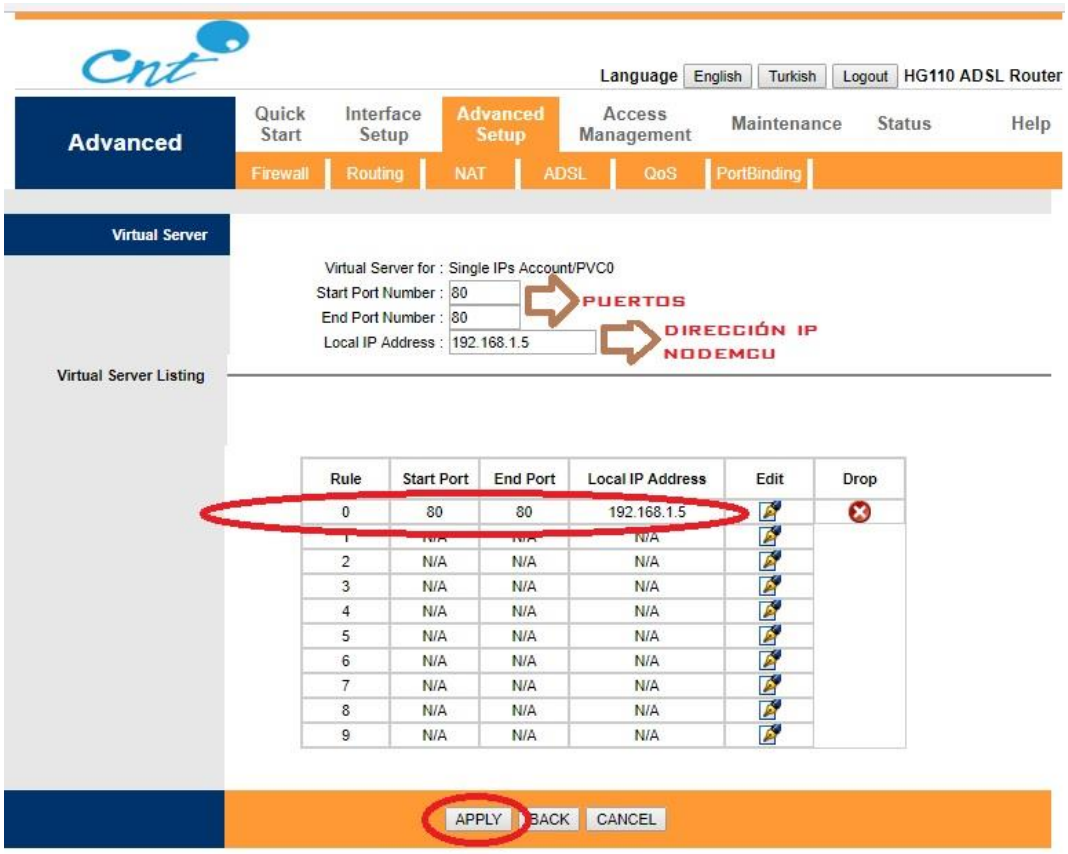


Figura 48-2: Puerto de comunicaciones y dirección IP asignada al módulo
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.2.2.2 Peticiones a través de la aplicación móvil

La tarjeta de desarrollo puede comportarse como un servidor web, puede crear páginas web en formato HTML y ahí visualizar la información que se desea mostrar. Cualquier dispositivo cliente puede hacer peticiones a través de una URL con la direccion IP del módulo con la ayuda de dos métodos fundamentales: *GET* y *POST* con la única finalidad de solicitar una respuesta del servidor como se puede ver en la figura 48-2.

Figura 49-2: Peticiones a través de los métodos GET y POST
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

- **Método GET**: Envía una petición desde el dispositivo cliente al servidor para obtener información. Como los mensajes acerca de la información del estado del sensor magnético.

- **Método POST**: Envía una petición desde el dispositivo cliente al servidor para agregar, actualizar información o mensajes que son procesados y de este modo el NodeMCU realice las correspondientes acciones en la puerta.

2.4.3 Encriptación de datos

Una vez entendido como se realiza la comunicación WiFi entre los dispositivos, es de vital importancia dotar de seguridad a la información que se envía y recibe de extremo a extremo. Esto con el fin de evitar que cualquier persona no autorizada manipule dichos datos y pueda causar graves daños o alterar el buen funcionamiento del sistema implementado.

Para el desarrollo del proyecto, se utiliza el cifrado de datos simétrico por bloques AES de 128 bits, el cual posee adicionalmente un vector de inicialización (IV), esto con el fin de que el mismo

texto plano con la misma clave, dé como resultado un distinto texto cifrado, lo cual refuerza el algoritmo y evita una vulnerabilidad en el sistema de cifrado.

El vector de inicialización es un bloque de bits requerido para permitir un cifrado en flujo o un cifrado por bloques. El tamaño del IV dependen del algoritmo de cifrado y del protocolo criptográfico y a menudo es tan largo como el tamaño de bloque o como el tamaño de la clave.

El cifrado del mismo texto con la misma clave da como resultado el mismo texto cifrado, lo cual es una considerable vulnerabilidad. El uso de un vector de inicialización añadido linealmente (mediante una operación XOR) o incluido delante del texto plano antes del cifrado resuelve este problema.

2.4.3.1 Proceso de cifrado de mensajes en el módulo NodeMCU

Una vez entendido el algoritmo de cifrado implementado en el capítulo I, se explica cómo fue aplicado dicho método dentro del microcontrolador para el envío y recepción de la información vía WiFi

Como hay un flujo de instrucciones que se ejecutan repetidamente en la programación misma de la placa de desarrollo, entonces existe un constante envío de mensajes acerca del estado actual del sensor magnético, esto con el fin de trasmitir información al usuario y dar a conocer si tanto la cerradura electrónica como la puerta, si se encuentran en estado abierto o cerrado, una vez leídos estos datos, en la programación se asigna a cada estado un texto claro.

Como cualquier texto que se desee cifrar es un tipo de dato *String*, es necesario transformar en números hexadecimales y almacenar dicho mensaje en otra variable de tipo *byte*. De acuerdo al formato de la función de encriptación que se utilizó.

La función que realiza este procedimiento de cifrado es:

```
aes.cbc_encrypt(plain, cipher, blocks, iv);
```

y se encuentra contenida dentro de la librería *AES.h.* Los parámetros de dicha función son:

- **Plain:** Vector de tipo byte que contiene el texto que se desea cifrar en número Hexadecimal.
- **Cipher:** Vector de tipo byte donde se almacena el texto cifrado
- **Blocks:** Valor de tipo entero que determina la dimensión de la matriz del bloque total del mensaje a encriptar. En este caso se tienen 4 filas de bytes por 4 columnas de bytes, es

decir una encriptación por bloques, se tienen dos componentes, por lo tanto, se coloca el valor de bloque=2.

- **IV:** Es el vector de tipo byte de inicialización importante para el procedimiento de cifrado por bloques *CBC*. En este caso el vector de inicialización se colocó en número hexadecimal como sigue:

byte iv[] = *{0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F};*

La clave de encriptación que será compartida entre emisor y receptor en dato String es: "**NodeMCU123456789**" que tiene un tamaño de 16 bytes, es decir una clave de 128 bits.

Una vez colocado todos los parámetros anteriores, como salida se obtiene un texto cifrado en código hexadecimal de 32 caracteres, al cual dicho mensaje solo el usuario final que tenga acceso a la aplicación móvil y luego de un procedimiento de descifrado conocerá el mensaje original.

Como se puede visualizar en la figura 49-2, se presenta un resumen del procedimiento de cifrado sobre el módulo NodeMCU.

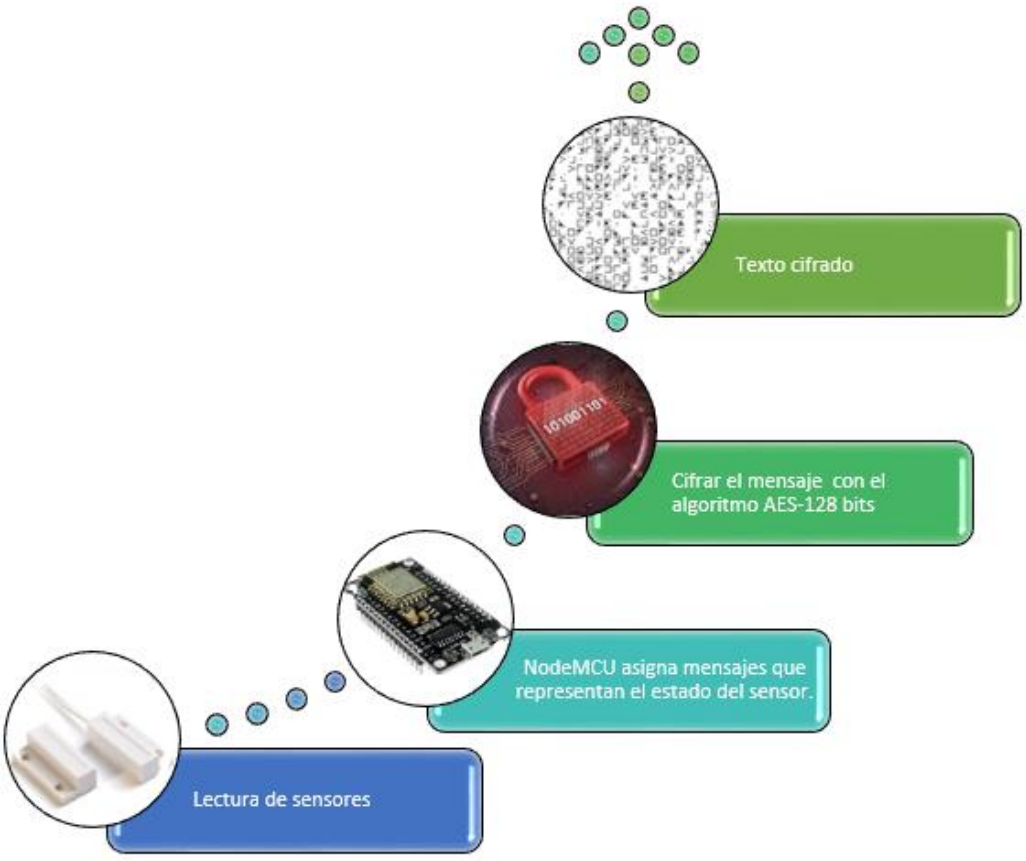


Figura 50-2: Proceso de cifrado en el módulo NodeMCU
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.3.2 Proceso de descifrado de mensajes en el módulo NodeMCU

Para el descifrado de la información hecha por una petición del cliente conectado a la red WiFi, a través de la aplicación móvil, se tiene un mensaje de tipo *String* que llega en código hexadecimal con un tamaño de 32 caracteres. Dada dicha longitud de texto cifrado, es necesario agruparlos en parejas de dos números, para lograr obtener un vector final de hasta 16 caracteres, esto con la finalidad de tener una matriz cuadrada que es necesaria para la función de desencriptación que se explicará más adelante.

El mensaje de caracteres hexadecimales se debe trasformar de tal modo que los mismos caracteres hexadecimales de tipo *String* se conviertan en datos numéricos de tipo *Byte* del mismo valor hexadecimal.

Esto se logra con la función interna del lenguaje C contenida en la librería *Stdlib.h.* La función que realiza esta conversión es:

```
int long val = strtol(const char *s, const char *p, base);
```

En donde los parámetros de dicha función son:

- **Val:** variable de tipo entero largo, donde se almacenará el dato luego de la transformación.
- **S:** Es la cadena de caracteres a convertir
- **P:** Es un puntero que se colocará inmediatamente al entero largo de la cadena s. puede tomar valor *NULL*, para no realizar esta acción.
- **Base:** Indica la base de la transformación, por defecto es decimal, puede también ser binaria, octal o hexadecimal.

Luego de realizada la operación de conversión de dato String a número, y los números hexadecimales sean agrupados en parejas, se tiene un vector de 16 numero hexadecimales.

La función que realiza este procedimiento de descifrado es:

```
aes.cbc_decrypt (cipher, check, blocks, iv) ;
```

y se encuentra contenida dentro de la librería *AES.h.* Los parámetros de dicha función son:

- **Cipher:** Vector de tipo byte que contiene los caracteres cifrados en número hexadecimal.

- **Check:** Vector de tipo byte donde se almacena los caracteres desencriptados. Este vector se debe trasformar a números hexadecimales y luego a caracteres de tipo *char*, para al final obtener el mensaje recibido desde la aplicación de tipo *String*.

- **Blocks:** Valor de tipo entero que determina la dimensión de la matriz del bloque total del mensaje a desencriptar. En este caso se tienen 4 filas de bytes por 4 columnas de bytes, es decir una desencriptación por bloques, se tienen dos componentes, por lo tanto, se coloca el valor de bloque=2.

- **IV:** Es el vector de tipo byte de inicialización importante para el procedimiento de descifrado por bloques *CBC*. En este caso el vector de inicialización se colocó en número hexadecimal como sigue:

byte iv[] = *{0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F};*

La clave de desencriptación que será compartida entre emisor y receptor en dato String es: "**NodeMCU123456789**" que tiene un tamaño de 16 bytes, es decir una clave de 128 bits.

Una vez colocado todos los parámetros anteriores, como salida se obtiene un texto claro, y de acuerdo a la instrucción asociada proveniente de la aplicación móvil, el módulo WiFi se encargará de realizar dicha tarea de control.

Como se puede visualizar en la figura 50-2, se presenta un resumen del procedimiento de descifrado sobre el módulo NodeMCU.

Figura 51-2: Proceso de descifrado en el módulo NodeMCU
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.3.3 Proceso de cifrado de mensajes en Android

El proceso de cifrado de la información en la aplicación móvil ocurre de manera similar al proceso de cifrado sobre la tarjeta de desarrollo. Como bien se sabe, la aplicación tiene diferentes pantallas de control, en las cuales se tiene botones de acción que son los encargados de enviar diversos mensajes claros, es decir instrucciones según lo requiera el usuario. Éste mensaje es cifrado gracias a la ayuda de funciones de encriptación empleadas dentro de la aplicación móvil. La función declarada en java es la siguiente:

```
public static byte[] encrypt(byte[] key1, byte[] key2, byte[] value) {
    try {
        IvParameterSpec iv = new IvParameterSpec(key2);
        SecretKeySpec skeySpec = new SecretKeySpec(key1, "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/NOPADDING");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec, iv);

        byte[] encrypted = cipher.doFinal(value);

        return encrypted;

    } catch (Exception ex) {
        ex.printStackTrace();
    }

    return null;
}
```

Figura 52-2: Función de encriptación en Android
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

En donde los parámetros de dicha función son:

- **Key1:** Vector de tipo byte que contiene los caracteres de la clave. La clave en String a convertir previamente en número hexadecimal es: "**NodeMCU123456789**"
- **Key2:** Vector de tipo byte que contiene los caracteres del vector de inicialización (IV). El vector de inicialización a convertir de caracteres String de código Hexadecimal a número hexadecimal es: **"000102030405060708090A0B0C0D0E0F"**
- **Value:** Es el mensaje que se quiere enviar. Previamente debe ser convertido a caracteres de tipo byte.

Y finalmente se retorna la variable *encrypted* de tipo byte, que contendrá el mensaje cifrado que se enviará hacia la tarjeta de desarrollo NodeMCU.

En la figura 52-2 Se observa un resumen del procedimiento de cifrado que ocurre sobre la aplicación móvil.

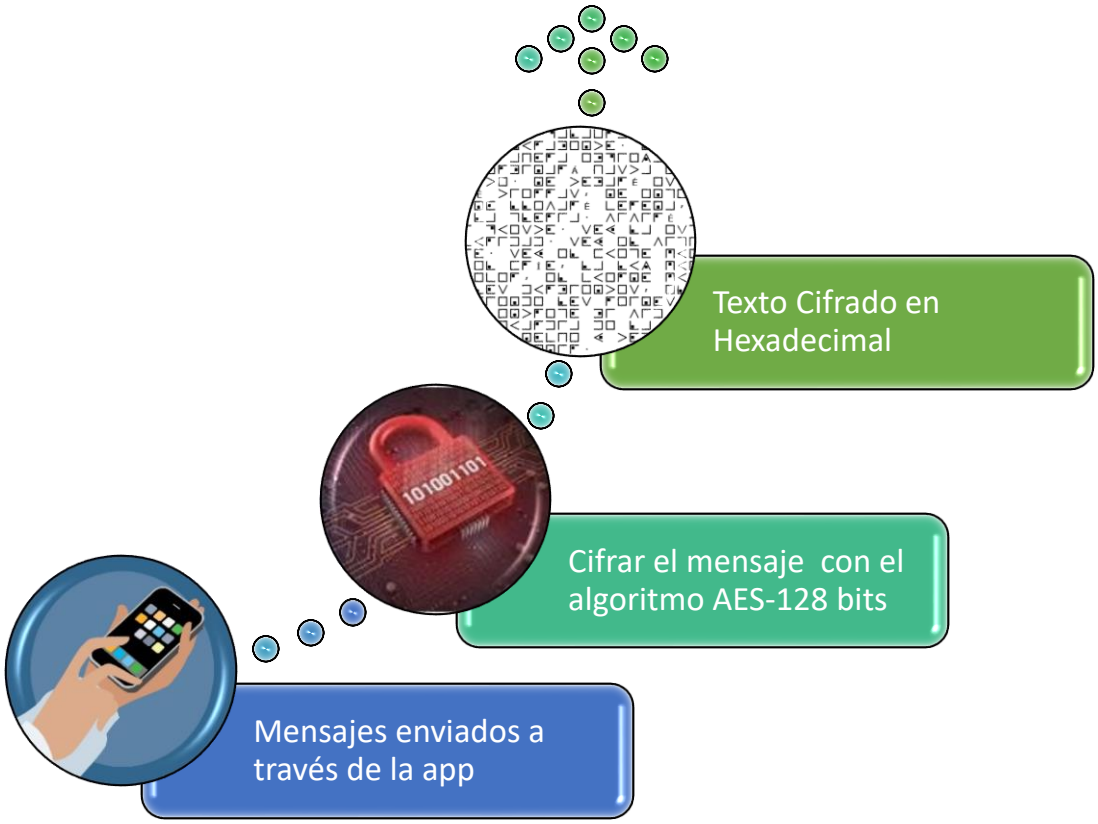


Figura 53-2: Proceso de cifrado en Android
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.3.4 Proceso de descifrado de mensajes en Android

El proceso de descifrado de los mensajes en la aplicación móvil ocurre cuando se dirige a la URL del servidor (NodeMCU). El mensaje mostrado en la página web se encuentra cifrado en código hexadecimal y es de tipo *String*. Para ello se llama la función declarada en java:

```
public static byte[] decrypt(byte[] key1, byte[] key2, byte[] encrypted) {
    try {
        IvParameterSpec iv = new IvParameterSpec(key2);
        SecretKeySpec skeySpec = new SecretKeySpec(key1, "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/NOPADDING");
        cipher.init(Cipher.DECRYPT_MODE, skeySpec, iv);

        byte[] original = cipher.doFinal(encrypted);

        return original;

    } catch (Exception ex) {
        ex.printStackTrace();
    }

    return null;
}
```

Figura 54-2 Función de desencriptación en Android
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

En donde los parámetros de dicha función son:

- **Key1:** Vector de tipo byte que contiene los caracteres de la clave. La clave en String a convertir previamente en número hexadecimal es: "**NodeMCU123456789**"
- **Key2:** Vector de tipo byte que contiene los caracteres del vector de inicialización (IV). El vector de inicialización a convertir de caracteres String de código Hexadecimal a número hexadecimal es: **"000102030405060708090A0B0C0D0E0F"**
- **encrypted:** Es el mensaje cifrado que se quiere desencriptar.

