ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

"IMPLEMENTACIÓN DE UN PROTOTIPO PARA EL CONTROL DE ACCESO REGISTRO Y AUTOMATIZACIÓN DE EVENTOS FÍSICOS MEDIANTE TECNOLOGÍA NFC PARA LA FIE-ESPOCH"

TRABAJO DE TITULACIÓN

TIPO: DISPOSITIVO TECNOLÓGICO

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR:

VÁSQUEZ SOLÍS CHRISTIAN EDUARDO

Riobamba-Ecuador

2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

"IMPLEMENTACIÓN DE UN PROTOTIPO PARA EL CONTROL DE ACCESO REGISTRO Y AUTOMATIZACIÓN DE EVENTOS FÍSICOS MEDIANTE TECNOLOGÍA NFC PARA LA FIE-ESPOCH"

TRABAJO DE TITULACIÓN

TIPO: DISPOSITIVO TECNOLÓGICO

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: VÁSQUEZ SOLÍS CHRISTIAN EDUARDO

TUTOR: ING. FRANKLIN GEOVANNI MORENO M. MSc.

Riobamba – Ecuador
2018

@2018, Christian Eduardo Vásquez Solís.

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA

EN TELECOMUNICACIONES Y REDES

El tribunal del trabajo de titulación certifica que: El trabajo de titulación: "IMPLEMENTACIÓN DE UN PROTOTIPO PARA EL CONTROL DE ACCESO, REGISTRO Y AUTOMATIZACIÓN DE EVENTOS FÍSICOS MEDIANTE TECNOLOGÍA NFC PARA LA FIE-ESPOCH", de responsabilidad del señor CHRISTIAN EDUARDO VÁSQUEZ SOLÍS, ha sido minuciosamente revisado por los miembros del tribunal del trabajo de titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
Ing. Julio Santillán Castillo Dr. **VICEDECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Patricio Romero **DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES**	_____	_____
Ing. Franklin Geovanni Moreno Montenegro. MSc **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
Ing. Geovanny Estuardo Vallejo Vallejo. Dr. **MIEMBRO DEL TRIBUNAL**	_____	_____

DEDICATORIA

Esta tesis se la dedico a Dios, Jesús y la Virgen María que siempre iluminan mi camino con sabiduría y conocimiento. Mi familia quien fue el pilar fundamental, principalmente a mis padres Eduardo y Gloria por siempre brindarme su apoyo y motivándome para nunca rendirme y siempre con trabajo y esfuerzo conseguir mis objetivos, por estar presentes en cada en cada uno de mis pasos a lo largo de toda mi vida al igual que mis hermanos Fernanda y Jairo por siempre ayudarme a ser una mejor persona en los ámbitos personales, académicos e intelectuales.

Mis amigos Javier, Jorge Luis, Diego, Jorge, Angie, Santiago, Gabriel, Denny, Daniela, Cristina y Darío con quienes hemos compartido grandes experiencias a lo largo de la carrera estudiantil gracias por contribuir a ser parte de una meta más y finalizar esta etapa estudiantil.

Christian…

AGRADECIMIENTO

Agradezco a Dios por permitirme culminar esta etapa universitaria junto con mi familia quienes fueron el soporte fundamental en mi formación académica, así también a mis amigos, familiares y personas desinteresadas que supieron apoyarme de sin esperar nada a cambio siendo un aporte y apoyo para la obtención de un objetivo más.

Gracias a la Escuela Superior Politécnica del Chimborazo, a la Carrera de Ingeniería Electrónica en Telecomunicaciones y Redes, que llego a transformarse en un hogar más que nos acogió y lleno de enseñanzas durante la vida politécnica.

Un agradecimiento especial al Ing. Franklin Moreno y al Dr. Geovanny Vallejo por su tiempo y enseñanzas, también agradecer a cada uno mis maestros quienes supieron trasmitir sus conocimientos, experiencias y motivaciones a lo largo de la carrera mediante sus trabajos y proyectos que fueron un aporte para la formación académica.

Christian

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

ÍNDICE DE ABREVIATURAS

(IoT):	Internet of Things
NFC:	Comunicación de Campo Cercano (Near Fiel Comunication)
ISM:	Industrial, Scientific and Medical
FCC:	Comisión Federal de Comunicaciones de los Estados Unidos
UHF:	Ultra High Frecuency
VHF:	Very High Frecuency
GFSK:	Gaussian Frequency Shift Keying (Modulación por desplazamiento de frecuencia gausiana)
FSK:	Frequency Shift Keying (Modulación por desplazamiento de frecuencia)
ECMA	Organización de estándares para la comunicación y la información.
NFC Forum	Asociación industrial sin fines de lucro encargada de regular la interacción
ECMA	European Computer Manufacturers Association
CSS	Cascading Style Sheets (Hojas de Estilo en Cascada).
PHP	Hypertext Preprocessor
WIFI	Wireless Fidelity (Fidelidad inalámbrica).
LF	Low Frecuency (Baja Frecuencia).
HF	High Frecuency (Alta Frecuencia).
EEPROM	Electrically Erasable Programmable Read-Only Memory (ROM Programable y borrable eléctricamente)

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de titulación tuvo por objetivo implementar un prototipo basado en dos dispositivos el primero para el control de acceso y registro mientras que el segundo dispositivo permite la automatización de eventos físicos como ON/OFF de equipos y sistemas autónomos dentro del recinto, los dos dispositivos basan su sistema de comunicación mediante tecnología NFC, existente en Smartphone de gama media y alta. Para la transmisión de información se ha programado una App móvil capaz de insertar comandos en Nfc Data Exchange Format, para el envio a través de ondas electromagnéticas cuando ocurra el acoplamiento de Tags activos NFC mediante la inducción del flujo de corriente en la etiqueta, dichos comandos son captados por Shield PN532 RFID/NFC de Adafruit bajo la comunicación SPI con los modos activo o pasivo dependiendo la operación a ejecutar, esta serie de instrucciones son interpretadas por la tarjeta de desarrollo ESP8266 NODE MCU funcionando en modo Client para el acceso a la red, con la configuración previa en la IDE de Arduino del SSID, Password e IP del servidor de la base de datos, estos datos serán enviados con tecnología WIFI al servidor Apache donde los SCRIPTS con codificación en php y html insertan en campos de la tabla TBACCESO que servirá como registro, después se compara las credenciales y horarios para crear el bloque de seguridad en el prototipo. De las pruebas realizadas se obtuvo tiempos de respuesta de 1 a 1.5sg. considerando una manera más rápida que la forma tradicional de acceso y registro para el uso de los laboratorios. El prototipo constituye una herramienta tecnológica rápida y segura. Se recomienda la implementación de los dispositivos en hogares, carros, etc para dar inicio de la IoT en Ecuador.

Palabras Claves: <TECNOLOGIA Y CIENCIAS DE LA INGENIERIA>, <TELECOMUNICACIONES>, NFC>, <ESP8266 NODE MCU (DISPOSITIVO)>, <CONTROL DE ACCESO>, <AUTOMATIZACIÓN DE EVENTOS>, <TECNOLOGÍA INALÁMBRICA (WIFI)>, <INTERNET DE LAS COSAS (IOT)>, <SHIELD PN532 RFID/NFC (DISPOSITIVO)>, <BASE DE DATOS>

SUMMARY

The following investigation's objective was to implement a prototype based on two devices, the first one for access control and registration while the second device allows the automation of physical events such as ON / OFF of equipment and autonomous systems within the enclosure, both devices base their communication system using NFC technology, existing in mid-range and high-end smartphones. For the transmission of information, a mobile App capable of inserting commands in the Nfc Data Exchange Format has been programmed for the sending through electromagnetic waves when the coupling of active NFC tags occurs through the induction of current flow in the label, The commands are captured by Shield PN532 RFID / NFC from Adafruit under SPI communication with active or passive modes depending on the operation to be executed, this series of instructions are interpreted by the development card ESP8266 NODE MCU operating in Client mode for access to the network, with the previous configuration in the Arduino IDE of the SSID, Password and IP of the database server, these data will be sent with WIFI technologies to the Apache server where the SCRIPTS with php and html coding insert in fields of the TBACCESO table that will serve as a record, then compare the credentials and schedules to create the security block in the prototype. From the tests carried out, response times of 1 to 1.5sg were obtained. Considering a faster way than the traditional way of access and registration for the use of laboratories. The prototype constitutes a fast and safe technological tool. It is recommended the implementation of devices in homes, cars, etc. So it will start the loT in Ecuador.