Y finalmente se retorna la variable *original* de tipo byte, que contendrá el mensaje claro que podrá ser leído por el usuario que haga uso de la aplicación móvil.

En la figura 54-2, se observa un resumen del procedimiento de descifrado de la información que se ejecuta sobre la aplicación.

Figura 55-2: Proceso de desencriptación en Android
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.4 Base de datos

Hay que mencionar que para el desarrollo de la aplicación móvil se tuvo que implementar dos tipos de bases de datos.

2.4.4.1 Base de datos almacenada en el teléfono inteligente

Como se estudió en el capítulo anterior, toda aplicación móvil tiene un ciclo de vida, es decir desde el momento en el que se abre la aplicación móvil hasta el momento en el que se la cierra. Entonces, al momento de finalizar la aplicación todos los valores que fueron almacenados en las distintas variables a lo largo del uso de la aplicación se borran.

Para solucionar este inconveniente la plataforma Android Studio nos ofrece algunas alternativas para el almacenamiento permanente de información en un smartphone acerca de las aplicaciones que se abren.

Para el desarrollo de la aplicación móvil se necesita un almacenamiento de datos mediante la clase llamada *SharedPreferences.* Por su sencillez de uso, estas preferencias no son más que datos que se guardan para ser compartidos con otros métodos u otras clases cuando la aplicación móvil se cierra, incluso si el teléfono se apaga o se reinicia.

Cada preferencia se guarda de forma privada e independiente gracias a un identificador único, una clave, y un tipo de valor primitivo (bool, int, string, float, long) sobre un fichero **XML**

ubicado en la carpeta del proyecto. El uso de esta clase en particular se lo realiza cuando no se tienen gran cantidad de datos que se tienen que recordar.

Los modos de acceso a las preferencias son:

- **MODE_PRIVATE.** Sólo la app desarrollada tiene acceso a estas preferencias.
- **MODE_WORLD_READABLE.** Todas las aplicaciones pueden leer estas preferencias, pero sólo la app desarrollada puede modificarlas. (obsoleta desde API 17 – Android 4.2)
- **MODE_WORLD_WRITABLE.** Todas las aplicaciones pueden leer y modificar estas preferencias. (obsoleta desde API 17 – Android 4.2)
- **MODE_MULTI_PROCESS:** Varios procesos pueden acceder a las preferencias.

Hay que aclarar que para instanciar la clase SharedPreferences se lo realiza de manera diferente cuando se trabaja sobre una *Activity*, un *Fragment* o un *Service.*

Para instanciar la clase sobre una *Activity*, se lo realiza de la siguiente forma:

```
SharedPreferences Preferences=getSharedPreferences("Mispreferencias", MODE_PRIVATE);
```

Figura 56-2: Instancia de la clase *SharedPreferences*
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Donde:

- **Preferences:** Nombre del objeto.
- **getSharedPreferences:** Método para llamar a la preferencia.
- **Mispreferencias:** Nombre que se asigna al fichero que contendrá el archivo XML.
- **MODE_PRIVATE:** Modo de operación sobre el archivo que se establecerá para otras aplicaciones.

Luego de crear el objeto, se puede leer o modificar los datos almacenados mediante una clave y su valor mediante los métodos get () o put ().

Método get()

Se obtiene valores del objeto Preferences. Algunos posibles casos son:

- getString(String nombre, String valorPorDefecto)
- getBoolean(String nombre, boolean valorPorDefecto)
- getInt(String nombre, int valorPorDefecto)

Un ejemplo se presenta a continuación:

```
String nombre = Preferences.getString("clave", "valorPorDefecto");
```

Figura 57-2: Línea de código con el método get().
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Método put()

Primero se invoca al método *edit()* para obtener un editor, con lo cual se podrá llamar al método *put()* para insertar un valor o actualizar sobre la preferencia, validando la edición con el método *apply()*. Algunos casos son:

- putString(String nombre,boolean valor)
- putBoolean(String nombre,boolean valor)
- putInt(String nombre,boolean valor)

Un ejemplo se presenta a continuación:

```
SharedPreferences.Editor editor = Preferences.edit();
editor.putString("nombre", "JUAN");
editor.apply();
```

Figura 58-2: Línea de código con el método put ()
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Como se visualiza en la figura 57-2, es el procedimiento de obtener y actualizar un valor en la clase *SharedPreferences* dentro de la aplicación.

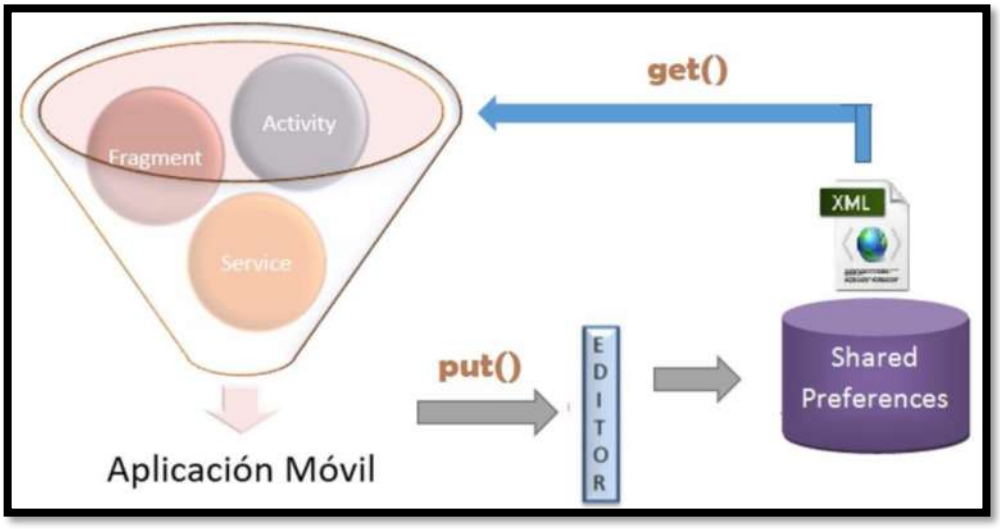


Figura 59-2: Funcionamiento del método get() y put()
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.4.2 Base de datos almacenada en la nube

Para reforzar la seguridad en la aplicación móvil, se requiere el uso de una base de datos en la cual se almacena la información de todos los usuarios que se registren en la misma.

Firebase es una plataforma de desarrollo móvil creada por Google. Almacena y sincroniza datos con todos los clientes en tiempo real, es decir que cualquier cambio que se realice en los datos por cualquier usuario, aplicación o dispositivo, se sincronizará de forma inmediata, esto con el objetivo de actualizar la información automáticamente con los datos más recientes.

La base de datos en tiempo real tiene la forma de un objeto JSON (JavaScript Object Notation), es decir los datos se almacenan en un árbol de valores que se pueden editar y consultar cuando el usuario lo requiera.

2.4.4.2.1 Características de la base de datos FireBase

- **Seguridad:** Dispone de varias reglas de seguridad para determinar quiénes tienen acceso de lectura, escritura en la base de datos.
- **Autenticación**: Permite identificar a los usuarios que acceden a la app, en este caso se usó el método de correo electrónico y contraseña
- **Trabajar en modo offline:** Los datos se mantienen en un *caché* interno si el dispositivo pierde conexión, manteniendo los datos nuevos en modo de espera, hasta que se recupere la conexión y los datos se actualicen finalmente.
- **Diversidad:** Es compatible en varias plataformas como: Android, IOS, Web, etc.

2.4.4.2.2 Creación de un nuevo proyecto Firebase

Antes que nada, se tiene que tener una cuenta creada de Gmail para poder hacer uso de este servicio gratuito. Para realizar este proceso se debe ingresar desde el navegador a la siguiente página web: **https://firebase.google.com/,** dando al botón *Acceder* como se ve en la figura 59-2.

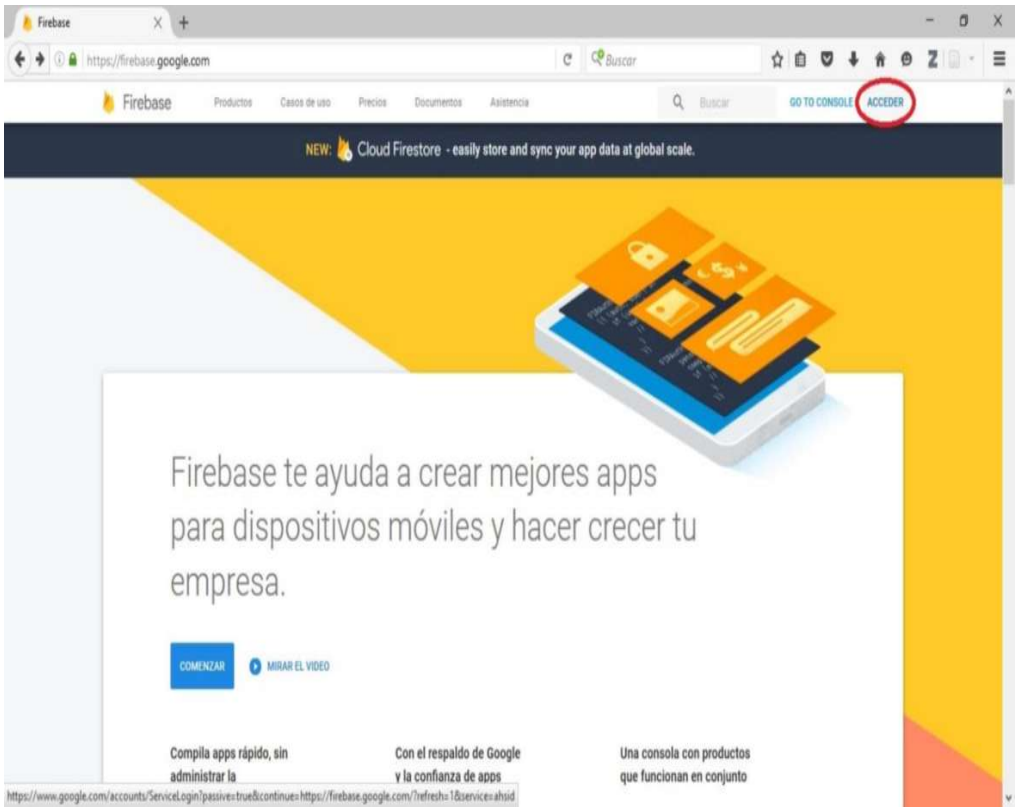


Figura 60-2: Acceso a Firebase
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Después, se ingresa los datos de una cuenta de Gmail asociada como se observa en la figura 60-2.

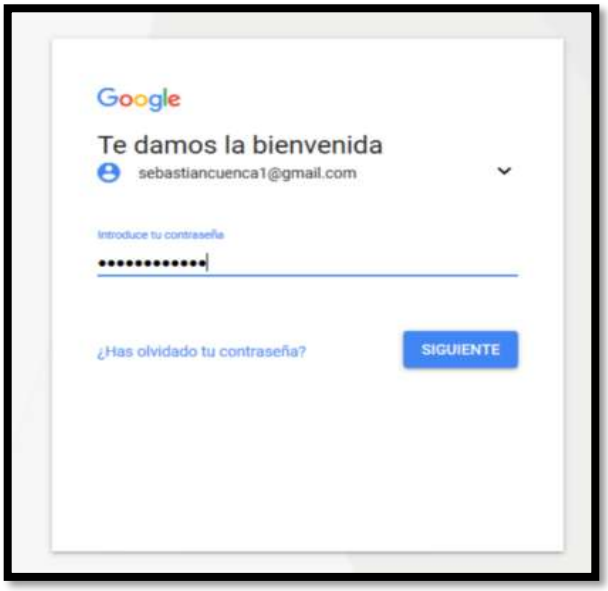


Figura 61-2: Ingreso a la cuenta de Gmail
Fuente: Sebastián Cuenca; Alex Manotoa; 2017.

Después de identificarse en la cuenta, es necesario presionar el botón *Go to console* en la parte superior derecha, teniendo la siguiente ventana para crear un nuevo proyecto, se llena toda la información necesaria y finalmente se obtiene la plataforma Firebase asociada a una cuenta.

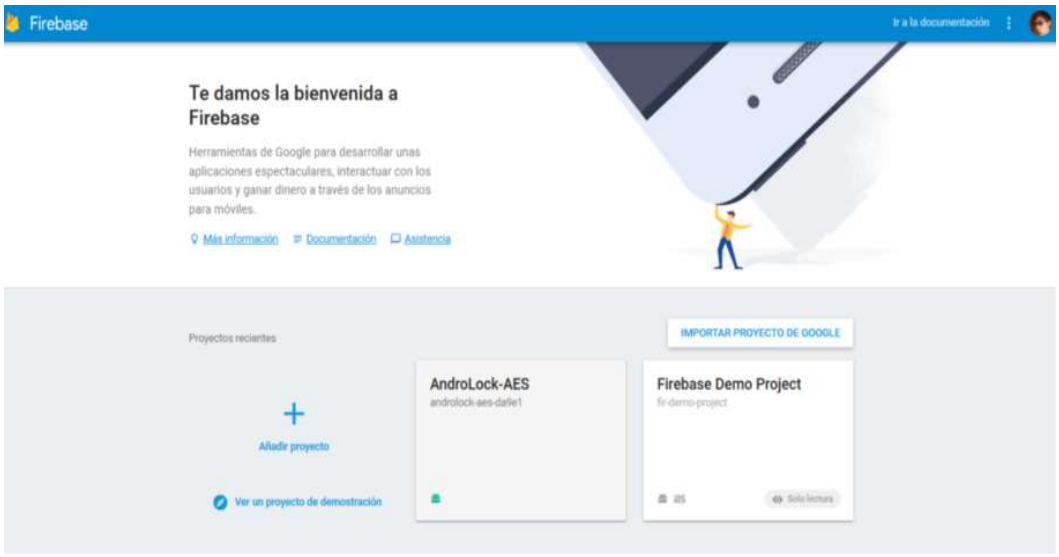


Figura 62-2: Entorno de desarrollo Firebase
Fuente: Sebastián Cuenca; Alex Manotoa; 2017.

Luego dirigirse en *Authentication*, y en la pestaña *MÉTODO DE INICIO DE SESIÓN*, es necesario habilitar el método *Correo Electrónico/Contraseña* como se visualiza en la figura 62-2. Este método es el implementado para el acceso a la aplicación móvil AndroLock-AES que controla al prototipo de cerradura electrónica WiFi.

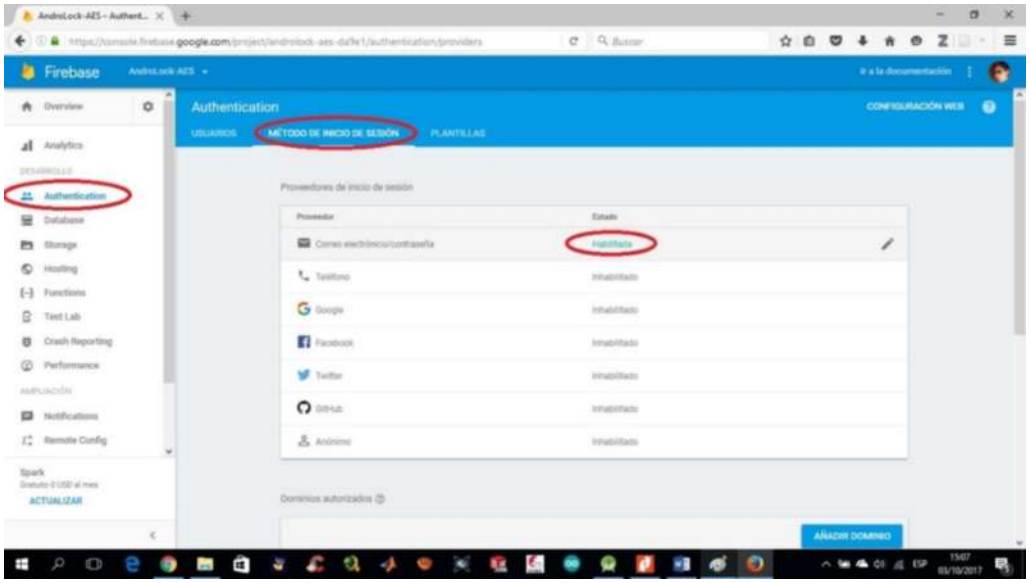


Figura 63-2: Selección del método de inicio de sesión
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Hechos los pasos anteriores ya se puede visualizar la base de datos en tiempo real con los usuarios registrados de manera automática en ella.

En la figura 63-2 se tiene el nombre de la base de datos que proviene desde la aplicación móvil, y los diferentes usuarios que pueden registrarse en ella con sus respectivos datos.

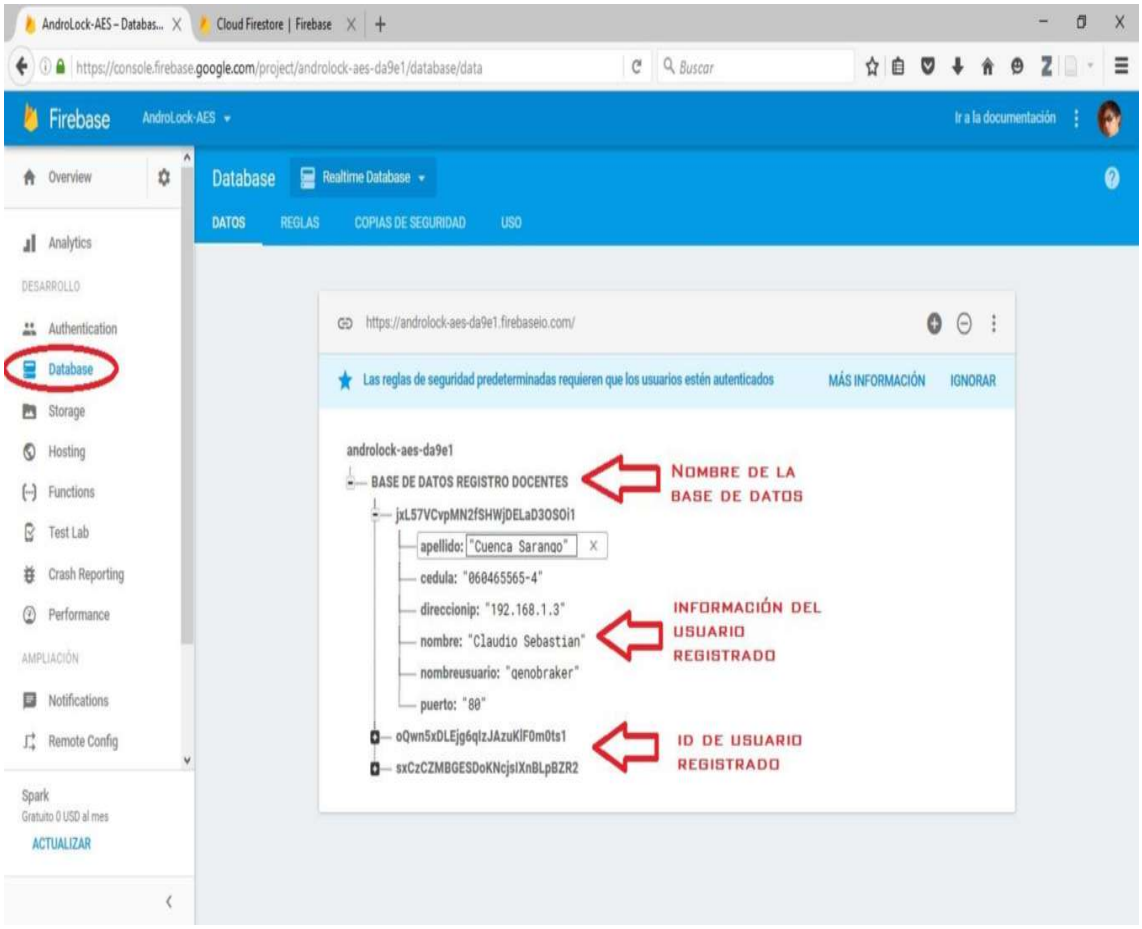


Figura 64-2: Base de datos en tiempo real
Fuente: Sebastián Cuenca; Alex Manotoa; 2017.

2.4.4.2.3 Sincronización de la Base de datos Firebase con la aplicación móvil

La ventaja de la plataforma Android Studio es que de manera sencilla se puede incorporar cualquier aplicación móvil el uso del servicio Firebase. Para la autenticación de los nuevos usuarios que se registren en la app, es necesario sincronizar el proyecto de Android Studio con el proyecto en la nube, para ello se requiere hacer clic sobre las herramientas mostradas en la imagen 64-2

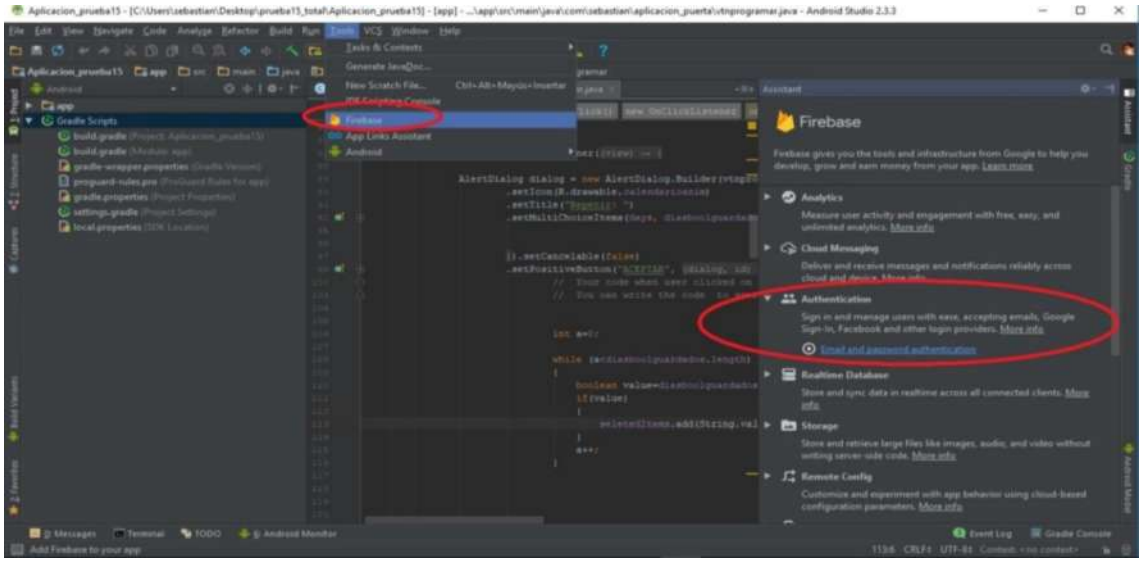


Figura 65-2: Sincronización entre Android Studio y Firebase.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Se activan los pasos *1* y *2* para que el programa realice las configuraciones necesarias para la correcta identificación de los usuarios cuando requieran iniciar sesión mediante un correo electrónico y una contraseña

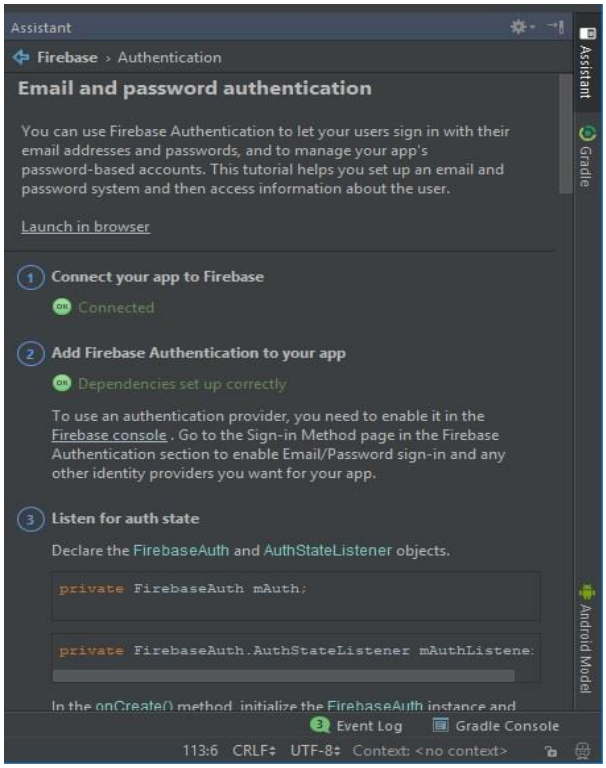


Figura 66-2: Sincronización completa de servicio de Autenticación
Fuente: Sebastián Cuenca; Alex Manotoa; 2017.

Después, como se ve en la figura 66-2, se da clic sobre la barra de herramientas en *Tool*, luego en *Realtime DataBase* y en la opción *Save and Retrieve Data.*

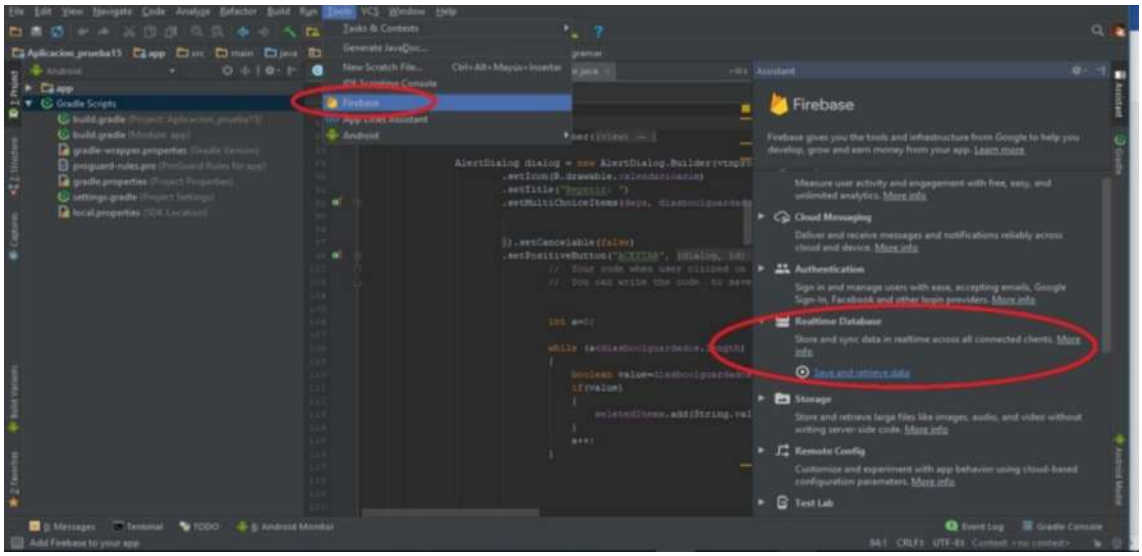


Figura 67-2: Selección del servicio Realtime DataBase
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

Se habilita cada uno de los pasos *1* y *2* que contienen principalmente las librerías y configuraciones necesarias para conectar la app con la Firebase. En los siguientes pasos, se presentan ejemplos de todas las clases necesarias y métodos para realizar cambios en los datos de cada usuario si así se lo requiere.

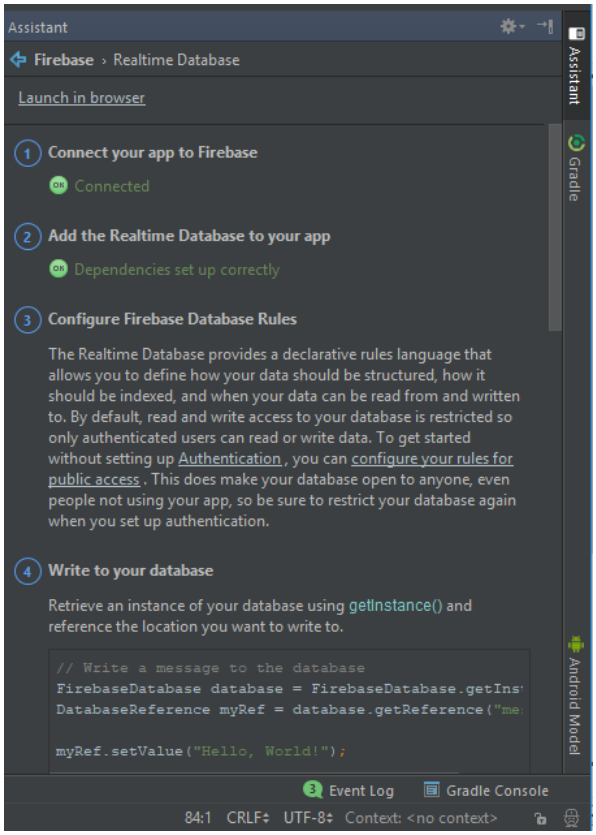


Figura 68-2: Sincronización completa con el servicio de base de datos
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.5 Sistema de Contingencia

Todo sistema electrónico debe tener un sistema de contingencia ante cualquier falla, para que el sistema que se quiere automatizar pueda mantenerse activo sin tener que dejar de funcionar. El mismo se encuentra en la figura 68-2, se puede ver el funcionamiento de los dos tipos de sistemas de respaldo implementados.

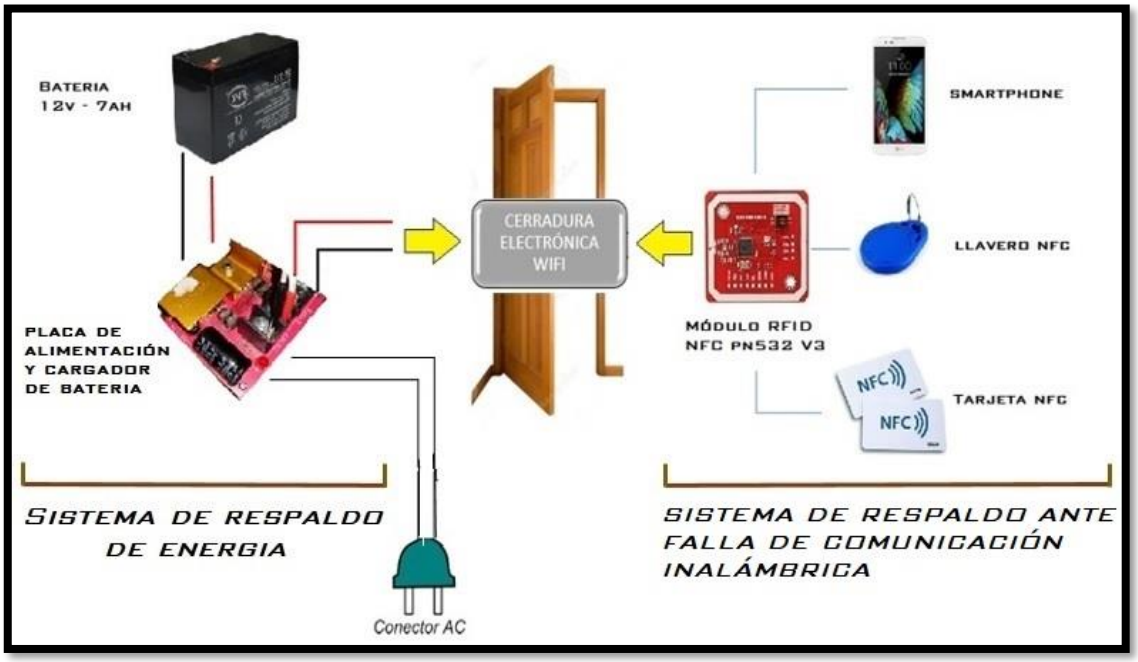


Figura 69-2: Sistemas de Contingencia
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017.

2.5.1 Sistema de respaldo de energía

Debido a que el sistema electrónico debe estar en constante actividad, es necesario la energía eléctrica para el funcionamiento de los dispositivos. Sin lugar a dudas, siempre existe un margen de falla, pues debido a varias circunstancias el servicio eléctrico en las edificaciones se ve suspendido por un periodo de tiempo. Para lo cual, existe la necesidad de colocar un sistema de respaldo de energía para esos casos especiales.

El sistema de respaldo de energía consiste en una placa electrónica y una batería de 12 Voltios a 7 Amperios. Dicha placa se alimenta mediante un adaptador a la toma de 110V de un tomacorriente. Como salida se obtienen 12 Voltios que servirán de alimentación a todo el circuito electrónico implementado, al mismo tiempo esta placa se conecta a la batería. Mientras haya

energía eléctrica la batería no entrará en contacto directo con la salida de alimentación que se conecta al sistema electrónico, pero a la vez la placa electrónica se encarga de cargar la batería de forma automática si ésta se encuentra descargada. La batería cumpe un ciclo de carga correspondiente, finalizando dicha carga, hasta que alcance los 13.8 Voltios manteniendo así la batería lista y cargada.

El momento en que se suspende la energía eléctrica, la batería se pone en funcionamiento de inmediato entrando en contacto con la salida de alimentación que se conecta a la placa electrónica del prototipo. Dependiendo de la corriente que consuma todo el circuito electrónico, durará la corriente de la batería. Entonces, al regresar la energía eléctrica, se desconecta la batería y se pondrá de nuevo en funcionamiento la placa de alimentación para el circuito. Con este método se reduce las posibilidades que se interrumpa el correcto funcionamiento del dispositivo electrónico debido a la falta de energía.

2.5.2 Sistema de respaldo ante falla de la comunicación Inalámbrica

El servicio de conectividad WiFi en algunas ocasiones se ve suspendido debido a varias situaciones que se presentan. Pues el dispositivo electrónico debe estar conectado siempre a una red WiFi, de otra forma el sistema se vería afectado si se interrumpiera la comunicación.

Por tal motivo, se ve la necesidad de montar un sistema que pueda trabajar de forma independiente de la conectividad WiFi. Es así que, se implementa un sistema de respaldo ante la falla de la comunicación inalámbrica, la misma consta de en un módulo lector RFID NFC Pn532 como se muestra en la figura 68-2, que encarga de leer dispositivos que posean la tecnología NFC (Near Field Communication). Tal es el caso de algunos smartphones, tarjetas y llaveros NFC, etc. Estos aparatos funcionarán como llaves electrónicas de acceso.

Para lograr esto, es necesario que el usuario cuando inicie su sesión por primera vez en la aplicación móvil, se dirija al menú de registro de llaves electrónicas NFC y proceder al registro de las tarjetas electrónicas que posea. Cada usuario cuenta con un espacio máximo de tres llaves electrónicas a ser registras, y una vez hecho esto, basta con acercar dichos elementos al módulo lector NFC para que el sistema de control de acceso electrónico funcione normalmente.

2.6 Implementación del dispositivo electrónico

Para verificar el correcto funcionamiento del prototipo, se optó por implementar todo el sistema en la puerta de una habitación en una casa residencial. Pudiendo trabajar sin problema alguno en la construcción del proyecto de investigación.