Keywords: <TECHNOLOGY AND SCIENCE OF ENGINEERING>, <TELECOMMUNICATIONS>, NFC>, <ESP8266 NODE MCU (DEVICE)>, <ACCESS CONTROL>, <AUTOMATION OF EVENTS,> <WIRELESS TECHNOLOGY (WIFI)>, <INTERNET DE THINGS (IOT)>, <SHIELD PN532 RFID / NFC (DEVICE)>, <DATABASE>

INTRODUCCIÓN

La innovación de la tecnología representa un movimiento en constante evolución de cambio profundo en la forma en que las personas interactúan con las máquinas, equipos, la información y entre sí, generando innovación, estandarización, seguridad, modelos comerciales, e invención de tecnología inalámbrica mediante dispositivos inteligentes, consideradas estas características como principales tendencias para las ciudades inteligentes que poco a poco son proyectadas por el Internet de las Cosas (IoT).

Con la investigación se pretende aportar en uno de los ejes para la transformación de la matriz productiva. "Transformar la matriz productiva para alcanzar el Buen Vivir", que dice "*Sustitución selectiva de importaciones con bienes y servicios que ya producimos actualmente y que seríamos capaces de sustituir en el corto plazo: industria farmacéutica, tecnología (software, hardware y servicios informáticos) y metalmecánica*". (Senplades, 2014, p. 12) sustenta así el presente trabajo de titulación.

IHS Technology (NYSE: IHS) realizo una publicación en Londres el 27 de febrero de 2014 que indica que los envíos globales de teléfonos celulares con tecnología NFC, aumentarán en un factor de más de cuatro desde 2013 hasta 2018, lo cual se ve expresado en la Figura 1-1 con un crecimiento hasta el 2018, alcanzando una penetración de NFC al 64 por ciento.(IHS Markit, 2016).

Diario "EL COMERCIO" publicó el 18 de febrero del 2017. Que el uso de teléfonos inteligentes creció en el año 2016 considerablemente en todos los segmentos de edad, siendo utilizados desde niños y adultos mayores, además, según el estudio del INEC sobre Tecnologías de la Información y Comunicación, menciona que 53 de cada 100 personas en el Ecuador posee un Smartphone.(Diario El Comercio, 2016).

Según la página web SHOPNFC nos presenta una amplia lista actualizada hasta el 6 de diciembre del 2017, una serie de teléfonos y tables compatibles con los diferentes chips de NFC en sus diferentes modelos y marcas, las cuales pertenecen a la gama media y gama alta. (Shopnfc, 2017).

Por lo expuesto anteriormente en las diferentes publicaciones se ha llegado a la conclusión que la mayoría de teléfonos utilizados por los ecuatorianos son Smartphone, los cuales pertenecen a la gama media o alta, y según lo establecido por SHOPNFC y IHS Markit estos dispositivos ya posee incorporado con un chip NFC, haciéndolos ideales para la utilización de las tecnologías de la banda ICM en High Frequency (NFC, BLUETOOTH, WIFI).

En el presente trabajo de titulación se realizará la implementación de un prototipo para el control de acceso, registro y automatización de eventos físicos mediante tecnología nfc para la FIE-ESPOCH, teniendo en cuenta las problemáticas que existen en la apertura y utilización de los laboratorios y aulas de la Fie, por lo cual se obliga a crear y diseñar un dispositivo para controlar el acceso, mejorando la seguridad en los recintos y optimizando el recurso humano y tecnológico.

Con el fin garantizar el acceso a los recintos a personal autorizado en su respectivo horario, y fomentar mayor seguridad para cada una de las aulas y en especial en los laboratorios que poseen una gran cantidad de equipos y dispositivos de gran valor, para lo cual nos enfocamos en la tecnología NFC que cumple las características de accesibilidad económica y transportación, disponibilidad y compatibilidad con diversas tarjetas de desarrollo y dispositivos.

Solucionando problemáticas que mayores molestias causa cuando las puertas de los laboratorios o aulas se encuentran cerradas o utilizadas por un sin número de usuarios los cuales requieren el uso de los mismos, sin importar horarios establecidos y sin responsabilidad por los enseres que se encuentran en el interior, por lo cual es necesario registrar al personal que ingresa al recinto. Viéndose en la extenuante labor de buscar al administrador o al encargado, para rápidas soluciones y cumplimiento de protocolos, implicando una pérdida de tiempo en la hora clase.

También se pretende optimizar recursos humanos (administrador y encargados) al no ser interrumpidos cuando estén realizando otras tareas o actividades dentro de la politécnica, y recursos tecnológicos que no han sido utilizados y tampoco implementados en la ESPOCH, Facultades, aulas y laboratorios.

Por lo tanto, la presente investigación tiene como objetivo el implementar un prototipo para el control de acceso, registro, y automatización de eventos físicos mediante tecnología NFC para la FIE-ESPOCH.

Como objetivos específicos se plantea para la investigación:

- Estudiar la tecnología inalámbrica NFC en el ámbito de control de acceso y automatización de eventos.
- Analizar las herramientas software que permitan el registro de los usuarios y comunicación con dispositivos electrónicos.
- Diseñar el App móvil que permitan el acceso y control los diversos eventos físicos.
- Elaborar el dispositivo que permita el control de acceso y automatización

CAPITULO I

1 MARCO TEÓRICO

En este capítulo se investigan las características necesarias de las diversas tecnologías inalámbricas, principalmente el funcionamiento de la tecnología NFC, dispositivos y herramientas que permitan la comunicación de esta tecnología, la cual es necesaria para la creación de un dispositivo electrónico, que permita el control de acceso, automatización y comunicación con otras tecnologías y equipos, acorde con los objetivos planteados.

1.1 Comunicación inalámbrica

Son tecnologías que no utilizan medios guiados ni canales físicos, cada tecnología es un sistema de comunicación mediante ondas electromagnéticas para la transmisión y recepción de datos entre los diversos equipos (Fernández Martínez *et al.*, 2009,p. 21). Para que exista la comunicación inalámbrica sus dispositivos deben estar interconectados dentro de un rango de cobertura.

Las tecnologías inalámbricas se clasifican según la zona de cobertura en cuatro categorías, WWAN redes inalámbricas de área ancha, WMAN redes inalámbricas de área metropolitana WLAN redes de área local y WPAN redes de área personal (Rivera *et al.*, 2016) , para el caso de estudio nos enfocaremos en las redes inalámbricas WLAN Y WPAN porque son las más empleadas en la actualidad.

1.1.1 Redes inalámbricas de área local (WLAN)

Es una red inalámbrica establecida geográficamente en un espacio pequeño, limitado para grupos de personas y dispositivos, utiliza ondas de radiofrecuencia para la comunicación (recepción y transmisión) sin medios guiados. Suelen ser redes de carácter privado, sencillas de configurar y brindan mayor movilidad a los usuarios dentro de la zona de cobertura. (Rivera *et al.*, 2016).

Lo que se quiere logar mediante esta tecnología es la eliminación de medios de transmisión guiados de cualquier tipo y reemplazarlos por tecnologías que utilizan ondas electromagnéticas que se encuentran dentro de la bamba ISM.(Network, 2014,p.31; Fuentes, 2016).

1.1.2 Redes Inalámbricas de Área Personal (WPAN)

Son catalogadas redes personales ya que su principal característica son sistemas de comunicaciones con un rango de cobertura es de 10 metros como máximo (Fuentes, 2016,p.1), permitiendo comunicaciones peer-to-peer debido a que no requiere de altos índices de transmisión de datos, los periféricos que intervienen en WPAN.

Ya vienen adecuados con protocolos simples y lo más óptimos que funcionan en dispositivos móviles como: PDAs, Smartphone, cámaras digitales, smartwatch, tablets y laptops (Mifsud Talón y Lerma-Blasco, 2013,p.226).

WPAN no necesita de una infraestructura previa o medios guiados hacia el exterior, de esta forma procura un uso eficiente de recursos. También puede considerarse como una capsula que se mueve por junto con la persona, dentro de esta estructura de red personal la IEEE ha creado grupos que divide en 4 estándares(Network, 2014,p.35).