2.6.1 Diseño de la placa del circuito electrónico impreso

Conociendo todos los elementos que intervienen en el desarrollo del prototipo se procede a simular el circuito sobre software Proteus versión 8.6 en ISIS como se muestra en la figura 69-2.

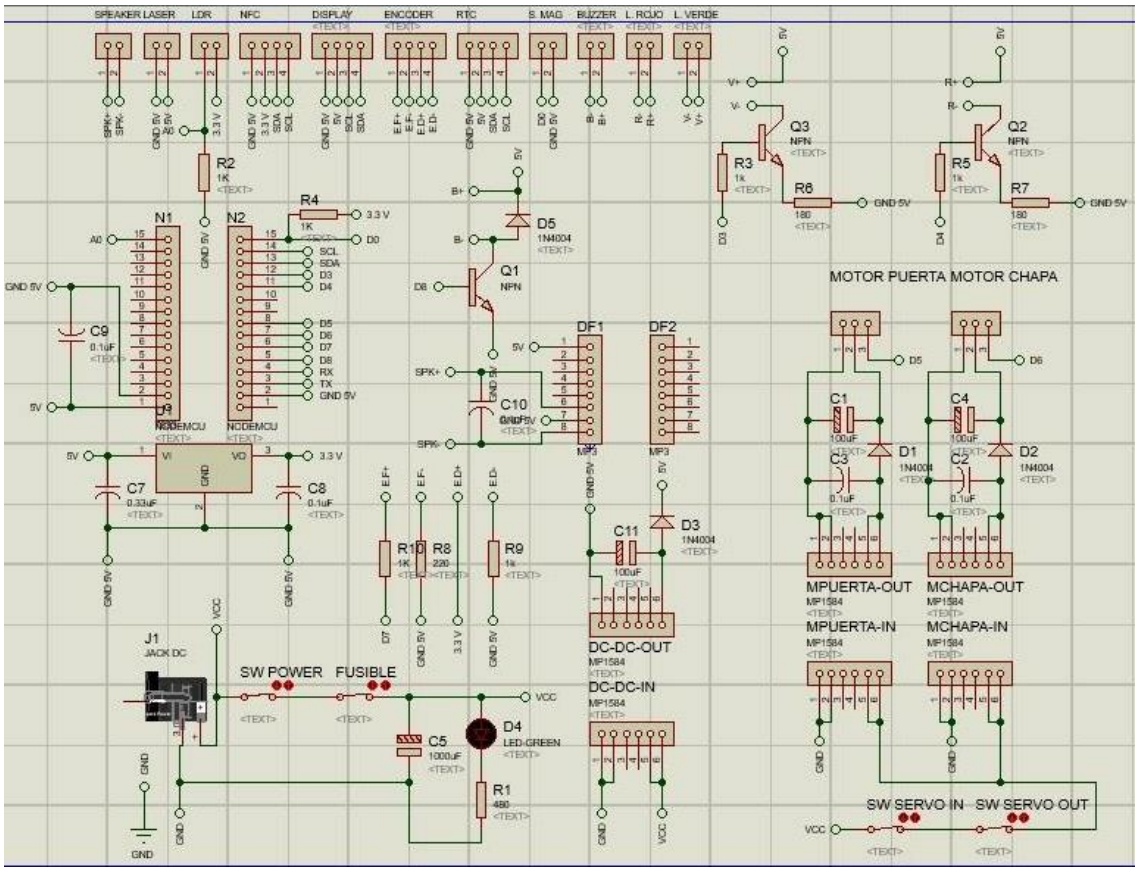


Figura 70-2: Simulación del circuito electrónico en ISIS en Proteus.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Una vez conectados todos los componentes, se procede a cambiar al entorno ARES para el diseño de la placa de circuito impreso (PCB).

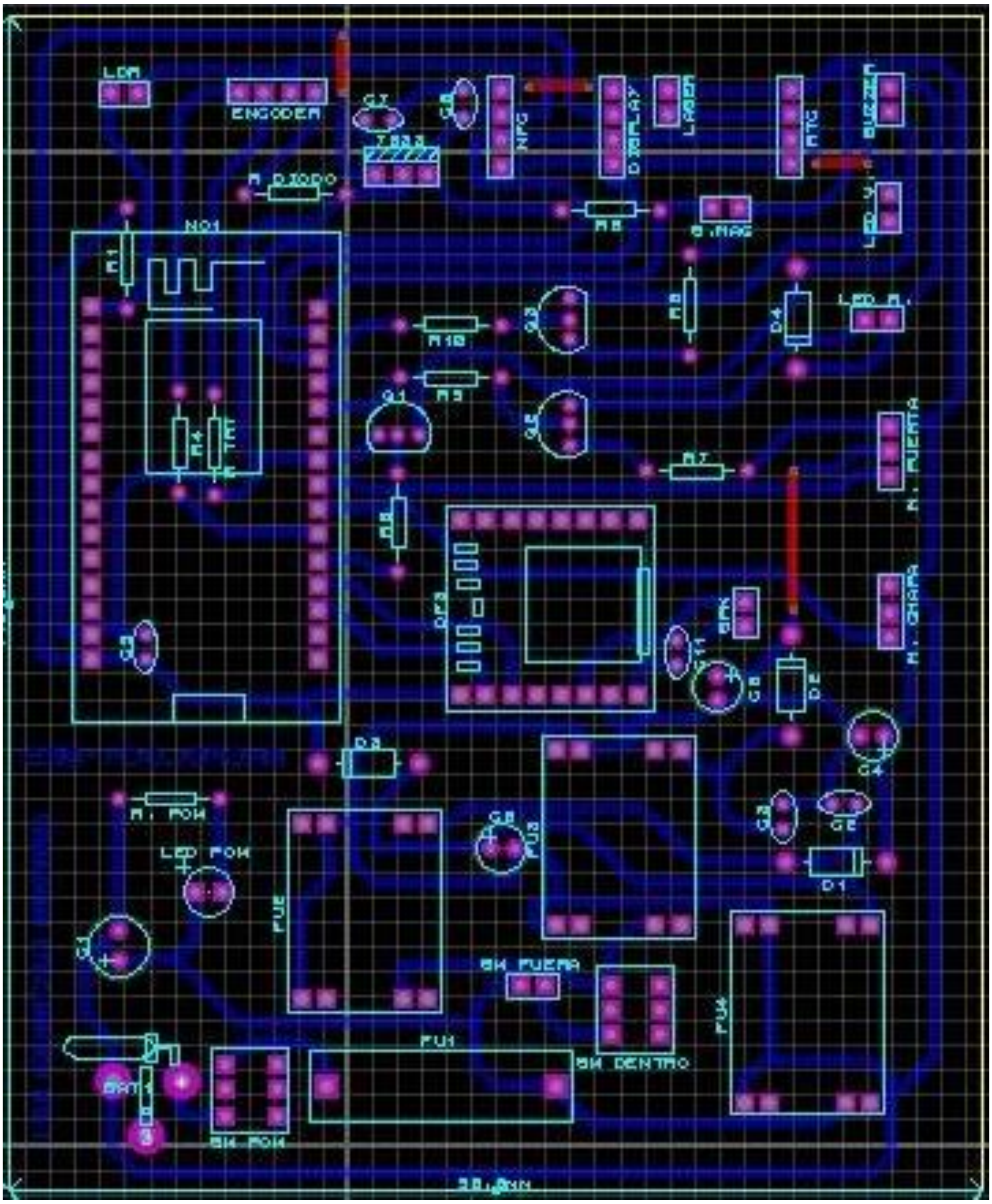


Figura 71-2: Diseño PCB de circuito electrónico en ARES en Proteus.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

A continuación, se tiene el modelo 3D de la placa de circuito impreso.

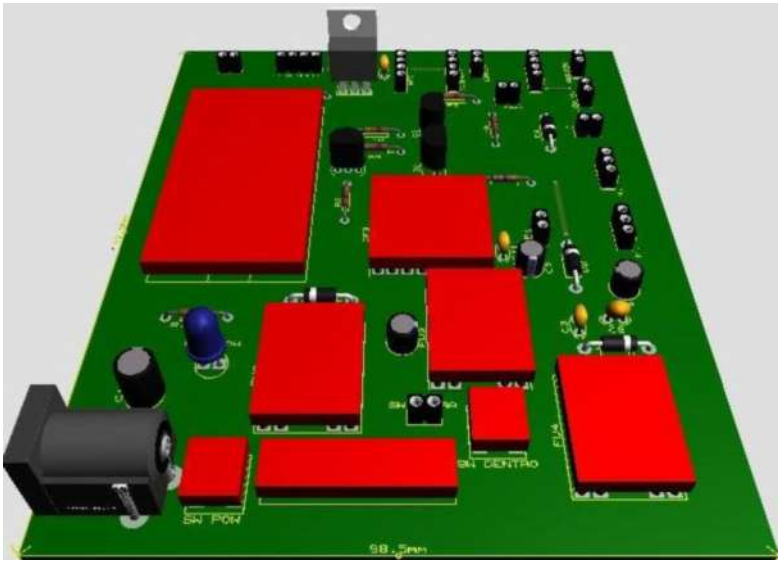


Figura 72-2: Representación en 3D circuito electrónico
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Y finalmente se colocan todos los elementos y se alimenta la placa para verificar que todo esté bien conectado.

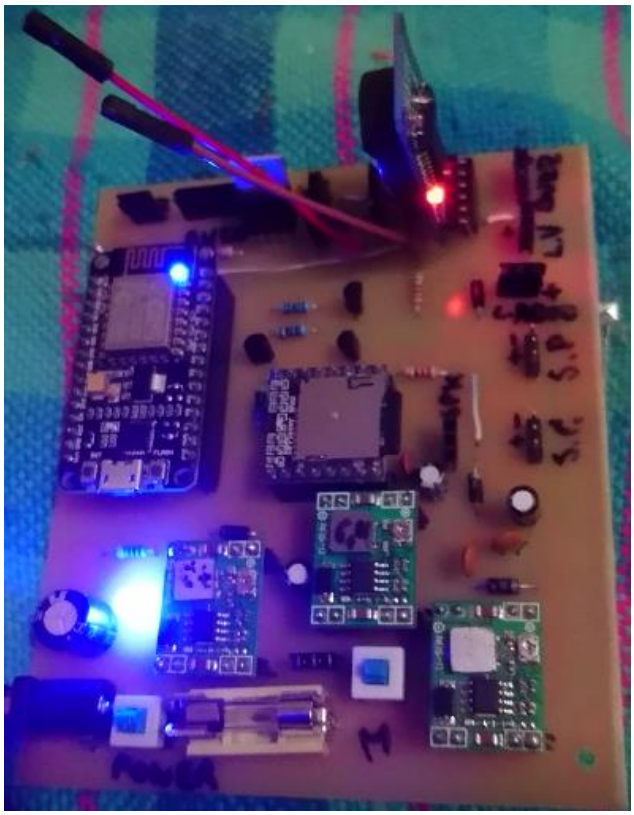


Figura 73-2: Placa real del circuito electrónico
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

2.6.2 Implementación final

Todos los componentes como conector al tomacorriente, servomotor para la puerta, la placa del circuito electrónico, la batería y placa de alimentación con el cargador. se colocaron en una caja de madera ubicada en la parte interior de la habitación y en la parte superior de la puerta como se ve en la figura 73-2. La caja tiene medidas:

- **Altura:** 15 cm
- **Ancho:** 55 cm
- **Profundidad:** 12 cm

Figura 74-2: Ubicación de elementos electrónicos en la caja de madera.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Figura 75-2: Sistema implementado sobre la puerta.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

CAPITULO III

3 PRUEBAS Y ANÁLISIS DE RESULTADOS

En el presente capítulo se muestra los resultados obtenidos de las pruebas realizadas luego de la implementación del prototipo de cerradura electrónica conectada a una red WiFi, para de esta manera verificar su correcto funcionamiento y, además garantizar el cumplimiento de los objetivos planteados.

3.1 Sistema implementado

3.1.1 Pruebas del Sistema mecánico

Dado las pruebas necesarias, y con la ayuda de un nivel digital se confirmó que todos los componentes instalados deben estar alineados de forma correcta para así evitar sobreesfuerzos mecánicos y se mantenga un movimiento fluido en la apertura y cierre completa de la puerta. La alimentación de los actuadores, debieron oscilar entre el rango mínimo y máximo mencionada en su hoja de datos para que tenga la potencia adecuada al momento de realizar cualquier movimiento.

3.1.1.1 Prueba de servomotor de brazo mecánico.

Con respecto al brazo mecánico que es el encargado de abrir o cerrar completamente la puerta de forma automática, el servomotor debió ser calibrado previamente para ajustar el rango de movimiento que necesita realizar. Entonces, mediante una serie de pruebas y observaciones en la programación del actuador se colocó el ángulo exacto cuando está en reposo o en movimiento.

Tabla 1-3: Rango de operación del servomotor de la puerta

Pruebas	Angulo inicial (Puerta cerrada)	Estado	Angulo posición final (apertura)	Estado
1	20	No cierra	140	No abre completamente
2	15	No cierra	150	No abre completamente
3	10	No cierra	160	No abre completamente
4	5	Cierra pero se fuerza el servo	165	Abre, pero se fuerza al servo
5	**3**	**Cierra Correctamente**	**170**	**Abre correctamente**
6	**0**	Cierra pero se fuerza el servo	180	Abre pero falta espacio

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Entonces en la tabla 1-3, se verifica que para que se mantenga en reposo el servomotor y no exista un sobresfuerzo, es decir su ángulo debe mantenerse fijo en todo momento, y por ningún motivo deba moverse, en la programación debe inicializarse en 3 grados, mientras que para que se abra completamente se debe llegar hasta los 170 grados

3.1.1.2 Prueba de servomotor en la chapa.

Para el mecanismo empotrado sobre el bombín de la cerradura, la correa dentada tuvo que regularse exactamente entre las dos poleas de acuerdo a la distancia entre ellas para permitir el giro al abrir la chapa o al cerrarla.

Si la banda se tiempla demasiado se puede romper, si se afloja demasiado, la banda se resbala entre las poleas y no permite abrir o cerrar la chapa de manera precisa.

Para verificar que entre o salga el pestillo conjuntamente con los seguros, se optó por un sensor de herradura y una rueda dentada colocados internamente, como se mencionó anteriormente, esto permite generar un contador en la programación y mediante una serie de pruebas se calibra al servomotor para para verificar que la chapa se abra o cierre correctamente.

Tabla 2-3: Rangos del servomotor de la chapa para jalar y soltar los seguros

Pruebas	Contador en espacios vacíos de la rueda dentada	Numero de vueltas	Estado
1	5	Ninguna	Sale el pestillo, pero no seguros
2	10	Ninguna	Sale el pestillo, pero no seguros
3	15	Una	Sale el pestillo, pero no seguros
4	20	Una	Sale el pestillo con el primer seguro
5	25	Una	Sale el pestillo con el primer seguro
6	30	Dos	Sale el pestillo con el primer seguro
7	32	Dos	Sale el pestillo con el primer y segundo seguro
8	35	Dos	Sale el pestillo con el primero y segundo seguro

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

De acuerdo a la tabla 2-3, se concluye que cuando exista una cuenta entre 0 a 15, el servo dará una vuelta, pero solo abrirá el pestillo. Cuando exista una cuenta entre 16 a 30, se abrirá el pestillo

y el primer seguro, y finalmente cuando exista una cuenta mayor a 30 se abrirá el pestillo, y sus dos seguros que es la capacidad máxima de la cerradura.

3.1.2 Pruebas de acceso de usuarios a la aplicación móvil

Como se visualiza en la figura 1-3, mediante un proceso de autenticación, se verificó que solamente los usuarios previamente registrados en la base de datos en tiempo real *Firebase* tendrán acceso a la aplicación móvil, de lo contrario no se tiene acceso al sistema de control.

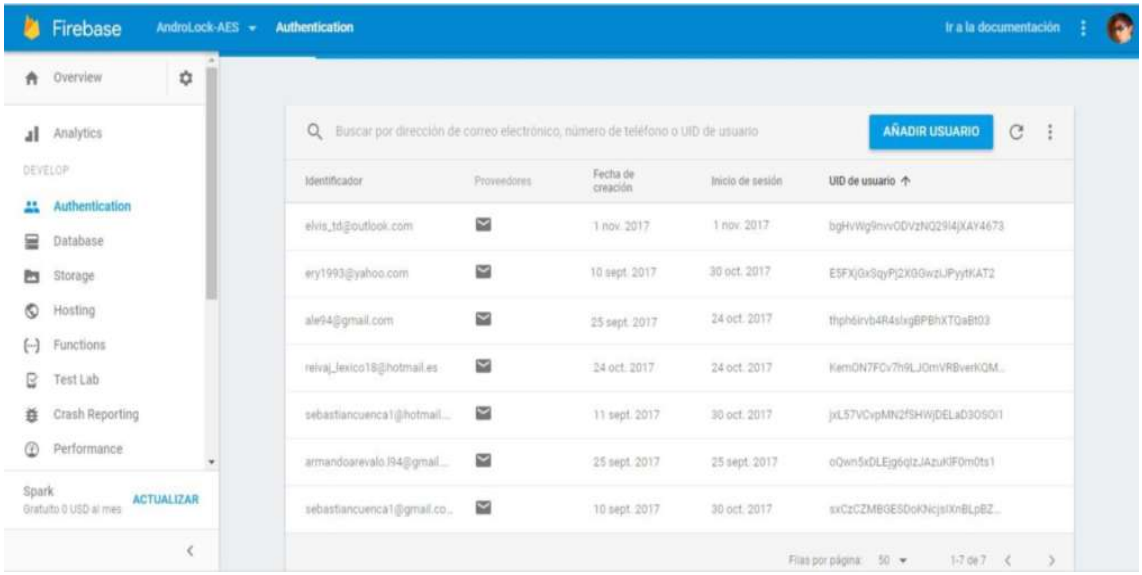


Figura 76-2: Usuarios registrados en la base de datos a través de la aplicación.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

En la tabla 3-3 se presenta un resumen de los resultados obtenidos

Tabla 3-3: Usuarios con acceso a la aplicación móvil

Usuario	Correo electrónico	Estado
Sebastian Cuenca	sebastiancuenca1@gmail.com	Tiene Acceso
Alex Manotoa	reivaj_lexico18@hotmail.es	Tiene Acceso
Alejandra Castillo	ale94@gmail.com	Tiene Acceso
Erika Taday	ery1993@yahoo.com	Tiene Acceso
Elvis Paucar	elvis_td@outlook.com	Tiene Acceso
Armando Arévalo	armandoarevalo.l94@gmail.com	Tiene Acceso

Viviana Aguilar	vivian_981@yahoo.com	No tiene Acceso
Roberto Chávez	robert_mchr@hotmail.com	No tiene Acceso
Lisbeth Molina	lismolina_1990@gmail.com	No tiene Acceso

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

3.1.3 Pruebas de comunicación WiFi.

Se hace una serie de pruebas para verificar que un dispositivo cliente esté conectado a una red WiFi y envié las peticiones a través de la aplicación móvil hacia el dispositivo electrónico implementado.