- Bluetooth (IEEE 802.15.1).
- HomeRF
- Infrarrojos (irDA)
- Zigbee (IEEE 802.15.4)
- ETSI HiperPAN
- RFID
- NFC

1.2 Banda ISM (Industrial, Scientific and Medical)

En este conjunto de bandas de radio frecuencia electromagnética no licenciadas, se encuentran las tecnologías NFC, WIFI, BLUETOOTH, ZIGBEE, WIMAX y otras más, estas bandas de radiofrecuencia electromagnética son reservadas internacionalmente para el uso no comercial en áreas de trabajo industriales, científicas y médicas,

Estos fueron definidas por la Unión Internacional de Telecomunicaciones (ITU) Articulo 5 de regulaciones de radio (RR 5.138, 5.150 y 5.280).(Herrera M, 2012, p. 1). Según la división establecida por la ITU las bandas ISM se encuentran ubicadas en distintas regiones del espectro electromagnético:

- HF (High Frecuency)
- VHF (Very High Frecuency)

- UHF (Ultra High Frecuency)
- Región de microondas la cual va desde 1GHz hasta 300GHz.

Para el caso de estudio se ha escogido tecnologías inalámbricas que se encuentran dentro de WLAN y WPAN cumpliendo con los objetivos establecidos en el anteproyecto, tecnologías fáciles de encontrar y que están implementadas en dispositivos móviles de gama media.

1.3 NFC

Es una comunicaion de campo cercano debido a la corta distancia que los dispositivos interactuan, estableciendo un canal inalámbrico de comunicacion entre 2 dispositivos. Su funcion principal es mantener una transmision, recepcion y viceversa de manera instantanea, donde las etiquetas y lectores deben estar a una distancia de cobertura menor a 5 cm, caracteristica principal por lo que se considera una comunicación segura y de una baja tasa de trasferencia. (© RF Wireless World, 2012), (Peña, 2012, p.60).

NFC que opera en la frecuencia de 13.567 Mhz en la banda de Alta frecuencia (High Frecuency) que se encuentra en la región 1 de radio frecuencia designadas para aplicaciones industriales, científicas y médicas (ICM), como se puede observar en la Tabla 1-1 que se encuentra resaltada.

Tabla 1-1: Rango de frecuencias de región 1 de las bandas ICM

Bandas		**Frecuencia Central**	**Ancho de banda**
Región 1			
13.553 Mhz	13.567 Mhz	13.560 Mhz	14 khz
26.957 Mhz	27.283 Mhz	27.129 Khz	326 Khz
40.66 Mhz	40.70 Mhz	40.68 Khz	40 Khz

Realizado por: VÁSQUEZ, Christian 2018

Las siglas NFC hace referencia a Near Field Comunication, “Comunicación de Campo Cercano” termino en español, aparece como la evolución de la tecnología estándar RFID y como un progreso en la convergencia de aplicaciones dentro de dispositivos móviles, permitiendo una comunicación segura a través de los servicios de las tarjetas inteligentes. (Chavarría Antonio, 2011, p. 20). En la Figura 1-1 se aprecia el logotipo de la tecnología inalámbrica NFC.

Figura 1-1: Logo tipo de NFC
Fuente: NFC Forum

1.3.1 Protocolos y Normativas

NFC se estandarizado bajo las normas ISO / IEC 18092 siendo compatible con tarjetas inteligentes contactless FeliCa de Sony, ISO / IEC 14443 (proximity cards), y ISO / IEC 15693 (vicinity cards). Estos protocolos tratan sobre la minimización de interferencias en los modos de comunicación, dando especificaciones de los parámetros de control de colisión, el protocolo de transporte, las velocidades de transferencia, sistemas de modulación, codificaciones y el formato de trama.

Para que pueda existir una comunicación entre dispositivos NFC es necesario un dispositivo **iniciador** y un destino que puede ser pasivo o activo llamado **objeto**. (Igoe, Coleman y Jepson, 2014).

1.3.2 Iniciador

Es el elemento activo que obtiene energía de una fuente de alimentación interna, capaz de generar ondas electromagnéticas para el inicio de comunicación, el mismo que permanecerá como elemento iniciador hasta que concluya la comunicación. (INTECO, 2013, p. 4).

1.3.3 Objeto

Es el elemento pasivo que emite una señal de respuesta junto con la información que tiene almacenada, cuando percibe energía del inicializador.

1.3.4 Protocolo de Señalización

El protocolo de señalización es el modo de comunicación que utiliza para él envió de datos entre el iniciador con el objetivo en cada una de las tarjetas, lectores y diversos dispositivos NFC.

Todo depende de su funcionalidad para el que fueron desarrollados los diferentes tipos de etiquetas NFC (Falke, Rukzio y Dietz, 2007,p.3), por lo cual el protocolo de señalización permitirá el intercambio de información entre 2 dispositivos, se considera 4 tipos existente:

- Tipo I ISO/IEC 14443A (NFC-A) Tipo II
- ISO/IEC 14443B (NFC-B)
- Tipo III FeliCa JIS X6319-4 (NFC-F)
- Tipo IV (NFC-A) y (NFC-B)

1.3.4.1 Tipo I ISO/IEC 14443A (NFC-A)

Este estándar se basa en lectura y reescritura, pero puede ser configurada solo para lectura, la comunicación en el tipo A emplea la codificación Miller (codificación de retardo) los datos binarios se transmiten a 106Kbps. (RF Wireless World, 2012).

1.3.4.2 Tipo II ISO/IEC 14443B (NFC-B)

Utiliza la codificación Manchester es relativamente similar al tipo A,lectura y escritura y puede ser configurada solo como lectura (RF Wireless World, 2012) la diferencia es en memoria:

- Tipo A 96 Bytes expandible a 2
- Tipo B 48 Bytes expandible a 2

1.3.4.3 Tipo III FeliCa JIS X6319-4 (NFC-F)

La señalización NFC-F está basado en los estándares japonés conocido como Felica JIS (Japanese Industrial Estándar), caracterizada por ser una comunicación más robusta.

Siendo muy utilizada para pagos mediante tarjetas inteligentes que incluye comando de mensajes extras y formatos. Dichas especificaciones para el formato NFC están definidas por la comunicación half dúplex, la interfaz digital.(Sony Imaging Products & Solutions Inc., 2018, p 3).

1.3.4.4 Tipo IV (NFC-A) y (NFC-B)

Los estándares son compatibles entre el tipo A y tipo B, permitiendo la lectura y escritura, así como la configuración de solo lectura, los cambios más notables son en velocidad (424Kbps) y capacidad de almacenamiento (32KB).

Al ser una tecnología basada en RFID, existe una compatibilidad entre **Tag NFC** y **Etiquetas RFID** debido a los estándares que incorpora NFC, eliminando la necesidad de crear una infraestructura NFC separada. (Vásquez Santiago, 2016, p 25).

1.3.5 Tipos de acoplamiento

El funcionamiento de NFC depende de la forma como adquiere la energía el elemento activo que por lo general es de una fuente de alimentación interna (Medina, 2017, p 12). La excitación de electrones inicia en una pequeña bobina que realiza las funciones de antena, esta se une a un chip pequeño, como se puede apreciar en la Figura 2-1, al energizarse la bobina el chip también se alimenta de esta manera inicia la comunicación NFC (Igoe, Coleman and Jepson, 2014).

Figura 2-1: Unión de la antena con el chip
Fuente:(Wahid et al., 2017,p 356).

Los mecanismos para la recepción de energía en las etiquetas se pueden realizar de 2 formas:

1.3.5.1 Acoplamiento inductivo

Es una técnica que produce un acoplamiento magnético donde interviene el iniciador (interrogador) y el objeto (transpondedor), en la figura 3-1 podemos apreciar como el campo magnético se genera en la antena del lector, he induce un flujo de corriente en la etiqueta específicamente en la antena del objeto. (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008, p. 175).

Dicha etiqueta está constituida por un elemento inductivo (bobina) y otro capacitivo (condensador), la intensidad de corriente en el elemento inductivo carga al elemento capacitivo, el mismo que genera voltaje para él envió de energía y datos. (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008, p. 175).