Tabla 4-3: Comunicación WiFi

Pruebas	Dirección IP privada	Dirección IP publica	Estado
1	192.168.1.2	186.46.226.245	Existe conexión
2	192.168.1.10		Existe conexión
3	192.168.1.8		Existe conexión
4	192.168.0.100	179.49.13.33	No hay conexión
5	192.168.0.80		No hay conexión
6	192.168.45.1	179.49.13.35	No hay conexión
7	192.168.56.1		No hay conexión
8	172.25.212.181	201.218.5.72	No hay conexión
9	169.254.203.65		No hay conexión
10	192.168.1.6	186.46.175.89	No hay conexión

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

De acuerdo a la tabla 4-3, los resultados anteriores no fueron los esperados, puesto que se concluye que el dispositivo no tiene salida a Internet. El resultado tiene que ver mucho con el proveedor del servicio de internet(ISP), en este caso dotado con un plan fijo de internet Fastboy por la compañía CNT de Ecuador.

Como el prototipo se encuentra conectado a una red local doméstica, se verificó que la IP asignada al router es dinámica, lo que no es conveniente para los propósitos del servidor implementado a través del módulo NodeMCU. También todos los puertos se encuentran bloqueados, es decir que cualquier usuario que se encuentre en una red remota no tendrá acceso al dispositivo.

Cabe resaltar que cualquier petición que se realice desde el dispositivo móvil hacia el prototipo es inmediata, teniendo tiempos de respuesta extremadamente cortos y obteniendo resultados satisfactorios en ese sentido referente a la comunicación inalámbrica en la red local.

3.1.4 Prueba de cifrado de información

Debido a que existe el constante intercambio de información entre el NodeMCU y la aplicación móvil (emisor y receptor), se procedió a verificar que los mensajes que se envían estén cifrados para que no puedan ser interceptados por agentes extraños, es por ello que colocando la URL de la dirección IP del módulo WiFi en un navegador web, como se muestra en la figura 1-3, el mensaje se encuentra cifrado.

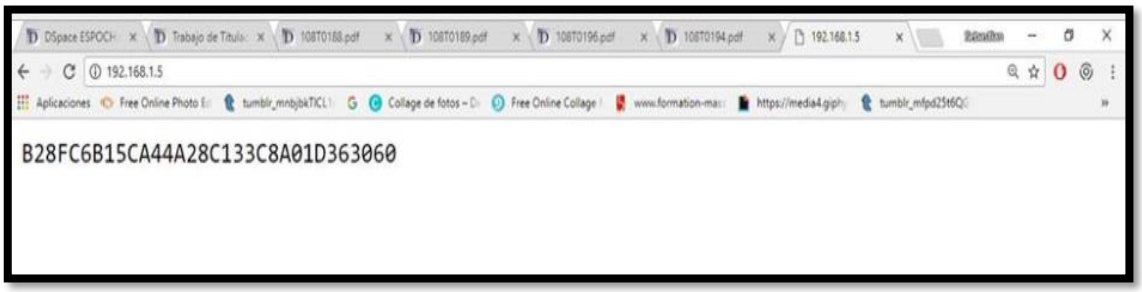


Figura 1-3 Mensaje cifrado.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Mientras si se envía el mensaje claro sin cifrar, entonces se tiene un mensaje como en la figura 2-3.

Figura 2-3: Mensaje plano.
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Un ejemplo es la lectura del sensor magnético, al cual se le asigna a su estado (cero o uno) un mensaje, en este caso si el sensor está abierto, se tiene el mensaje que se muestra en la figura 3-3.

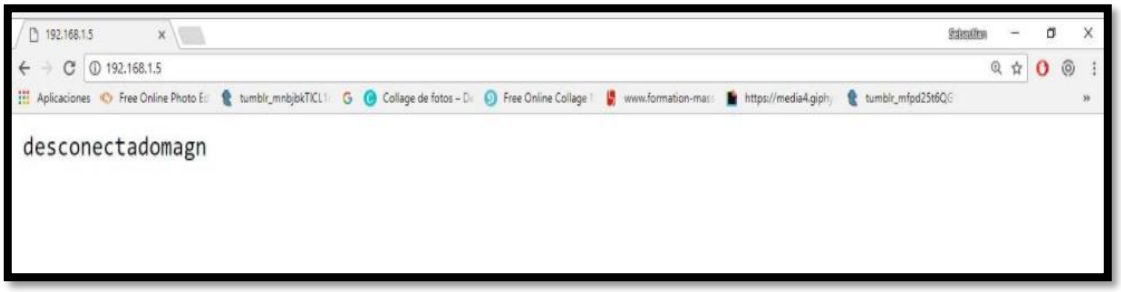


Figura 3-3: Mensaje plano
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Y cuando se aplica la función de encriptación se tiene un mensaje mostrado en la figura 4-3.

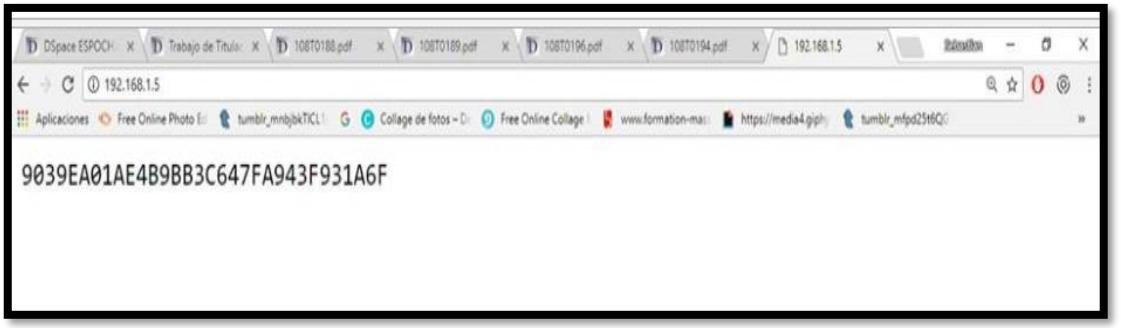


Figura 4-3: Mensaje cifrado
Realizado por: Sebastián Cuenca; Alex Manotoa; 2017

Finalmente, se comprobó que gracias al algoritmo de cifrado AES-128, se pudo cifrar asignando a cada instrucción un mensaje que se envía desde la app, este mensaje se cifra y se dirige por la red hasta que llega al NodeMCU, luego este usa la clave de cifrado para desencriptar el mensaje y de ese modo comparar con variables predefinidas para realizar cualquier acción que requiera.

El proceso inverso de enviar información desde el modulo WiFi hacia la aplicación ocurre de manera similar. Con esto se asegura que ninguna persona ajena podrá descifrar el mensaje que se envía a menos que tenga la clave de encriptación.

3.1.5 Pruebas de la lectura de llaves electrónicas

Para el sistema de respaldo en caso de la caída de la red WiFi, los usuarios existentes en la base de datos en la nube pudieron registrar llaves electrónicas que cuenten con la tecnología NFC como

se ven en la tabla 5-3. Cada elemento que se presente sobre el lector tiene un código único, y ese código se almacena en el microcontrolador para que el usuario pueda tener un control de acceso sin necesidad de ingresar a la aplicación móvil de forma rápida y segura.

Tabla 5-3: Registro del usuario más su llave electrónica NFC.

Correo electrónico de usuario	Tipo de llave electrónica	Código NFC
sebastiancuenca1@gmail.com	Smartphone	1234
reivaj_lexico18@hotmail.es	Smartphone	3293
ale94@gmail.com	Llavero	217561190
ery1993@yahoo.com	Llavero	134120220161
elvis_td@outlook.com	Tarjeta	224423427

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

3.1.6 Alcance de detección de la tarjeta NFC

Se realiza pruebas de la distancia de detección cuando se usan tarjetas electrónicas NFC.

Tabla 6-3: Comunicación llave electrónica de tipo tarjeta.

Pruebas	Alcance (cm)	Estado
1	10	No hay comunicación NFC
2	8	No hay comunicación NFC
3	6	No hay comunicación NFC
4	5	Existe comunicación NFC
5	4	Existe comunicación NFC
6	3	Existe comunicación NFC

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Como se puede observar en la tabla 6-3, para que exista comunicación entre el módulo NFC, y las llaves electrónicas, la distancia mínima requerida es de 5 cm, a partir de la cual habrá conexión y por lo tanto tendrá acceso es decir se abrirá la puerta.

Tabla 7-3: Comunicación llave electrónica de tipo llavero

Pruebas	Alcance (cm)	Estado
1	10	No hay comunicación NFC
2	8	No hay comunicación NFC
3	6	No hay comunicación NFC
4	4	No hay comunicación NFC
5	2	Hay comunicación NFC
6	1	Hay comunicación NFC

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

En cuanto al llavero electrónico se puede observar en la tabla 7-3, que existe conexión a una distancia mínima de 2 cm, y en adelante mientras no supere este parámetro tendrá total acceso.

Tabla 8-3: Comunicación llave electrónica de tipo smartphone

Dispositivos NFC	Alcance (cm)	Estado
2	10	No hay comunicación NFC
3	8	No hay comunicación NFC
4	6	No hay comunicación NFC
5	4	Hay comunicación NFC
6	2	Hay comunicación NFC
7	1	Hay comunicación NFC

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Cualquier teléfono móvil que cuente con la tecnología NFC también puede ser detectado, y para establecer comunicación tiene que estar a una distancia mínima de 4 cm, caso contrario no tendrá acceso como se muestra en la tabla 8-3.

3.1.7 Tiempo de respuesta en procedimiento manual vs automático

Los tiempos se calcularon con la ayuda de un cronómetro y comparando los tiempos que toma en abrir y cerrar la puerta de forma manual, frente al proceso automático como se observa en la tabla 9-3.

Tabla 9-3: Valores de tomados de tiempo del proceso manual vs automático

Pruebas	Tiempo (segundos)			
	Apertura Manual	Cierre Manual	Apertura Automática	Cierre Automático
1	35	28	26	16
2	31	26	22	15
3	26	22	21	13
4	28	20	20	15
5	29	24	18	12
6	26	20	18	11
7	20	18	16	10
8	26	22	17	11
9	27	21	19	13
10	20	17	19	13
11	32	27	16	11
12	25	22	17	12
13	27	23	16	10
14	28	21	17	11
15	21	17	19	13
Promedio	26,73	21,87	18,73	12,4

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Para el procedimiento manual se lo realizó a una distancia de 10 metros, a partir de la cual una persona acorta la distancia hasta llega a la puerta, saca el llavero, verifica la llave y finalmente la introduce en el mecanismo para abrir la puerta y de manera similar para salir de la habitación.

Para el procedimiento automático se tomó el tiempo a partir de cual el usuario abre por primera vez la aplicación, inicia sesión y finalmente da las instrucciones de apertura y cierre de la puerta.

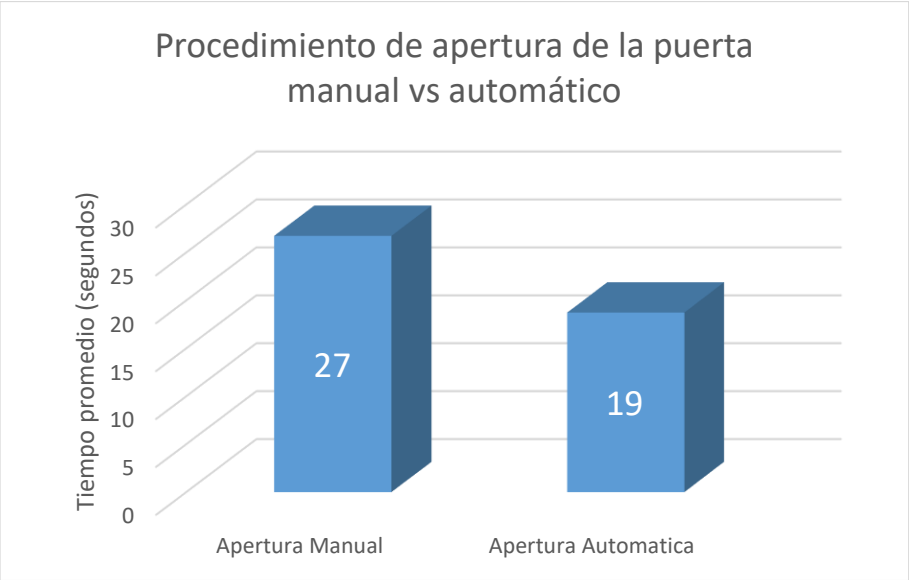


Gráfico 1-3: Comparación del tiempo promedio para un proceso de apertura
Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Los resultados obtenidos, fueron que para el procedimiento manual toma un tiempo promedio de 27 segundos aproximadamente para abrir la puerta y un tiempo de aproximadamente 22 segundos que toma cerrar la puerta, lo cual es un procedimiento lento e incómodo.

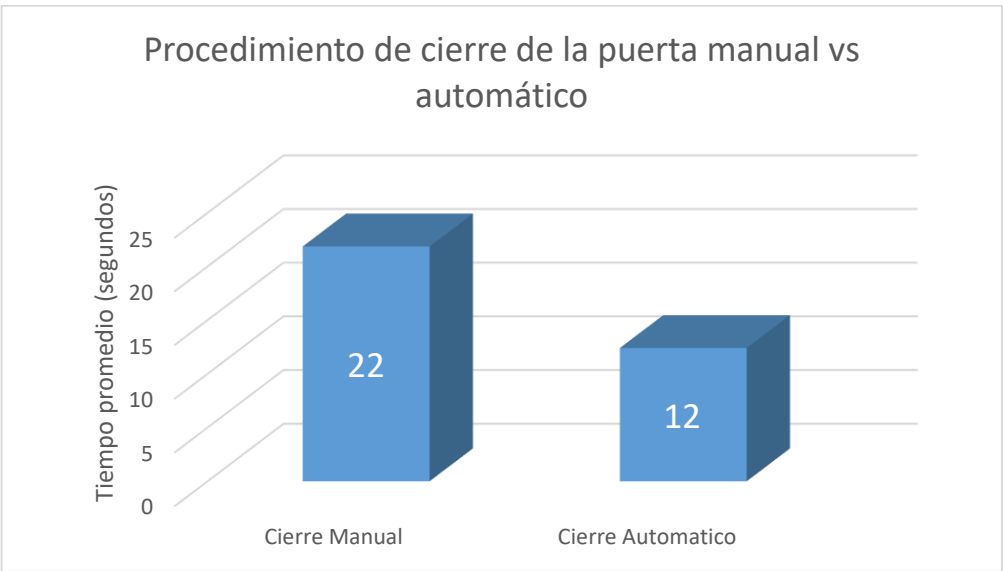


Gráfico 2-3: Comparación del tiempo promedio para un proceso de cierre
Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Mientras que para el procedimiento automático toma un tiempo de aproximadamente 19 segundos abrir la puerta y toma un tiempo de 12 segundos poder cerrarla, con la ventaja que este

procedimiento es más rápido, más sencillo y menos tedioso que el anterior, se visualiza una clara mejorar al implementar el prototipo como se ven en las comparaciones de apertura y cierre de la puerta de los gráficos 1-3 y 2-3 respectivamente.

Porcentaje de mejora frente a la apertura

Aplicando la ecuación 1-3, se verifica la mejora que presenta el sistema automático frente a un sistema manual se tiene:

Ecuación 1-3: Porcentaje de mejora del proceso automático vs manual

$$\textbf{Papertura} = \frac{\boldsymbol{Tiempo\ manual - Tiempo\ automático}}{\boldsymbol{Tiempo\ manual}}\ \boldsymbol{x\ 100}$$

$$\textbf{Papertura} = \frac{\mathbf{26,73 - 18,73}}{\mathbf{26,73}}\ \boldsymbol{x\ 100}$$

$$\textbf{Papertura} = \mathbf{29,93}\ \%$$

De esta forma se comprobó que, con el sistema automático implementado, el proceso de apertura de la puerta es un 29,93% más rápido que un proceso manual.

Porcentaje de mejora frente al cierre de la puerta

Aplicando la ecuación 2-3, se verifica la mejora que presenta el sistema automático frente a un sistema manual se tiene:

Ecuación 2-3: Porcentaje de mejora del proceso automático de cierre frente al manual

$$\textbf{Pcierre} = \frac{\boldsymbol{Tiempo\ manual - Tiempo\ automático}}{\boldsymbol{Tiempo\ manual}}\ \boldsymbol{x\ 100}$$

$$\textbf{Pcierre} = \frac{\mathbf{21,87 - 12,4}}{\mathbf{21,87}}\ \boldsymbol{x\ 100}$$

$$\textbf{Pcierre} = \mathbf{43,29}\ \%$$

De esta forma se comprobó que, con el sistema automático implementado, el proceso de cierre de la puerta es un 43,29% más rápido que un proceso manual.

3.1.8 Consumo de energía del prototipo

Para saber sobre el consumo de corriente y potencia que necesita el circuito electrónico de control, se realizó un censo de carga de cada uno de los elementos utilizados como se detalla en la tabla 10-3.