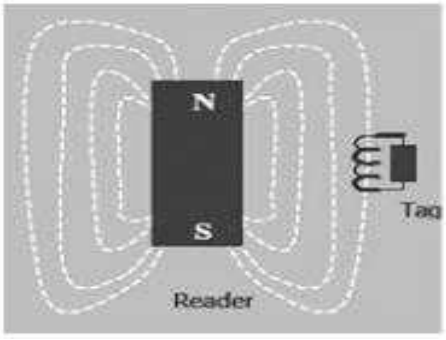


Figura 3-1: Acoplamiento Inductivo
Fuente: (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008. p. 176).

1.3.5.2 Propagación por ondas electromagnéticas

Este método se basa en la zona de far field (campo lejano) donde el lector genera y envía señales de radio, más conocidas como ondas electromagnéticas hacia el receptor que es encargado de recibir en un punto específico la energía de ondas electromagnéticas planas para el acoplamiento.

Como se puede ver en la figura 4-1, donde la energía recibida depende de la distancia a la que se encuentre el receptor. (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008, p.176).

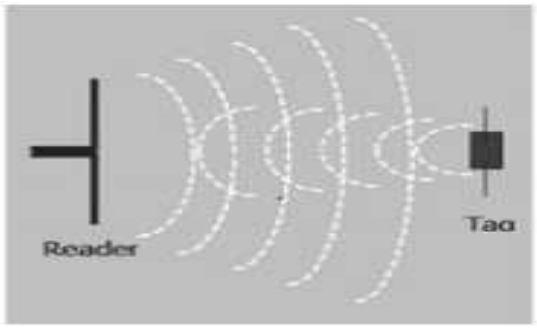


Figura 4-1: Propagación por ondas electromagnéticas
Fuente:(Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008, p. 176).

Se considera que los dispositivos NFC utilizan el acoplamiento inductivo para la comunicación e intercambio de información y energía, mientras que RFID utiliza la propagación por ondas electromagnéticas.

NFC es una tecnología que trabaja en distancias cortas y la propagación por ondas electromagnéticas es un método basa en la zona de far field. Algunos dispositivos NFC pueden llegar a funcionar con los 2 métodos por los estándares que comparten (Igoe, Coleman y Jepson, 2014).

1.3.6 Funcionamiento

El funcionamiento de NFC se basa mediante 5 etapas (Campa Ruiz, 2011), que son:

- **Descubrimiento**: Búsqueda y reconocimiento de dispositivos.
- **Autenticación**: Verificación de autorización o algún cifrado para su comunicación.
- **Negociación**: Establecimiento de parámetros como la velocidad de transmisión, tamaño, acciones solicitadas, identificación del tipo de dispositivo y aplicación.
- **Transferencia**: Comprobada la negociación puede comenzar la transferencia de datos.
- **Confirmación**: El elemento destino confirma el intercambio de energía o comunicación.

NFC fue es diseñado para una comunicaron bidireccional a partir de lo establecido en la tecnología RFID que realiza la comunicación por una sola vía, otorgando un intercambio seguro de información y su funcionamiento puede ser como una etiqueta básica o como un lector, esta característica es conocida como comunicación "punto a punto" entre los dispositivos. NFC.(MCI Capacitacion-MCI ELECTRONIC, 2015).

1.3.7 Componentes

NFC está constituido por una pequeña bobina que también hace la función de antena, un pequeño chip de almacenamiento, y en algunos casos incluye una fuente de alimentación interna en dispositivos activos (Igoe, Coleman and Jepson, 2014).

En la Figura 5-1 se aprecia la unión de la bobina (antena) y chip que son incorporados dentro de muchos elementos como: llaveros, teléfonos, tarjetas (bancarias, de control de acceso), stickers y pegatinas de diversas formas (Ortiz, 2006, p. 18).

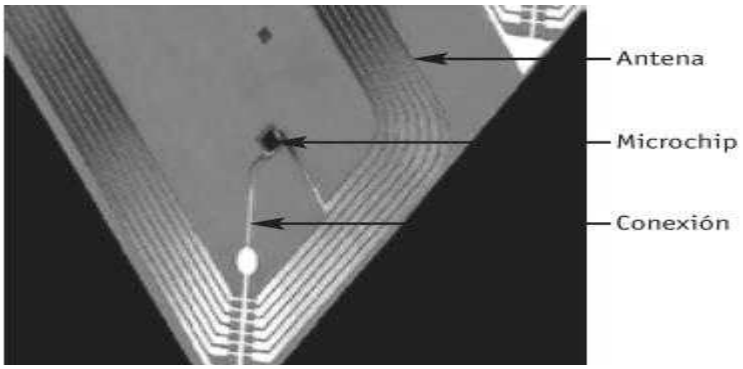


Figura 5-1: Etiqueta simple de NFC
Fuente: (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008 ,p 37)

Para que se establezca la comunicación de un sistema NFC se utiliza componentes similares a la tecnología RFID, el sistema de comunicación debe de componerse principalmente de cuatro elementos:

- Etiquetas(Tags)
- Lectores
- Antenas
- Sustrato

1.3.7.1 Etiquetas (tags)

Está constituido por un microchip de silicio unido a una antena, un transmisor o un receptor de ondas de radio, un modulador para enviar señales de respuesta lógica de control, memoria interna, y algunas de ellas un sistema de energía (esto es lo que distingue de una etiqueta activa de una pasiva).

Una etiqueta NFC con una fuente de alimentación interna se considera una etiqueta activa, mientras que un dispositivo sin fuente de alimentación interna, se considera una etiqueta pasiva. Dichas etiquetas funcionan de forma similar al de un transponder, cuando captan señales como receptor. ((INTECO), 2013,p 5).

Tipos de etiquetas

Las etiquetas NFC son construidas según estándares establecidos desde el 2002, tanto la tecnología como los componentes sigue siendo desarrolladas por distintas empresas, las mismas que ponen a disposición un sin número de modelos, marcas, distinta capacidad de almacenamiento, velocidades de transmisión más altas.

La Tabla 2-1 podemos ver de forma generalizada la construcción de etiquetas con distintos estándares, modos de comunicación, memoria y velocidades.

Tabla 2-1: TIPOS DE ETIQUETAS NFC

TIPO	ESTANDAR	MODOS	MEMORIA	VELOCIDAD
Tipo 1	ISO 14443 A	Solo lectura Lectura y escritura	96 bytes	106 kbit/s
Tipo 2	ISO 14443 A	Solo lectura Lectura y escritura	48 bytes	106 kbit/s
Tipo 3	SONY FeliCa	Solo lectura Lectura y escritura	2 kbytes	212 kbit/s
Tipo 4	ISO 14443 Tipo A y B	Solo lectura Lectura y escritura	32 kbytes	106 kbit/s 424 kbit/s

Fuente: ((INTECO), 2013,p 5)

1.3.7.2 Lectores

Lector o más conocido como el **dispositivo iniciador** se encarga de generar una onda electromagnética para alimentar el circuito pasivo, el cual permite un acoplamiento inductivo o comunicación entre los dispositivos y la señal de respuesta que es devuelta al lector junto con la información almacenada en memoria.(Bueno Delgado, Pavón Mariño y De Gea Garcia, 2011, p 15).

1.3.7.3 Antenas

Las antenas de los dispositivos nfc permitiendo la generación y recepción de ondas de campos magnéticos del inicializador hacia el elemento pasivo, dependen del tipo de antena que se utilice para determinar el rango de cobertura del campo electromagnético, las antenas de forma cuadrada, cilíndrica, circular y espiral son los más comunes. (Bueno Delgado, Pavón Mariño y De Gea Garcia, 2011,p 15).

1.3.7.4 Sustrato

Brinda protección a la antena y al chip (circuito integrado), también constituye el soporte para el ensamblaje como se aprecia en la Figura 6-1 cada una de las partes de la etiqueta básica nfc o rfid.