Tabla 10-3: Censo de carga de los dispositivos electrónicos

COMPONENTE	CORRIENTE (A)	VOLTAJE (V)	POTENCIA (W)
Módulo NodeMCU	0,1	5	0,5
Módulo NFC Pn532	0,03	3,3	0,099
Módulo RTC DS3131	0,0003	5	0,0015
Módulo Display OLEDSSD1606	0,02	5	0,1
Módulo Mp3 DFPlayer	0,02	5	0,1
Buzzer	0,009	5	0,045
Leds	0,02	5	0,1
Láser	0,015	5	0,075
Servomotor 17Kg	0,68	7,3	4,964
Servomotor 20kG	1,65	6,4	10,56
TOTAL	**2,5443**		**16,5445**

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

Se tomó en cuenta todos los componentes descritos anteriormente cuando el sistema está trabajando a plena carga. Tomar en cuenta que el sistema cuando está en reposo consume una corriente de 120 mA.

3.1.9 Rendimiento de la batería.

Para determinar el tiempo de duración de la batería cuando el sistema quede sin conexión a la energía eléctrica, se realiza el siguiente análisis.

Consumo de la batería a plena carga

Ecuación 3-3: Duración de batería

$$\boldsymbol{Duración} = \frac{Capacidad\ de\ la\ batería\ (mAh)}{Consumo\ (mA)}$$

$$\boldsymbol{Duración} = \frac{7\ (Ah)}{2.54\ (A)}$$

$$\boldsymbol{Duración} = 2.75\ horas$$

Consumo de la batería en reposo

$$\boldsymbol{Duración} = \frac{Capacidad\ de\ la\ batería\ (mAh)}{Consumo\ (mA)}$$

$$\boldsymbol{Duración} = \frac{7\ (Ah)}{0.120\ (mA)}$$

$$\boldsymbol{Duración} = 58.33\ horas$$

Tabla 11-3: Consumo de la Batería

Batería	Consumo (A)	Duración (Horas)
Sistema con carga	2.54	2.75
Sistema en reposo	0.120	58.33

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

3.1.10 Análisis económico del prototipo.

A continuación, se presenta la lista de los elementos necesarios para la construcción del prototipo implementado y el costo de los mismos adquiridos en Ecuador.

Tabla 12-3: Lista de los materiales utilizados para la construcción del prototipo.

ESTRUCTURA	ELEMENTOS	CANTIDAD	VALOR $
MÉCÁNICA	Puerta	1	150
	Cerradura	1	38
	Riel	1 m	10,5
	Rodamiento	1	13,75
	Brazo de madera	1	5
	Caja de protección de elementos	1	15
	Piezas 3D	8	48
	Tornillos, tuercas y rodelas	40	2
	Caja Chapa	1	50
	Correa dentada	2 m	5,6
	Costo total de la estructura mecánica		**337,85**
ELECTRÓNICA	Módulo NodeMCU	1	13
	Módulo NFC Pn532	1	23
	Módulo RTC DS3131	1	5
	Pila Litio 3V	1	2
	Módulo Display OLEDSSD1606	1	12,5
	Módulo Mp3 DFPlayer	1	5
	Tarjeta SD 4GB	1	6
	Buzzer	1	1
	Speaker 8ohm	1	1,5

	Sensor magnético	1	3
	Optoacoplador (Sensor de herradura)	1	1
	Láser	1	1,5
	Fotoresistencia	1	0,8
	Fuente Step-Down Mp1584	3	9
	Placa impresa CNC	1	20
	Batería Seca 12V-7AH	1	35
	Cargador de Batería y fuente de alimentación	1	40
	Servomotor 17Kg	1	22
	Servomotor 20kG	1	45
	Transistores	3	0,45
	Resistencias	11	0,55
	Leds	3	0,6
	Diodos rectificadores	4	0,8
	Capacitores	10	1,5
	Jack DC	1	0,5
	Espadines	5	5
	Fusible 2,5 A	1	1,5
	Cables de conexión	7 m	3,5
	Switches	2	1,5
	Regulador 7833	1	1
	Costo total de la parte electrónica		**263,2**
COSTO TOTAL DEL PROTOTIPO			601,05

Realizado por: Manotoa Alex; Cuenca Sebastián, 2017.

De acuerdo a la tabla 12-3, la estructura mecánica presenta un costo de 337,85 dólares americanos (USD), y 263 USD de la parte electrónica. Sumados dan un costo total de desarrollo del prototipo de 601,05 USD. No se tomó en cuenta el valor del desarrollo de la aplicación móvil.

Algunos precios de ciertos elementos de la estructura mecánica como la puerta, cerradura, rodamientos, cajas de protección pueden ser retirados los mismos se encuentran instalados en la habitación de una residencia.

Hay que tener en cuenta que este dispositivo electrónico posee una gran funcionalidad, seguridad, versatilidad e innovación que ofrece el sistema, en comparación a otros dispositivos similares existentes en el mercado.

CONCLUSIONES

- El diseño del prototipo está compuesto por un sistema mecánico y electrónico que, implementado sobre una puerta se logra abrirla y/o cerrarla de forma automática, cumpliendo con los requerimientos planteados en el proyecto de investigación.

- Debido al uso de la placa de desarrollo NodeMCU, se consigue que el dispositivo electrónico pueda conectarse a una red WiFi permitiendo de este modo el intercambio de información.

- La app desarrollada es compatible con dispositivos móviles que cuenten con el sistema operativo Android a partir de la versión 5.0. La aplicación envía instrucciones hacia módulo WiFi conectado a la red y de esta manera se controla la apertura y cierre de la puerta.

- La aplicación móvil cuenta con un sistema de autenticación de usuarios mediante un correo electrónico y contraseña que están almacenados en una base de datos en tiempo real en la nube proporcionado por el servicio de Google *Firebase,* con esto se asegura que solamente usuarios autorizados puedan controlar el sistema electrónico.

- La seguridad de datos inalámbricos se consigue con la implementación del algoritmo de encriptación simétrico AES con una clave de 128 bits. Los mensajes enviados y recibidos tanto en la placa de desarrollo como en la aplicación móvil son encriptados y desencriptados eficazmente logrando un nivel de seguridad bastante confiable ante los ataques informáticos en la comunicación.

- Ante la caída de la red WiFi se implementa un sistema basado en la tecnología NFC mediante un registro de llaves electrónicas por usuario, brindando de esta manera un control de acceso sin hacer uso de la aplicación móvil.

- Ante cortes eléctricos, el prototipo tiene a disposición un sistema de respaldo de energía que consta de una batería y un cargador automático, con lo cual el sistema electrónico se mantiene en perfecto funcionamiento.

- Se comprueba el funcionamiento del prototipo en la puerta de una casa residencial tanto de su control como de su conectividad y tiempo de respuesta obteniendo resultados satisfactorios.

RECOMENDACIONES

- Dentro de los materiales usados para la fabricación del prototipo de cerradura electrónica se debe verificar cada elemento del sistema mecánico este a nivel, y los actuadores se encuentren calibrados correctamente, pues de esto depende que el prototipo funcione en óptimas condiciones.

- En cuanto a la selección de los servomotores, se tiene que realizar cálculos adecuados acerca del torque necesario para mover los mecanismos.

- Se recomienda actualizar el firmware de la tarjeta de desarrollo NodeMCU, para que el módulo funcione de manera correcta.

- Al realizar la programación del módulo WiFi, se debe descargar las librerías compatibles que permitan el funcionamiento de los elementos electrónicos conectados de forma correcta.

- Se recomienda que en la configuración del router que sirve como punto de acceso de los diferentes dispositivos conectados, se reserve una dirección IP fija, para el módulo WiFi y establecer de manera sencilla la comunicación con la aplicación móvil.

- Acerca de la programación en Android Studio, se debe incluir las librerías necesarias, declarar comandos que permitan almacenar las variables esenciales, pues estas son volátiles. También se debe brindar los permisos que requiere la app desarrollada para su ejecución en un Smartphone.

- Se debe constatar que las librerías de encriptación y desencriptación tanto de la aplicación móvil como del módulo WiFi sean compatibles. Es decir que el mismo mensaje que se envía, sea el mismo que se reciba desde una interfaz hacia otra y viceversa.

- Identificar previamente en la hoja de datos los pines SCL y SDA del módulo NodeMCU, para conectarlos con la placa lectora NFC y así exista una correcta comunicación I^2C.

- Medir los datos de corriente que consume todo el circuito electrónico, y entonces elegir una batería adecuada que dote al sistema de energía suficiente, para mantenerlo siempre activado.

- Se recomienda hacer uso de la información recolectada en el presente trabajo de investigación, con el fin de mejorar el prototipo o ayudar en proyectos futuros basados en dispositivos que cuenten con comunicación WiFi.

BIBLIOGRAFÍA

¿CÓMO FUNCIONA LO INALÁMBRICO? [En línea] 2013. [Consulta: 17 de Septiembre de 2017.] Disponible en: https://arodriguezr.wordpress.com/como-funciona-lo-inalambrico/.

BATERIAS Y ACUMULADORES. [En línea] [Consulta: 28 de Septiembre de 2017.] Disponible en: http://www.areatecnologia.com/baterias-y-acumuladores.htm.

Ciclo de vida de una aplicación Android. [blog] 24 de Febrero de 2011. [Consulta: 26 de Septiembre de 2017.] Disponible en: http://droideando.blogspot.com/2011/02/ciclo-de-vida-de-una-aplicacion-android.html.

Definición de Router. [En línea] [Consulta: 25 de Septiembre de 2017.] Disponible en: https://www.definicionabc.com/tecnologia/router.php.

Desarrollo de apps. [blog] 21 de Marzo de 2017. [Consulta: 16 de Setiembre de 2017.]Disponible en : https://www.yeeply.com/blog/tipos-de-app-y-para-que-sirven/.

Etapas de carga de una batería. [En línea] 2016. [Consulta: 28 de Septiembre de 2017.] Disponible en: http://saguerelectronica.webnode.cl/products/etapas-de-carga-de-una-bateria/.

Fotorresistencia. [En línea] 11 de Enero de 2017. [Consulta: 15 de Septiembre de 2017.] Disponible en: https://ingenieriaelectronica.org/fotorresistencia-definicion-caracteristicas-y-tipos/.

GONZÁLES, Antony. *El módulo DS3231, un reloj para Arduino.* [En línea] 22 de Mayo de 2014. [Consulta: 19 de Septiembre de 2017.] Disponible en: http://panamahitek.com/el-modulo-ds3231-un-reloj-para-arduino/.

GONZÁLES, Antony. *Como funciona un servomotor.* [En línea] 2 de Diciembre de 2016. [Consulta: 15 de Septiembre de 2017.] Disponible en: http://panamahitek.com/que-es-y-como-funciona-un-servomotor/.

GONZÁLEZ, Daniel. *Conociendo ESP8266 / NodeMcu.* [En línea] 08 de Febrero de 2017. [Consulta: 13 de Septiembre de 2017.] Disponible en: http://danielmartingonzalez.azurewebsites.net/conociendo-esp8266-nodemcu-el-modulo-wifi-para-iot/.

Introducción a SolidWorks. [En línea] [Consulta: 28 de Septiembre de 2017.] Disponible en: http://www.marcombo.com/Descargas/9788426714589-SolidWorks/descarga_primer_capitulo_libro_solidworks.pdf.

RODRÍGUEZ, Jose Maria & SAN MARTÍN, Maimon. *El modelo OSI y las direcciones IP.* [En línea] [Consulta: 24 de Septiembre de 2017.] Disponible en : https://www.adrformacion.com/udsimg/wserver12/1/redes2.pdf.

La comunicación inalámbica. [En línea] Junio de 2005. [Consulta: 15 de Septiembre de 2017.] Disponible en: http://www.aulaclic.es/articulos/wifi.html.

Ley de Inercia. [En línea] 2010. [Consulta: 15 de Octubre de 2017.] Disponible en: http://contenidosdigitales.ulp.edu.ar/exe/fisica/1_ley_de_inercia.html.

LLAMAS, Luis. *Ingeniería Informática y diseño.* [En línea] [Consulta: 19 de Septiembre de 2017.] Disponible en: https://www.luisllamas.es/arduino-mp3-dfplayer-mini/.

MARRERO, Yran. *Criptografía como un Elemento de Seguridad.* [En línea] 18 de Septiembre de 2003. [Consulta: 16 de Septiembre de 2017.] Disponible en: http://bvs.sld.cu/revistas/aci/vol11_6_03/aci11603.htm.

Mini pantalla OLED . [En línea] [Consulta: 19 de Septimbre de 2017.] Disponible en: http://tienda.bricogeek.com/descatalogado/483-mini-pantalla-oled-128x64.html.

MUÑOZ, Yolanda. *¿Qué tipos de cerraduras existen?* [En línea] [Consulta: 12 de Septiembre de 2017.] Disponible en: https://comunidad.leroymerlin.es/t5/Bricopedia-Reparaci%C3%B3n-y/Qu%C3%A9-tipos-de-cerraduras-existen/ta-p/79408#.

POUSA, Adrián. *ALGORITMO DE CIFRADO SIMÉTRICO AES.* [En línea][Tesis de maestría].Universidad Nacional de la Plata,Facultad de Informática,Lugar(Argentina). Diciembre de 2011. [Consulta: 27 de Septiembre de 2017] Disponible en: http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf.

Programación Android, Service. [En línea] Febrero de 13 de 2014. [Consulta: 09 de Octubre de 2017.] Disponible en: http://www.proyectosimio.com/es/programacion-android-service/.

Programación de desarrollo de aplicaciones móviles. [blog] 5 de junio de 2015. [Consulta: 02 de Octubre de 2017.] Disponible en: http://aplicmovil101desmovil.blogspot.com/2015/06/politica-de-eliminacion-y-el-ciclo-de.html.

Sensores Fundamentos. [En línea] [Consulta: 14 de Septiembre de 2017.] Disponible en: http://cmapspublic2.ihmc.us/rid=1H2B63T5G-1SLKJ1L-J52/Sensores%20fundamentos,%20tipos%20y%20caracter%C3%ADsticas.pdf.

Servomotores. [En línea] [Consulta: 15 de Septiembre de 2017.] Disponible en: http://www.areatecnologia.com/electricidad/servomotor.html.

Tecnología Wi-Fi. [En línea] [Consulta: 16 de Septiembre de 2017.] Disponible en: https://www.ecured.cu/Tecnolog%C3%ADa_Wi-Fi.

Tecnologias de Comunicacion Inalambrica. [En línea] Diciembre de 2002. [Consulta: 15 de Septiembre de 2017.] Disponible en: http://www.eveliux.com/mx/Tecnologias-de-Comunicacion-Inalambrica.html.

Tipos de cerraduras. [En línea] 11 de Octubre de 2016. [Consulta: 12 de Septiembre de 2017.] Disponible en: http://www.mastiposde.com/cerraduras.html.

VIALFA, Carlos. *TCP/IP*. [En línea] 7 de Marzo de 2017. [Consulta: 24 de Septiembre de 2017.] Disponible en: http://es.ccm.net/contents/282-tcp-ip.

GONZÁLEZ, Victor. *El ciclo de vida de una aplicación de Android.* [En línea] 10 de diciembre de 2013. [Consulta: 02 de Octubre de 2017.] Disponible en: https://www.androidsis.com/el-ciclo-de-vida-de-una-aplicacion-de-android/.

ZAMORA, Jose Angel. *¿Qué es Firebase?* [En línea] 19 de 05 de 2016. [Consulta: 27 de Septiembre de 2017.] Disponible en: https://elandroidelibre.elespanol.com/2016/05/firebase-plataforma-desarrollo-android-ios-web.html

ANEXOS

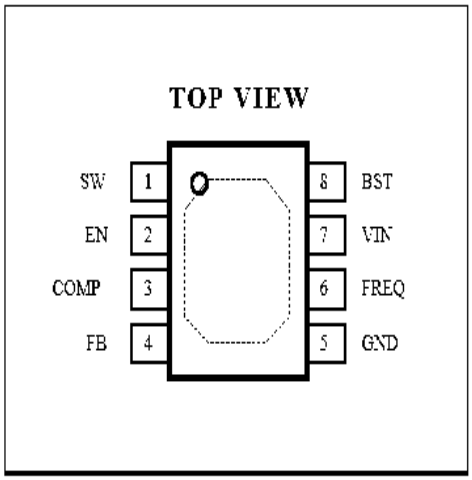
ANEXO A: Datos Técnicos de los módulos Electrónicos

- Convertidor DC-DC Step-Down MP 1584.

* For Tape & Reel, add suffix –Z (e.g. MP1584EN–Z);

For RoHS Compliant Packaging, add suffix –LF. (e.g. MP1584EN–LF–Z)

PACKAGE REFERENCE



ABSOLUTE MAXIMUM RATINGS (1)

Supply Voltage (V_{IN}).....–0.3V to +30V

Switch Voltage (V_{SW})..... –0.3V to V_{IN} + 0.3V

BST to SW .....–0.3V to +6V

All Other Pins.....–0.3V to –6V

Continuous Power Dissipation (T_A= +25°C)(2)

..... 2.5W

Junction Temperature.....150 °C

Lead Temperature .....260 °C

Storage Temperature..... –65°C to +150 °C

Recommended Operating Conditions (3)

Supply Voltage V_{IN} .....4.5V to 28V

Output Voltage V_{OUT}.....0.8V to 25V

Operating Junct. Temp (T_J) .....–20°C to –125°C

Thermal Resistance (4)	θ_{JA}	θ_{JC}	
SOIC8E	50	10...	°C/W

Notes:

1) Exceeding these ratings may damage the device.

2) The maximum allowable power dissipation is a function of the maximum junction temperature T_J(MAX), the junction-to-ambient thermal resistance θ_{JA}, and the ambient temperature T_A. The maximum allowable continuous power dissipation at [illegible] P_D(MAX)=(T_J(MAX)-T_A)/θ_{JA}. Exceeding the maximum allowable power dissipation will cause excessive die temperature, and the regulator will go into thermal shutdown. Internal thermal shutdown circuitry protects the device from permanent damage.

3) The device is not guaranteed to function outside of its operating conditions.

4) Measured on JESD51-7, 4-layer PCB.

ELECTRICAL CHARACTERISTICS

V_{IN} = 12V, V_{EN} = 2.5V, V_{COMP} = 1.4V, T_A = +25□C, unless otherwise noted.