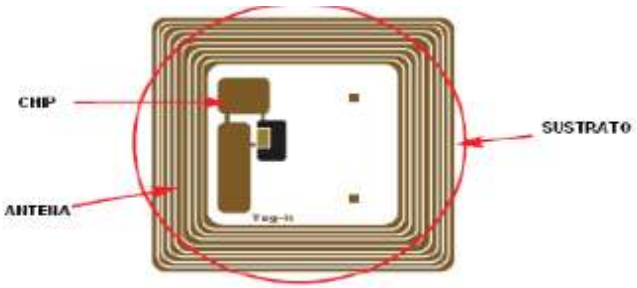


Figura 6-1: Componentes de la etiqueta
Fuente:(Jurado y Salazar, 2013,p. 8)

1.3.8 Modos de comunicación

La comunicación NFC utiliza el acoplamiento inductivo esto ocurre cuando dos dispositivos nfc entran en contacto y el objeto pasivo absorba energía del elemento activo. Esta característica de transmisión y recepción de forma simultanea hace única a NFC de las tecnologías inalámbricas (Portillo García, Bermejo Nieto y Bernardos Barbolla, 2008,p 50), estos 2 modos se detallan a continuación:

1.3.8.1 Modo Activo

Cuando se trata de comunicaciones entre dos dispositivos activos, es decir con fuentes generadoras de campos de radio frecuencia, tanto el NFC Inicializador como el NFC Tag generan sus propios campos electromagnéticos, este inicia cuando el NFC Inicializador genera energía y la trasmite hacia el NFC Tag.

El cual al recibir la señal electromagnética empieza a energizar el Tag con su fuente de alimentación interna propia, para el envio de la información almacenada bajo los parámetros establecidos por el elemento iniciador (Lector) (Medina, 2017,p 13).

Todo este proceso es identificado en la Figura 7-1, en la primera parte identificado como 1 se visualiza como el lector genera las ondas electromagnéticas, es decir el proceso iniciador explicado anteriormente.

En la segunda parte identificado con el número 2 se aprecia la respuesta producida por el NFC Tag, en el grafico se identifican claramente de color azul, el intercambio y procesamientos de datos digitales.

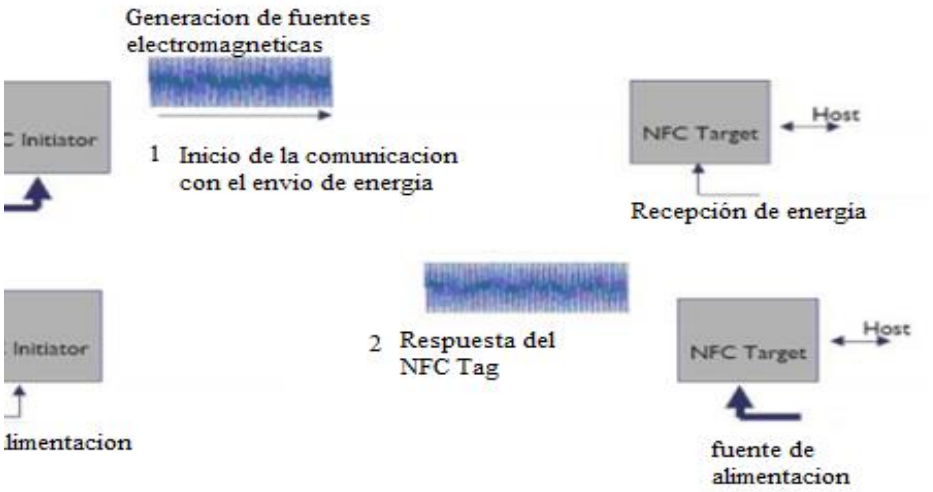


Figura 7-1:Comunicación entre dispositivos activos
Fuente:(Medina, 2017,p 13) **Modificado:** VASQUEZ, Christian 2018

1.3.8.2 Modo Pasivo

En la Figura 8-1 se observa el modo de comunicación, iniciando en el elemento Lector con la generación de campos magnéticos y el dispositivo pasivo recibe la señal electromagnética y utiliza la modulación de la carga para responder con la información almacenada bajo los parámetros enviados por el Lector (Campa Ruiz, 2011,p 13).

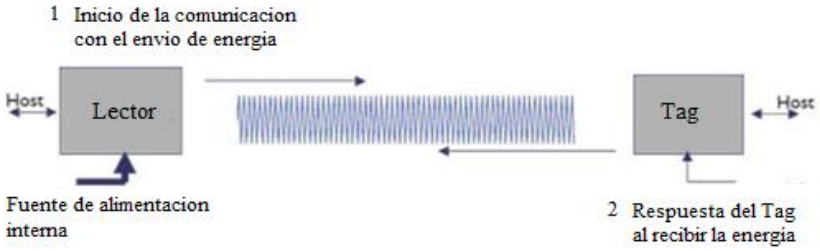


Figura 8-1: Comunicación de dispositivos pasivos
Fuente:(Medina, 2017,p 12)

A continuación, detallamos cada uno de los pasos que se desarrollan para el modo de comunicaron pasiva.

1. Primero se genera una energía el elemento activo con su fuente de alimentación interna, esta energía es enviada a la bobina y antena la cual produce un campo de ondas electromagnéticas como se ve en la Figura 9-1, estas son enviadas de forma omnidireccional similar a un dipolo ideal.

Figura 9-1: Generación y envió de campos electromagnéticos
Fuente: (http://learn.teslabem.com/pn532-adafruit-nfc-rfid-shield-para-arduino-contrasena-pc/)

2. Aprovecha la energía generada por el elemento activo como se aprecia en la Figura 10-1 donde, el elemento pasivo absorbe energía del dispositivo activo a través de un campo magnético.

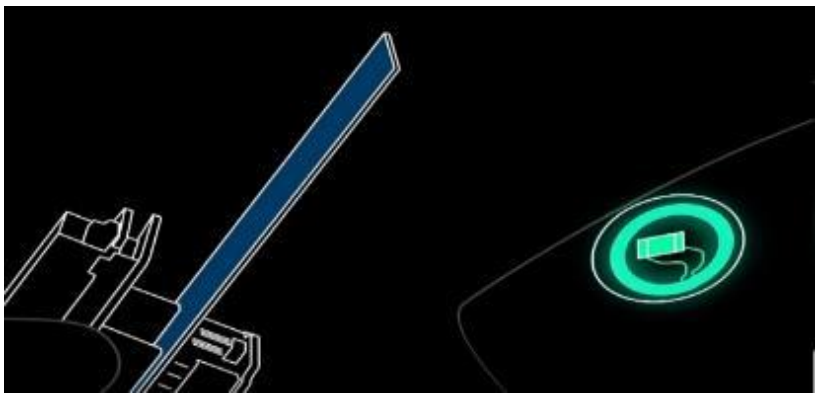


Figura 10-1: Recepción de la señal electromagnética en el elemento pasivo
Fuente: (http://learn.teslabem.com/pn532-adafruit-nfc-rfid-shield-para-arduino-contrasena-pc/)

3. Esta recepción de energía se produce hasta que se active el elemento pasivo y sea capaz de activar el chip de almacenamiento para él envió de información, esto se aprecia en la Figura 11-1.

Figura 11-1: Energización del elemento pasivo
Fuente: (http://learn.teslabem.com/pn532-adafruit-nfc-rfid-shield-para-arduino-contrasena-pc/).

4. Una vez energizado el elemento pasivo, este genera su respuesta aprovechando la modulación de la carga, estableciendo el envio e intercambio de energía he información,

este proceso se puede ver en el gráfico de la Figura 12-1. (Bueno Delgado, Pavón Mariño y De Gea Garcia, 2011 p. 15).

Figura 12-1: Envió de respuesta del dispositivo pasivo
Fuente: (http://learn.teslabem.com/pn532-adafruit-nfc-rfid-shield-para-arduino-contrasena-pc/)

1.3.9 Modos de Operación

Los dispositivos con NFC admiten tres modos de operación (Cavoukian, 2011, p 11), que se detallan a continuación:

- Lectura/escritura de etiquetas
- Emulación de tarjetas
- P2P

1.3.9.1 Lectura/escritura

En las especificaciones de los estándares ISO 14443 y FeliCa nos indica que el dispositivo activo NFC, puede leer un chip o etiqueta pasiva es decir sin alimentación. Este puede ser la lectura de un llavero o un adhesivo (ROHDE&SCHWARZ, 2018). en donde los chips de destino comienzan a funcionar cuando son estimulados por los readers (lectores) (RFID Journal, 2007).

1.3.9.2 Peer to Peer

Esta comunicación inicia cuando el emisor no genera energía, y solo refleja y modula la energía transmitida por el elemento receptor para transmitir información. (NFC.INTECO, 2013).

Este modo establece una comunicación bidireccional entre 2 dispositivos autoalimentados, permitiendo el intercambio de información de cualquier tipo de datos como imágenes, parámetros de configuración de enlaces WLAN/Wi-Fi. (Peña, 2012, p. 61) y *WLAN/Wi-Fi.* (ROHDE&SCHWARZ, 2018)

1.3.9.3 Emulación de tarjeta

Los dispositivos activos pueden actuar como destinos pasivos de forma inteligente cuando sea requerido para la transmisión de información no siempre los dispositivos activos son compatibles o aceptan la operación a ejecutarse. (Cavoukian, 2011,p 8).

Un ejemplo claro son los teléfonos inteligentes que son 2 elementos activos que recogen la información alojados en el destino pasivo, para realizar determinadas acciones en función de su contenido.(INTECO, 2013).

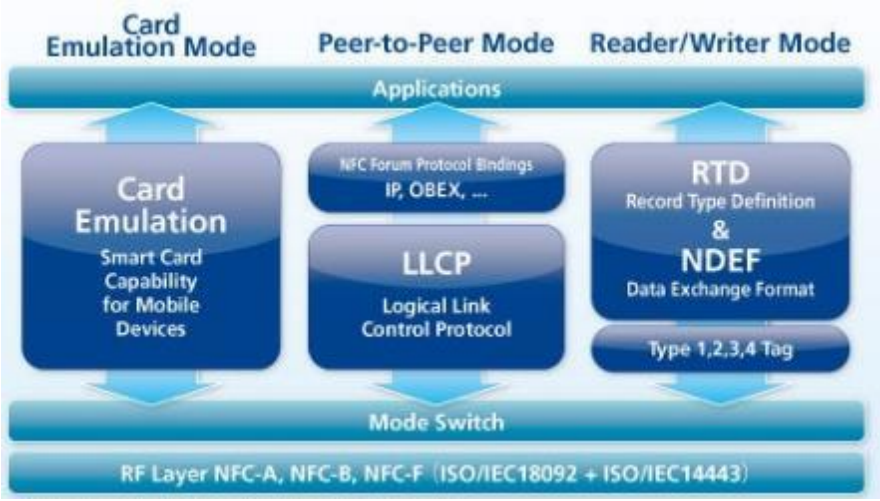


Figura 13-1: Modos de operación
Fuente: (Sony Imaging Products & Solutions Inc., 2018,p. 2)

En la figura 13-1 se puede ver de forma detallada las capas implementadas en cada uno de los modos de operación, mediante la utilización de protocolos de tecnologías inalámbricas para brindar seguridad para la transmisión, cabe aclarar que sigue desarrollándose diversos protocolos de seguridad en NFC.

1.3.10 Seguridad en la tecnología NFC

Como todo sistema se comunicación siempre es propenso a vulnerabilidades y la tecnóloga NFC no es la excepción debido a que es una comunicación por radiofrecuencia, existen diversos tipos de ataques estos pueden tan simples como también muy elaborados (Portillo García, Bermejo Nieto and Bernardos Barbolla, 2008), como:

- Evitar la comunicación entre el lector y la etiqueta (Jaula de Faraday)
- Spoofing,
- Inserción,
- Replay
- Denegación de servicio.

Estas amenazas son más propensas y han cumplido su cometido en la tecnología RFID, esta es la principal razón para la creación de NFC, solucionando en esta tecnología algunas vulnerabilidades y brindando mayor seguridad por trabajar en un rango menor a 20 cm, pero sigue latente la lectura de etiquetas pasivas con cualquier lector y suplantación de códigos para el uso fraudulento.

También cabe la posibilidad que cualquier individuo que posea un software o aplicación pueda acceder al contenido de la etiqueta, modificarla, eliminar, corregir o aumentar información, así como la inserción de errores (Chavarría Antonio, 2011,p 26).

Esto amenaza es solucionada con la utilización de dispositivos activos mediante el modo de operación peer to peer (p2p), permitiendo mayor seguridad para la transferencia de datos, y dando la opción que el usuario elija a que dispositivos desea conectarse.

Las investigaciones para la seguridad en la tecnología NFC se basa en un circuito electrónico integrado de esta forma se garantiza la confidencialidad del almacenamiento de datos en memoria mediante una clave privada que encriptada la información transmitida (Falke, Rukzio y Dietz, 2007, pág. 5).

1.3.11 NDEF (NFC DATA EXCHANGE FORMAT)

Es un formato de mensaje binario muy liviano creado por NFC Forum, para encapsular cargas utilices dentro de un solo mensaje, permitiendo el intercambio de datos entre dispositivos NFC (equipos y etiquetas). (Sabella, 2016, p 1).

En la figura 14-1 podemos observar la estructura de un mensaje NDEF, cada mensaje está formado por registros llamados RECORD, cada record está constituido por una cabecera (HEADER) y una carga útil (PAYLOAD). Las cabeceras (HEADER) contienen información útil como la longitud de información, tipo e identificación.(NFC Forum, 2006, p 7)

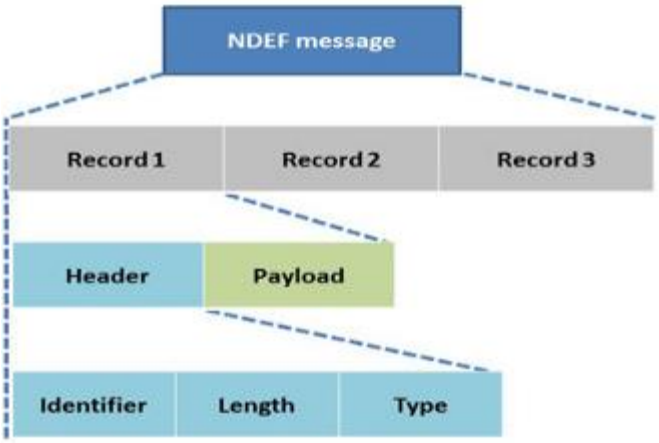


Figura 14-1: Estructura de un mensaje NDEF
Fuente: (Sabella, 2016, http://www.dummies.com/consumer-electronics/nfc-data-exchange-format-ndef/)

1.4 WIFI

Es una tecnología de comunicaciones de datos inalámbrica con especificaciones del estándar 802.11115, que utiliza el aire como medio de transmisión, permitiendo la interoperabilidad entre diversos equipos y dispositivos sin la necesidad de hilos o medios guiados, los estándares de redes que utilizada wifi son 802.11(b, a, g, n)(Jiménez, 1994,pp 15).

- 802.11a permite hasta 54 Mbps en las bandas no licenciada a 5 GHz.
- 802.11b permite hasta 11 Mbps en la banda no licenciada a 2.4 GHz.
- 802.11g permite hasta 54 Mbps en la banda no licenciada a 2.4 GHz.
- 802.11n permite hasta 600 Mbps en las bandas no licenciadas a 2.4 GHz y 5 GHz.

Las siglas WIFI significan Wireless Fidelity y su logotipo se puede apreciar en la Figura 15-1, el estándar que wifi opera en una frecuencia libre de 2.4 Ghz y 5 Ghz, utilizando como método de acceso al medio a CSMA/CD (Rivera *et al.*, 2016).

La IEEE creó la CSMA/CD bajo la evolución de estándares anteriores que daban problemas, en la actualidad los proveedores de estos equipos garantizan la compatibilidad entre dispositivos de diversas marcas (MCGRAW-HILL INTERAMERICANA DE ESPAÑA, 2018, p 17).

Como se enfatiza en la Figura 15-1 la red LAN es similar a la red WLAN brindando compatibilidad entre equipos, convergencia de la red, acceso a internet en cualquier punto dentro del área de cobertura, escalabilidad de la red, facilidad de instalación y soporta usuarios móviles. (Abadía, 2010,p 5).

Figura 15-1: Red de área local WIFI
Fuente:(Rivera et al., 2016, https://html1-f.scribdassets.com/63cka3kdj45w4w3q/images/8-659ba1ec05.jpg)

1.5 Domótica

Es el conjunto de sistemas informáticos y de nuevas tecnologías aplicadas al hogar capaces de automatizar una serie de tareas habituales como calefacción, encendido y apagado de iluminación, monitoreo, aperturas de cerraduras y comunicación con dispositivos, utilizando métodos de "electrónica, robótica, informática y telecomunicaciones" (Huidobro *et al.*, 2007,p 16), (Hernández Balibrea, 2012).