Parameter	Symbol	Condition	Min	Typ	Max	Units
Feedback Voltage	V_{FB}	4.5V < V_{IN} < 28V	0.776	0.8	0.824	V
Upper Switch On Resistance	$R_{DS(ON)}$	V_{BST} – V_{SW} = 5V		150		mΩ
Upper Switch Leakage		V_{EN} = 0V, V_{SW} = 0V, V_{IN} = 28V		1		μA
Current Limit			4.0	4.7		A
COMP to Current Sense Transconductance	G_{CS}			9		A/V
Error Amp Voltage Gain [1,3]				200		V/V
Error Amp Transconductance		I_{COMP} = ±3μA	40	60	80	μA/V
Error Amp Min Source current		V_{FB} = 0.7V		5		μA
Error Amp Min Sink current		V_{FB} = 0.9V		–5		μA
VIN UVLO Threshold			2.7	3.0	3.3	V
VIN UVLO Hysteresis				0.35		V
Soft-Start Time [1,3]		0V < V_{EA} < 0.8V		1.5		ms
Oscillator Frequency		R_{FB-G} = 100kΩ		900		kHz
Shutdown Supply Current		V_{EN} = 0V		12	20	μA
Quiescent Supply Current		No load, V_{FB} = 0.9V		100	125	μA
Thermal Shutdown				150		□C
Thermal Shutdown Hysteresis				15		□C
Minimum Off Time [1,3]				100		ns
Minimum On Time [1,3]				100		ns
EN Up Threshold			1.35	1.5	1.65	V
EN Hysteresis				300		mV

Note:

3) Guaranteed by design.

- Características Técnicas módulo DFplayer Mini.

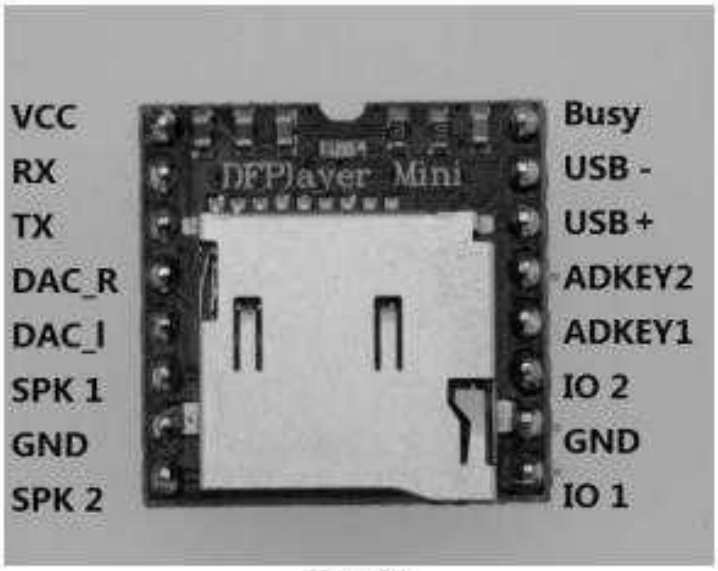


Figure 2.1

No	Pin	Description	Note
1	VCC	Input Voltage	DC3.2–5.0V;Type: DC4.2V
2	RX	UART serial input	
3	TX	UART serial output	
4	DAC_R	Audio output right channel	Drive earphone and amplifier
5	DAC_L	Audio output left channel	Drive earphone and amplifier
6	SPK2	Speaker-	Drive speaker less than 3W
7	GND	Ground	Power GND
8	SPK1	Speaker+	Drive speaker less than 3W
9	IO1	Trigger port 1	Short press to play previous(long press to decrease volume)
10	GND	Ground	Power GND
11	IO2	Trigger port 2	Short press to play next（long press to increase volume）
12	ADKEY1	AD Port 1	Trigger play first segment
13	ADKEY2	AD Port 2	Trigger play fifth segment
14	USB+	USB+ DP	USB Port
15	USB-	USB- DM	USB Port
16	BUSY	Playing Status	Low means playing \High means no

- Características Técnicas módulo RTC DS3231.

RECOMMENDED DC OPERATING CONDITIONS

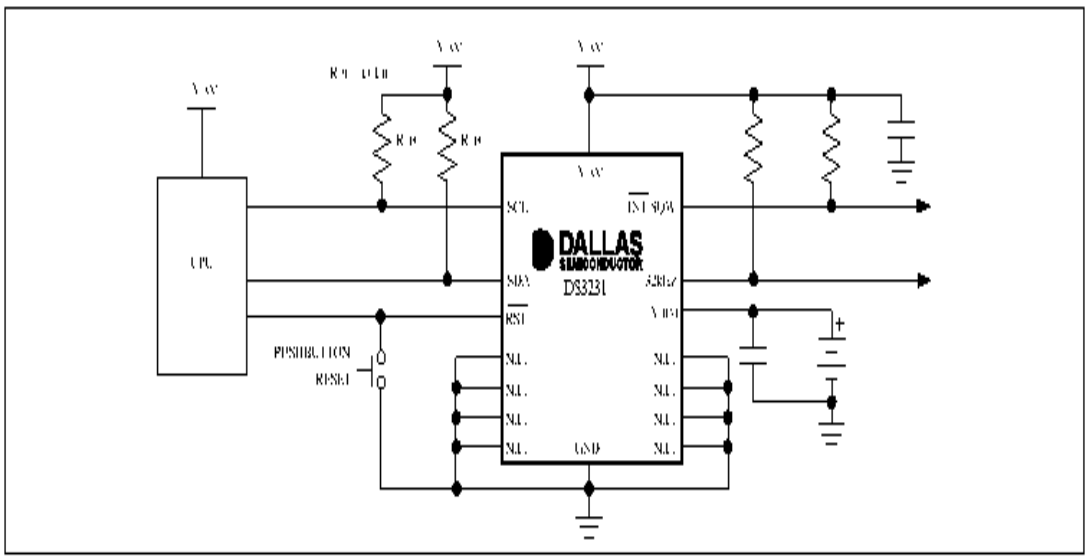
(T_A = T_{MIN} to T_{MAX}, unless otherwise noted.) (Notes 1, 2)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}		2.3	3.3	5.5	V
	V_{BAT}		2.3	3.0	5.5	V
Logic 1 Input SDA, SCL	V_{IH}		0.7 x V_{CC}		V_{CC} + 0.3	V
Logic 0 Input SDA, SCL	V_{IL}		-0.3		+0.3 x V_{CC}	V
Pullup Voltage (SDA, SCL, 32kHz, INT/SQW)	V_{PU}	V_{CC} = 0V			5.5V	V

ELECTRICAL CHARACTERISTICS

(V_{CC} = 2.3V to 5.5V, V_{CC} > V_{BAT}, T_A = T_{MIN} to T_{MAX}, unless otherwise noted.) (Typical values are at V_{CC} = 3.3V, V_{BAT} = 3.0V, and T_A = +25°C, unless otherwise noted.) (Notes 1, 2)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
Active Supply Current	I_{CCA}	(Notes 3, 4)	V_{CC} = 3.63V			200	µA
			V_{CC} = 5.5V			300	
Standby Supply Current	I_{CCS}	I²C bus inactive, 32kHz output on, SQW output off (Note 4)	V_{CC} = 3.63V			110	µA
			V_{CC} = 5.5V			170	
Temperature Conversion Current	$I_{CCSCONV}$	I²C bus inactive, 32kHz output on, SQW output off	V_{CC} = 3.63V			575	µA
			V_{CC} = 5.5V			650	
Power-Fail Voltage	V_{PF}			2.45	2.575	2.70	V
Logic 0 Output, 32kHz, INT/SQW, SDA	V_{OL}	I_{OL} = 3mA				0.4	V
Logic 0 Output, RST	V_{OL}	I_{OL} = 1mA				0.4	V
Output Leakage Current 32kHz, INT/SQW, SDA	I_{LO}	Output high impedance		-1	0	+1	µA
Input Leakage SCL	I_{LI}			-1		+1	µA
RST Pin I/O Leakage	I_{OL}	RST high impedance (Note 5)		-200		+10	µA



- Características Técnicas módulo SSD1306.

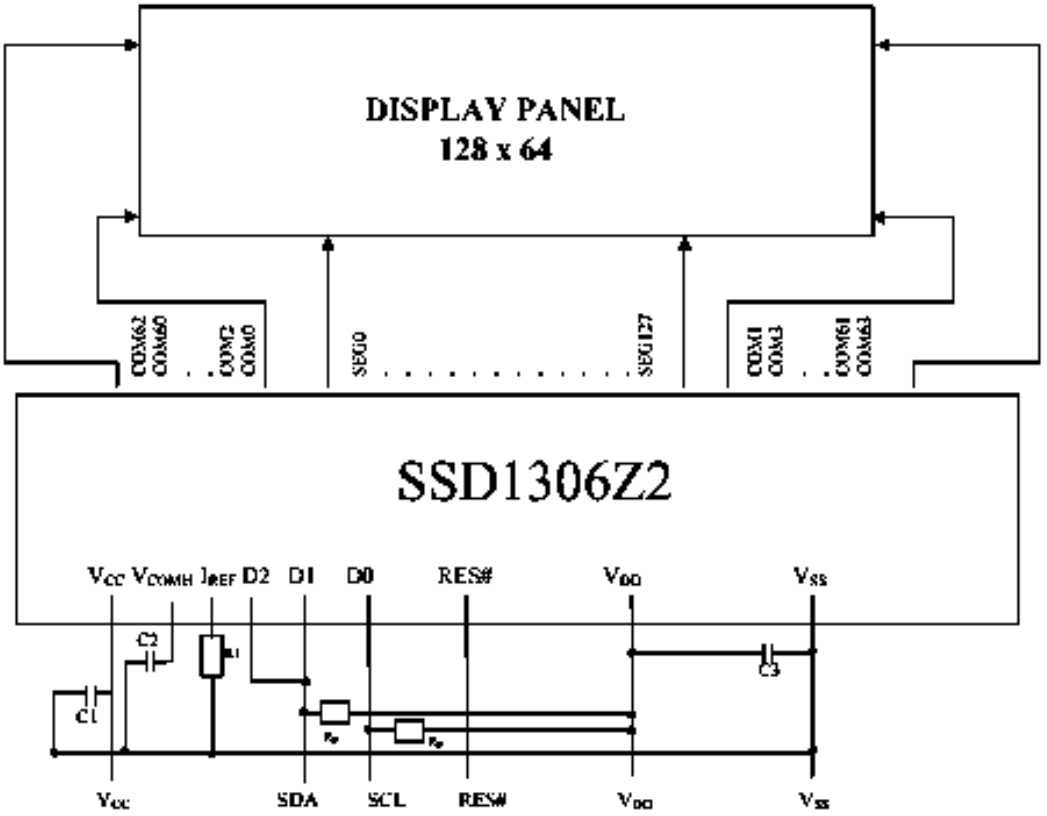
  - Resolution: 128 x 64 dot matrix panel
  - Power supply
    - V_{DD} = 1.65V to 3.3V, < V_{BAT} for IC logic
    - V_{BAT} = 3.3V to 4.2V for charge pump regulator circuit
    - V_{CC} = 7V to 15V for Panel driving
  - For matrix display
    - Segment maximum source current: 100uA
    - Common maximum sink current: 15mA
    - 256 step contrast brightness current control
  - Embedded 128 x 64 bit SRAM display buffer
  - Pin selectable MCU Interfaces:
    - 8-bit 6800/8080-series parallel interface
    - 3 /4 wire Serial Peripheral Interface
    - I^2C Interface
  - Screen saving continuous scrolling function in both horizontal and vertical direction
  - Internal charge pump regulator
  - RAM write synchronization signal
  - Programmable Frame Rate and Multiplexing Ratio
  - Row Re-mapping and Column Re-mapping
  - On-Chip Oscillator
  - Chip layout for COG & COF
  - Wide range of operating temperature: -40°C to 85°C

3 ORDERING INFORMATION

Table 3-1: Ordering Information

Ordering Part Number	SEG	COM	Package Form	Reference	Remark
SSD1306Z2	128	64	COG	9	o Min SEG pad pitch : 47um o Min COM pad pitch : 40um o Die thickness: 300 +/- 25um
SSD1306TR1	104	48	TAB	12, 61	o 35mm film, 4 sprocket hole, Folding TAB o 8-bit 80 / 8-bit 68 / SPI / I^2C interface o SEG, COM lead pitch 0.1mm x 0.997 =0.0997mm o Die thickness: 457 +/- 25um

The configuration for I^2C interface mode is shown in the following diagram:
(V_{DD}= 1.65V ~ 3.3V, V_{CC}=7V~15V, I_{REF}=12.5uA)



Pin connected to MCU interface: RES#, SDA, SCL
Pin internally connected to V_{SS}: BS0, BS2, CL, D[7:3], E, R/W#, CS#, D/C#, BGGND
Pin internally connected to V_{DD}: BS1, CLS
V_{BAT}, C1P, C1N, C2P, C2N, V_{BREF}, FR should be left open.

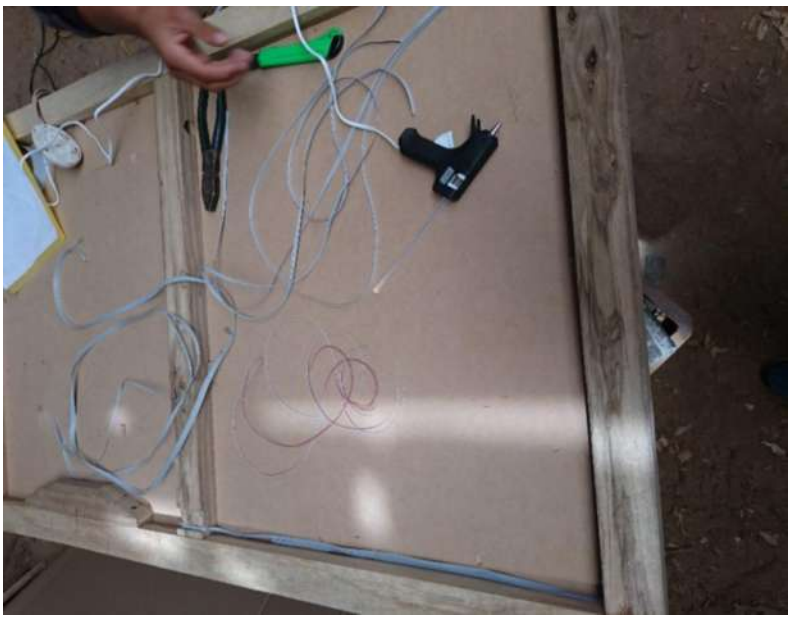
C1, C2: 2.2uF [1]
C3: 1.0uF [1]
R_P : Pull up resistor

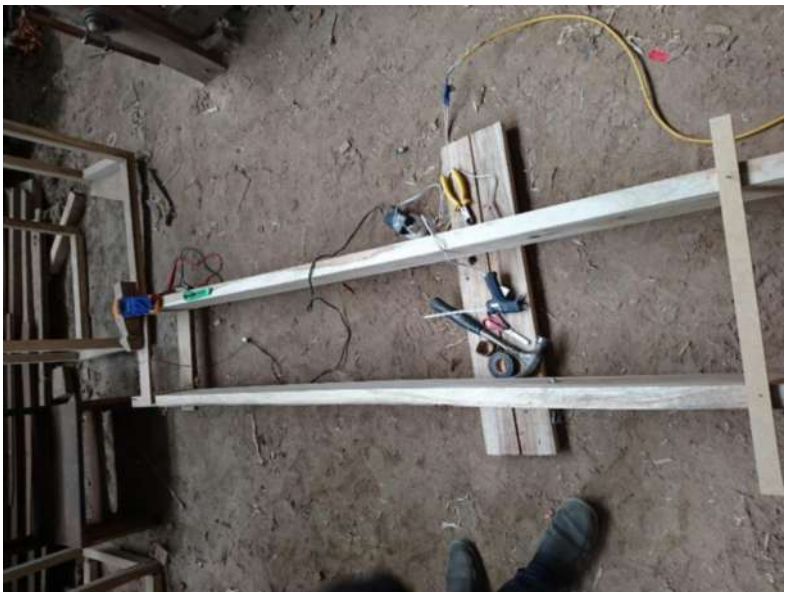
Voltage at I_{REF} = V_{CC} – 2.5V. For V_{CC} = 7.5V, I_{REF} = 12.5uA:
R1 = (Voltage at I_{REF} - V_{SS}) / I_{REF}
= (7.5-2.5) / 12.5u
=400KΩ

Note
[1] The capacitor value is recommended value. Select appropriate value against module application.

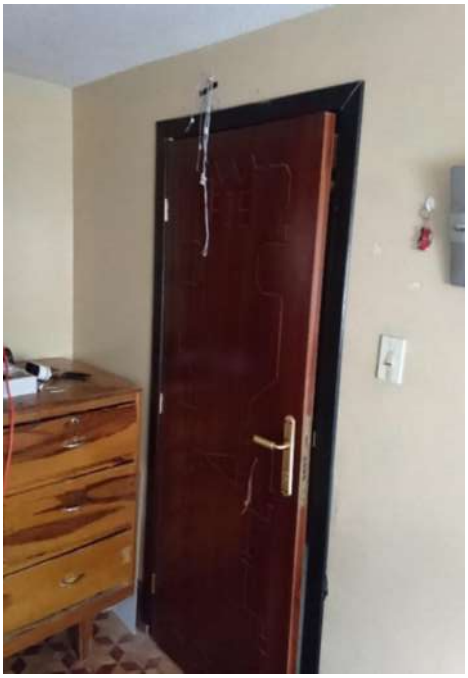
ANEXO B: Proceso de construcción del prototipo.

Cableado interno de la puerta y el marco.