Los procesos tecnológicos sufridos por estos últimos años han creado he implementado un sin número de dispositivos que se puedan conectar al internet, los cuales pueden tratar la información ("trasmitirla, recibirla, procesarla y almacenarla" (Huidobro *et al.*, 2007,p 18)), implementando métodos y dispositivos para tener una mejor calidad de vida haciendo de la vivienda confortable cómoda y segura (Números and EIAD, 2014),

Los objetivos de las funciones domóticas es generar confort, seguridad, ahorro energético y control sobre los dispositivos conectados a la red (Martín, Fernando y Vacas, 2006,p 21), lo mencionado anteriormente se puede apreciar de mejor manera en la Figura 16-1.

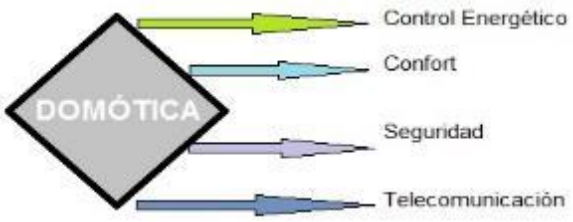


Figura 16-1: Funciones básicas de la domótica
Fuente: http://www.monografias.com/trabajos105/protocolo-domotica-firewire-ieee-1394-y-zigbee/image003.jpg

Dentro de este alcance tecnológico de la domótica los autores Numeros y EIAD mencionan una segmentación que es planteada de la siguiente manera (Números y EIAD, 2014,p 1):

- **Domótica**: es un término para referirse a sectores domésticos
- **Inmotica**: término utilizado para ambientes más grandes como sectores empresariales
- **Urbotica**: tecnología aplicada en ciudades

1.5.1 Componentes del sistema domótica

Las automatizaciones de hogares están enfocadas en el bienestar y confort de usuarios permitiendo gestionara y controlar cada uno de los sistemas implementados en el domicilio, para logar la comunicación entre el usuario y la acción deseada en el dispositivo final, los elementos que pueden intervenir o estar integrados (Hernández Balibrea, 2012,p 9) son:

- **Controlador:** Es un dispositivo encargado de la gestión, control y análisis del sistema donde existen uno o varios controladores (Hernández Balibrea, 2012,p 9)**.**

- **Actuador:** Son elementos que ejecutan instrucciones de un controlador que se deben a un sistema automatizado de control, realizando una acción que cambio, de un estado anterior a un estado actual generalmente instrucciones (ON / OFF) en un dispositivo o cambio de parámetros de un sistema retroalimentado por ejemplo (contactores /relés y electroválvulas), (Domínguez y Sáez, 2006,pp 52-53)**.**

- **Sensor:** Son pequeños dispositivos que tienen como función captar y recibir información acerca de magnitudes físicas y químicas de un sinnúmero de variables del medio que los rodea, de ambientes interiores como ambientes exteriores, estas variables pueden ser potencia, volumen, presión, peso velocidad, co2 etc. Dicha información recogida es enviada a un sistema para su interpretación. (Fernández, 2012,p 8).

- **Bus:** El bus o también llamado soporte al medio físico que está encargado ser el canal entre el sistema y dispositivos finales, encargado de las funciones de intercambio de señales (sentencias de control) y de la alimentación (Domínguez y Sáez, 2006, p 65) Otros autores también la consideran como puerta de enlace usada para el envió de datos y monitoreo de la red (Fernández Martínez *et al.*, 2009).

- **Interface:** Es el medio por el cual podemos visualizar datos o información que el sistema nos arroja por medio del cual podemos tener conocimiento del funcionamiento y la

estabilidad del sistema (Cobos y Ortiz, 2017,p 5), estos dispositivos pueden ser "pantallas, móvil, Internet y conectores" (Hernández Balibrea, 2012,p 9).

1.6 Sistemas de Control de Acceso

Los sistemas de control de acceso son dispositivos que poseen diversos métodos para la identificación de personal autorizado, capaces de comprobar la identidad de cada uno de los usuarios, teniendo como objetivo principal la restricción del acceso al público en general a las diferentes áreas protegidas (Mojica y Gamba, 2010,p 5; Cosentino, 2013,p 152).

Es necesario conocer el nivel de seguridad que debe ser aplicar (Mojica y Gamba, 2010, p 5), esto depende de los elementos que se desean proteger, pueden ser zonas donde se maneje dinero, propiedad intelectual, zonas de producción, etc.

Estos antecedentes determinan que método de control de acceso puede ser el mejor para emplearse (Cosentino, 2013, p 153), considerando variables como tiempo de ingreso, aislamiento, efectividad del sistema, método de cuarentena, incomodidad causada, tráfico y costo.

Los sistemas de control de acceso más utilizados en la actualidad son:

- Lectores de proximidad
- Lector de tarjetas inteligentes
- Lectores Biométricos (identificación por características Huella /Facial)
- Lector de pin
- Lector Código de barras

1.6.1 Lectores de proximidad

Dentro de los lectores de proximidad tenemos una compatibilidad entre dos las tecnologías NFC y RFID la diferencia entre estas tecnologías, es la distancia a la que se funcionan, por lo que se considera que al utilizar tecnología RFID es una forma insegura para el control de acceso y no será considerado dentro de estos sistemas de acceso (Mundo NFC, 2012).

- **Tarjetas NFC Pasivos**

Son elementos que permiten almacenar información o datos dentro de un chip en el interior, estas tarjetas no brindan garantías necesarias en el ámbito de la seguridad ya que son fácilmente modificables, un claro ejemplo de estos elementos se muestra en la Figura 17-1.

Figura 17-1: Tarjetas pasivas
Fuente: http://www.arci.com.mx/wp-content/uploads/2013/06/lectores-de-proximidad.jpg

- **Dispositivos NFC activos**

Son considerados dispositivos mucho más seguros ya que el código o instrucción para la apertura de la puerta viaja mediante el canal de ondas electromagnéticas de los 2 dispositivos y no son almacenado en alguna memoria como se indica en la Figura 18-1.

Figura 18-18: Dispositivos activos
Fuente: https://www.digitalsecuritymagazine.com/wp-||| content/uploads/2016/11/IDTronica-Sistemas-uAcces.jpg

1.6.2 Lector de tarjetas inteligentes

Son tarjetas que tienen implantado en su interior un microprocesador que realiza diferentes cálculos, almacena información y permite la manipulación de programas encriptados como ejemplo tenemos en la Figura 19-1 , todo esto esta normalizado por el estándar ISO 7816 donde estipulan parámetros en el almacenamiento EEPROM o Flash (Romo, 2015, p. 4; Cobos y Ortiz, 2017, p 10).

Figura 19-1: Tarjeta Inteligentes
Fuente: https://www.ecured.cu/images/c/ce/Tarjeta_inteligente.gif

1.6.3 Lectores Biométricos

Los dispositivos biométricos están compuestos por un conjunto de sensores que se encargan de captar los rasgos morfológicos únicas que cada ser humano tiene y nos diferencia. Entre las características más destacadas de las personas tenemos cara, manos y ojos, estas características infieren en los equipos biométricos que identifican formas y miden geometrías (Tolosa Borja y Álvaro, 2010, p 1).

Existen varios tipos de reconocimiento que se enfocan en el ser humano estos son:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

1.6.4 Lector de Códigos de barras

Los códigos de barras utilizan un código binario mediante espacios y barras negras estas pueden tener diversas formas, el funcionamiento del código de barras se basada mediante la luz que es reflejada en las barras y espacios, dichas barras tienen formas alfanuméricas o numéricas las cuales son leídas por un lector laser que es un escáner óptico (Almonacid, 2007, p. 2; Cobos y Ortiz, 2017,p 8).

1.6.5 Tabla comparativa de sistemas de acceso

Según los parámetros expuestos en la Tabla 3-1 se analizó que el sistema con mayor seguridad y costo son los biométricos, pero el sistema de acceso con lectores de proximidad NFC activos son igualmente seguros y de bajo precio.