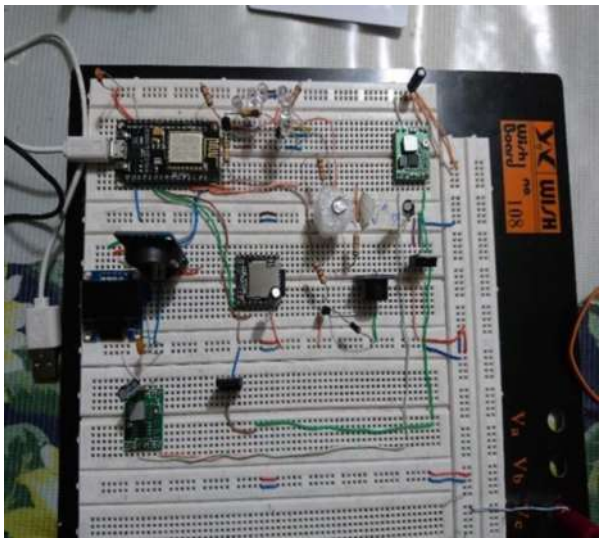


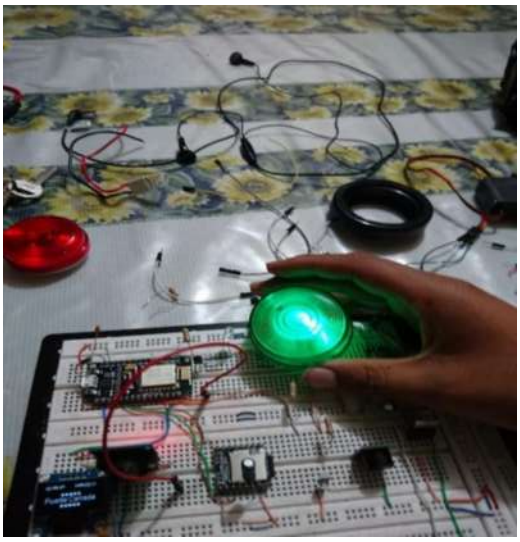


Instalación de la puerta terminada.

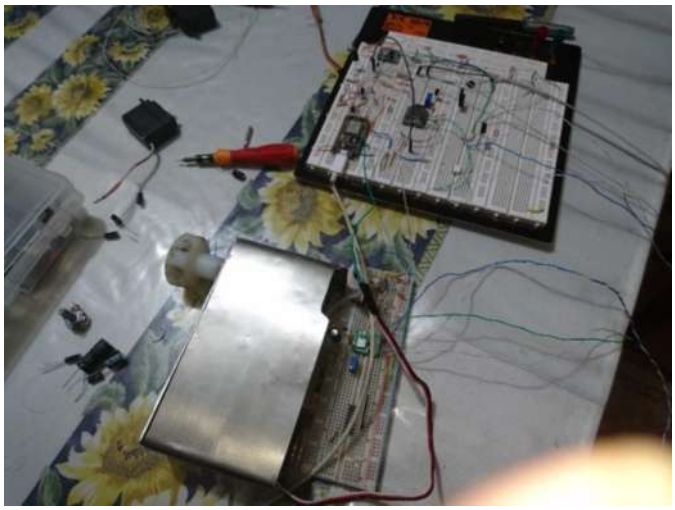


Pruebas del circuito en la protoboard.



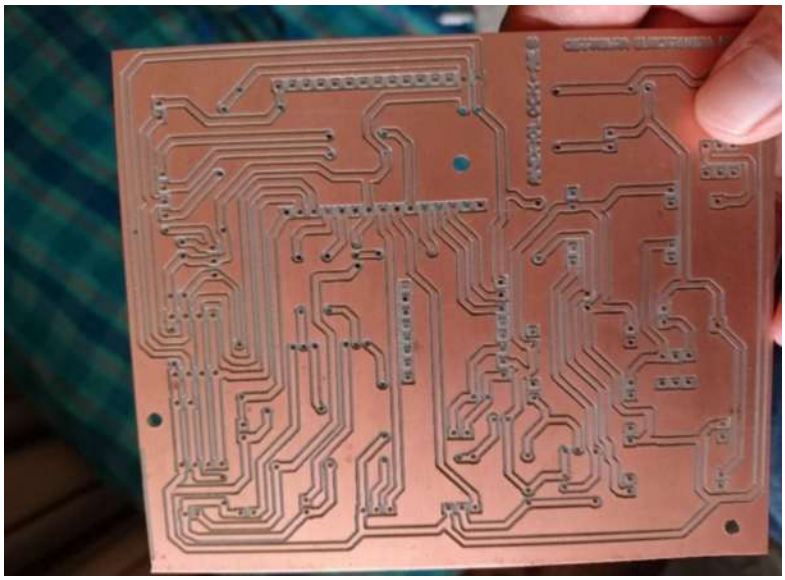


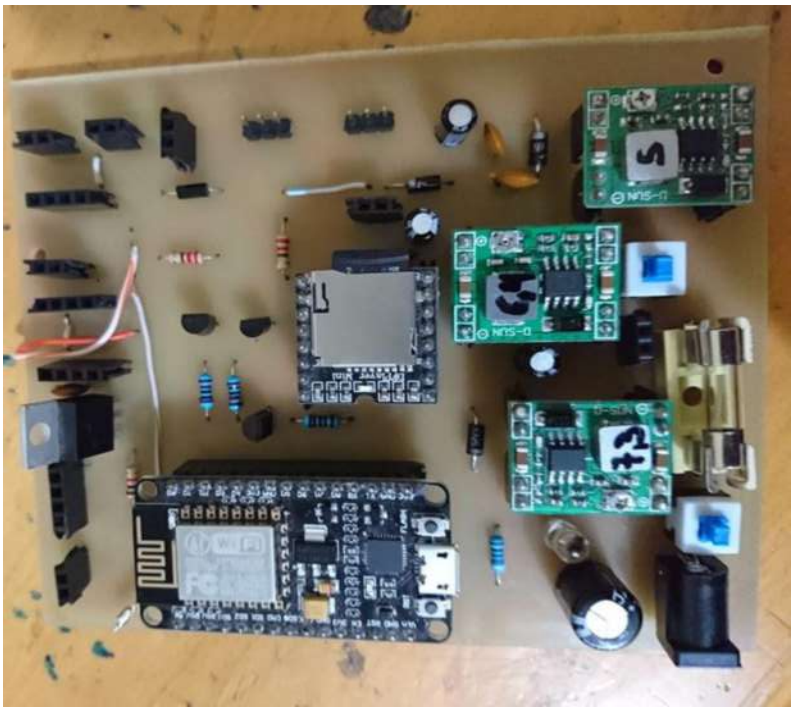
Calibración de la cerradura.



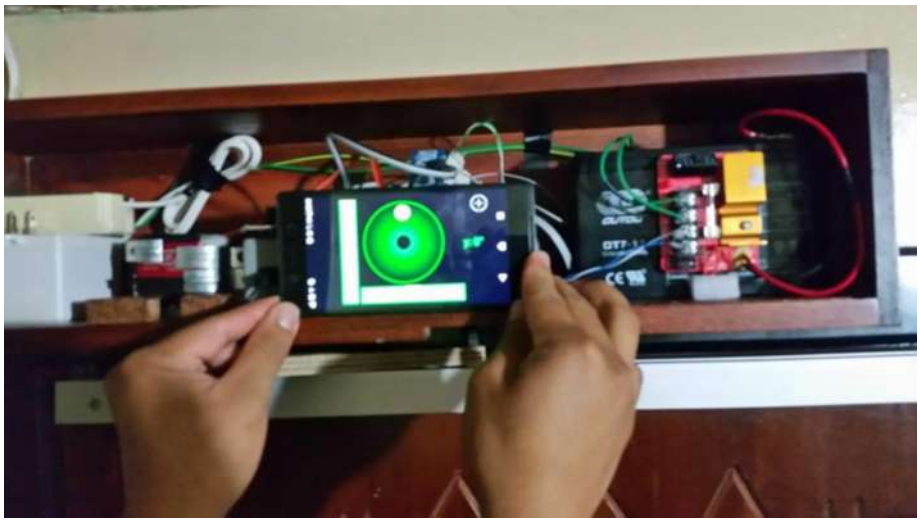
Backap de Energía para un buen funcionamiento del circuito.

Placa de circuito impreso





Puesta a nivel del mecanismo.



Prototipo terminado y funcionando correctamente

ANEXO C: Manual de usuario de la aplicación móvil.

Manual de Usuario

(Manejo de la aplicación móvil para el control del sistema ANDROLOCK- AES)

ANDROLOCK-AES es un sistema electrónico junto con una aplicación, creada he implementada con el objetivo de ofrecer una interfaz gráfica, llamativa y multifuncional entre el usuario y el prototipo que se diseñó.

Gracias al uso de esta aplicación se puede tener un mejor manejo y control del prototipo el mismo que consiste en retener y soltar los pestillos y seguros de la cerradura electrónica junto con la apertura y cierre de la puerta.

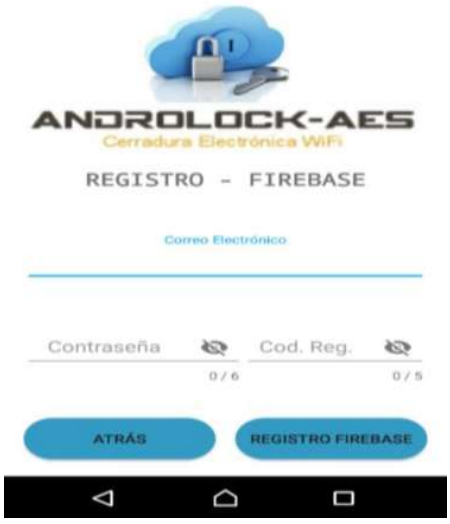
Requerimientos Técnicos:

- Dispositivos móviles.
- Sistema Operativo Android.
- Versión iguales o superiores a 5.0.
- Clave de registro @12Ab.

Acceso al Sistema:

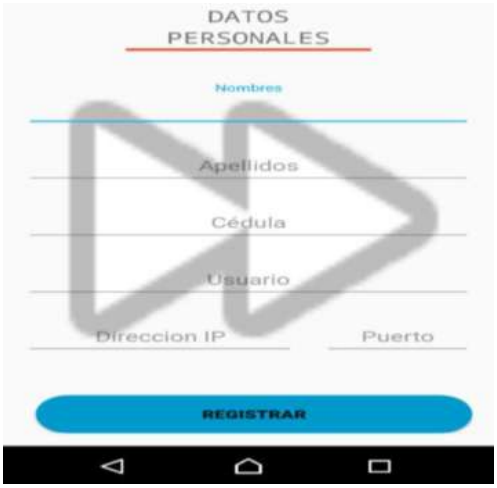
Para poder ingresar al sistema de control primero tiene que registrarse en la base de datos dando clic en el botón **REGISTRESE AQUÍ.** Como se puede observar en la siguiente figura.

Una vez que haya hecho clic en el botón se direccionará a la siguiente ventana. Como se puede observar en la figura. En esta pantalla tiene que llenar con sus datos de correo electrónico, contraseña, y la clave de acceso, debajo de cada espacio en blanco. Una vez que haya llenado todos los parámetros dar clic en el botón **REGISTRÓ FIREBASE.**



Ahora se requiere registrar los datos personales del usuario es recomendable que

llene con datos reales ya que después se podrá visualizar en la aplicación móvil. Una vez concluido este proceso, dar clic sobre el botón ***REGISTRAR*** para completar la acción de registro del nuevo usuario.

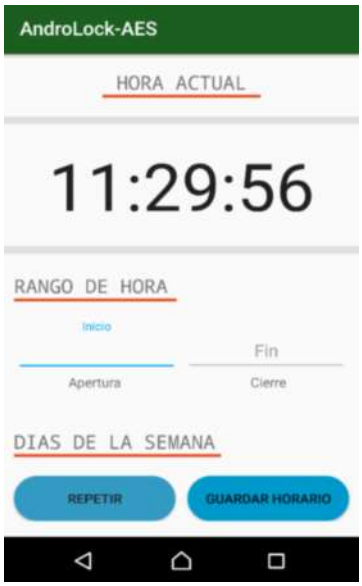


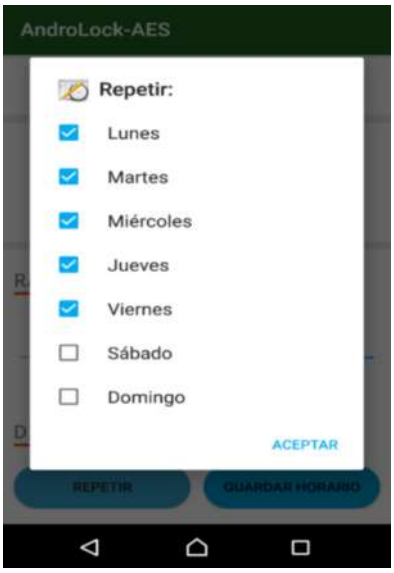
La ventana que se muestra a continuación es el inicio de sesión donde tendrá que reingresar los datos de correo electrónico más la contraseña, y hacer clic en **ACCEDER**, esto se lo hace con el objetivo de verificar el registro que se realizó anteriormente y a la vez iniciar sesión, terminado con estos pasos tendrá acceso y control completo del sistema.

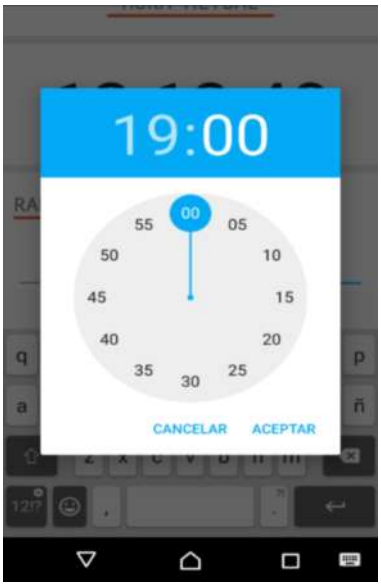
En esta sección se puede observar que se ingresó correctamente y está listo para usar los diferentes controles que posee la aplicación móvil, así tenemos como primera instancia una imagen de un candado cerrado, que al tocarlo este se activa de manera instantánea lo que quiere decir la puerta empezará a abrir y el candado cambiará de estado también como se puede observar en las imágenes presentadas. Ahora si se desea cerrar la puerta, se tiene que presionar sobre el candado abierto por unos 3 segundos de esta forma se enviará una petición para que realice la apertura de la puerta.

A continuación, se tiene también la opción de abrir y cerrar la puerta de manera automática para lo cual deslizando la pantalla hacia la derecha entraremos a la opción de control temporal, como se puede ver en la figura, para realizar el control mantener presionado sobre el icono unos 2 segundos luego soltarlo, entonces empezara el proceso de apertura y cierre automático de la puerta. La apertura es inmediata mientras que para el cierre se tiene que esperar unos segundos.

En la parte inferior de la pantalla se puede observar que tenemos una opción de apertura programada para lo cual tenemos que mantener presionado sobre el botón para ingresar al menú de programación de la puerta, al ejecutar esta opción entramos a la configuración donde tenemos la posibilidad de seleccionar la apertura y cierre a libre elección del usuario, sea este por días o por horas. Como se puede apreciar en las siguientes figuras.



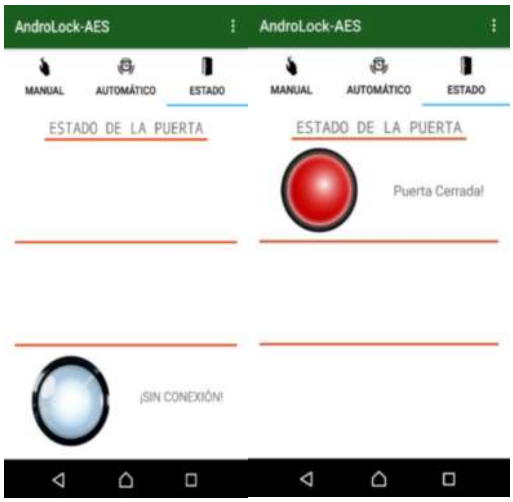




Una vez seleccionado y elegido cada parámetro damos clic en GUARDAR HORARIO y se guardarán los datos de programación. En la figura anterior podemos ver este proceso.

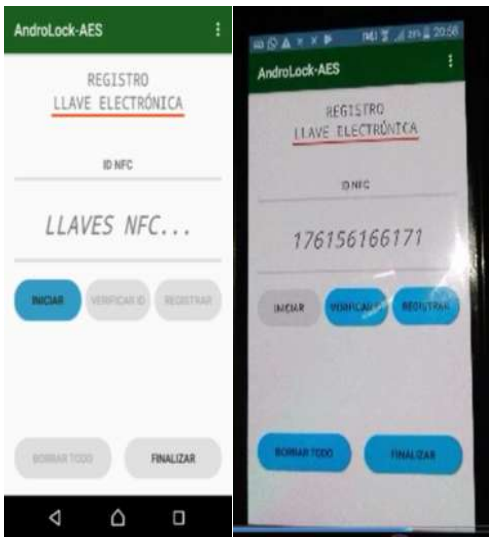
Adicional a esto tenemos la posibilidad de ver en qué estado se encuentra la puerta si es abierta, cerrada o no existe conexión, y en la aplicación los indicadores a cada acción mencionada son los siguientes: sí se activa el botón rojo quiere decir puerta cerrada, si se activa el botón verde significa que la puerta

está abierta, y para el botón de color plomo indica que no hay conexión con la comunicación wifi, es decir es un sistema de control muy completo en cuanto a la funcionalidad. En las imágenes se puede apreciar de mejor manera.



En el caso donde exista problemas de comunicación wifi esta implementado un sistema de control alterno para el manejo del prototipo el cual primero consta de un registro de tarjetas NFC que son tecnologías de corto alcance, que a la vez permite la apertura y cierre de la puerta sin necesidad de comunicación wifi. Para el registro se tiene que acceder a la ventana de inicio la misma que al deslizar la pantalla de izquierda hacia la derecha aparecerá, ya que esta oculta en la parte izquierda del celular.

Tenemos que dar clic en el botón **iniciar** después mostrar las llaves electrónicas sobre la puerta luego dar clic en **verificar ID** y tiene que coincidir los dígitos que se muestra en el display luego hacer clic en registrar y la llave quedará registrada. Una vez terminado el proceso de registro hacer clic en **FINALIZAR** y listo.



Otra opción para realizar el control de apertura y cierre de la puerta es por medio de voz, un uso más versátil y funcional lo único que se tiene que hacer es dar clic sobre en icono del parlante y saltará una ventana de diálogo en donde tiene que decir abrir puerta o abrir para iniciar la apertura y para cerrar tiene que decir; cerrar o cerrar puerta y la acción se ejecutará inmediatamente.

Por ultimo podemos mirar los datos de registro de usuario, haciendo clic sobre Mi **Cuenta** cómo se puede ver en la siguiente figura.