Tabla 3-1: Comparativa entre los sistemas de acceso

SISTEMA DE CONTROL DE ACCESO CARACTERISTICAS	CÓDIGO DE BARRAS	TARJETAS INTELIGENTES	SISTEMAS BIOMÉTRICOS	NFC ACTIVO	NFC PASIVO
Modificación de la información	No Modificable	Modificable	No Modificable	No Modificable	Modificable
Seguridad de los Datos	Mínima	Mínima	Alta	Alta	Baja
Capacidad de Almacenamiento de Datos	Lineales(8-30 caracteres) 2D hasta 7200 caracteres	Hasta 8MB	No aplica	Hasta 224KB	Hasta 8MB
Precio	Bajo	Medio-Bajo	Alto	Medio- Alto	Medio-Bajo
Estándares	Estables	Estables	No estándar	Propietario y en evolución hacia el estándar	Propietario y en evolución hacia el estándar
Ciclo de Vida	Corto	Largo	Indefinido	Depende de la batería (3 a 5 años)	Indefinido
Distancia de Lectura	Línea de vista (hasta 1.5m)	1 hasta 10 metros	Depende del biométrico	Requiere contacto	Requiere contacto
Interferencia Potencial	Cualquier modificación en las barras y objetos entre el código y el lector	Ambientes o campos que afecten la transmisión de radio frecuencia.	Puede ser bloqueo del contacto, o bloqueo de línea de vista e inclusive el ruido	La interferencia es muy limitada, debido a la potencia de transmisión	La interferencia es muy limitada, debido a la potencia de transmisión

Fuente:(Cobos y Ortiz, 2017, pp 14) **Modificado por:** Vasquez, Christian 2018

1.7 Tarjetas de desarrollo

Es una placa electrónica hardware que poseen un microcontrolador creado para lenguajes específicos, este gestor permite el diseño y construcción de circuitos, prototipos esta herramienta permite probar la funcionalidad de un proyecto pequeño o un sistema.

En la actualidad existen una amplia gama de tarjetas de desarrollo equipadas con distintas características entre las más utilizadas están Raspberry Pi, Arduino y desde el 2015 está disponible en el mercado ESP8266 en sus diversas versiones.(Cárdenas *et al.*, 2013, p 2; Quispe, 2017).

1.7.1 Arduino

Es una plataforma electrónica open-source de fácil uso de hardware y software, poseen pines analógicos y digitales que pueden ser usados como entradas y salidas, lectura o escritura se puede observar todas las especificaciones en la Tabla 4-1, donde todas las instrucciones y códigos son ejecutadas en el microcontrolador que la tarjeta mediante una interfaz de software denominada la IDE de arduino.(Perales, Barrero y Toral, 2016, p 4).

Tabla 4-1: Especificaciones de un arduino mega

Microcontrolador	**AT mega 328**
Operation Voltaje	5 V
Input Voltaje (Recomendado)	7-12 V
Input Voltaje (limite)	6- 20 V
Digital I/O	14
Analog Input Pints	6
DC Current for I/O Pin	40 mA
DC Current for 33.V Pin	50 mA
Flas Memory	32 KB
SRAM	2 KB
EEPROM	1 KB
Clock Speed	16 Mhz

Fuente:(Comenzando y Arduino, 2009, pp 2)

1.7.2 Raspberry pi

Es considerada una pequeña computadora (SBC) permite simular diferente tipo de código fuente para la ejecución de comandos, mucho mejores características que otras tarjetas de desarrollo, el dispositivo se puede apreciar en la Figura 20-1 y como se ve es pequeño, posee un procesador ARM de 1 GHz, GPU VideoCore IV y 512 Mbytes de memoria RAM, utiliza tarjetas de memoria SD externa para el funcionamiento. (Ruiloba y Quito, 2017, p 19; Colligan, 2018)

Figura 20-1: Dispositivo Raspberry pi
Fuente: https://images-na.ssl-images-amazon.com/images/I/91zSu44%2B34L._SX466_.jpg

1.7.3 ESP8266 Node MCU

Es un pequeño chip que fue creado bajo la necesidad de las IoT, su función principal es la conexión entre el internet y el microcontrolador, mediante una red WIFI autónoma que vienen integrada en este kit de desarrollo, posee limitados pines denominados GPIOs

Tiene las mismas funcionalidades que arduino, los componentes del chip ESP8266 (ESP-12E) se puede ver en la Figura1 21-1, lomas destacable es la facilidad de codificación en lenguajes de programación como LUA y la IDE de arduino (ELECTRONILAB, 2016).

Las nuevas versiones de ESP8266 denominadas NodeMCU cuenta con un chip CH340 que permite una comunicación USB – serial. Este elemento posee grandes características como (ELECTRONILAB, 2016):

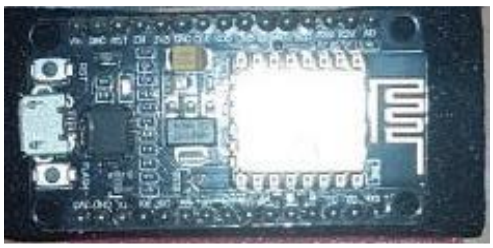


Figura 21-1 Componentes del ESP8266
Fuente: https://programarfacil.com/wp-content/uploads/2017/01/esp-01-partes.jpg

- Código abierto
- Interactivo
- Programable
- Bajo costo
- Sencillo
- Inteligente
- Wifi
- Compatible con arduino
- Usb-ttl
- Plug&play
- 10 gpio cada gpio puede ser pwm,
- I2c
- 1-wire
- Fcc certified wi-fi module
- Pcb antena

En la Tabla 5-1 podemos identificar cada uno de los pines del dispositivos (Rodrigo, 2016)

Tabla 5-1: Data shield del ESP8266 NODE MCU

PIN	FUNCION	PIN	FUNCION
A0	TOUT / ADC 0	D0	GPIO16/USER/WAKE
RSV	RESERVED	D1	GPIO5
RSV	RESERVED	D2	GPIO4
SD3	SD03	D3	GPIO0/FLASH
SD2	SD02/SV POWER	D4	GPIO2/TXD1
SD1	SD01/3.3V	3V3	3.3V
CMD	SDCMD/GROUND	GND	GND
SD0	SDSD0/GPIO	D5	GPIO14/HSCLK
CLK	SDCLK/SDIO	D6	GPIO12/HMISO
GND	GND/VART	D7	GPIO13/RXD2/HMDSI
3V3	3V3HSPI/SPI	D8	GPIO15/TXD2/HCS
EN	EN/KEY	D9	GPIO3/RXD0
RST	RST/SYSTEM	D10	GPIO1/TXD0
GND	GND/ADC	GND	GND
Vin	VIN 5V/RESERVED	3V3	3.3V

Fuente: Vasquez, Christian 2018

1.7.4 Comparación entre tarjetas de desarrollo

En la Tabla 6-1 se analizó las mismas características en los tres dispositivos y se llegó a la conclusión que la mejor opción sería la tarjeta de desarrollo ESP8266 NODE MCU, por ser prácticamente el reemplazo de arduino que nos brinda una interfaz muy amigable para la programación, conexión wifi y costos bajos.

Tabla 6-1: Comparación entre placas de desarrollo

TARJETAS DE DESARROLLO / **CARACTERISTICAS**	***Raspberry pi***	***Arduino***	***ESP8266 Node MCU***
Voltaje de operación	5 V	5 V	3.3 V o 5 V
Entorno Desarrollo	Linux, Eclipse, Windows	IDE de Arduino	IDE de Arduino o LUA
Sistema Operativo	Raspbian		-
Pines Analógicos	-	6	1
Pines Digitales	-	14	-
Pines GPIO	32	-	15
Ethernet	-	Integrado	-
Precio	$ 65	$ 18	$ 9
WIFI	-	-	Integrado
USB	4	-	-

Fuente:(Ruiloba y Quito, 2017,pp 22)

CAPITULO II

2 REQURIMIENTOS HARDWARE Y SOFTWARE DEL PROTOTIPO

En el presente capítulo se pretende dar a conocer la concepción del sistema de control de acceso y la automatización de eventos físicos habituales, mediante la descripción de los dispositivos físicos y gestores de software a emplearse, además de una explicación detallada en cada uno de los procesos de diseño, implementación y funcionamiento del prototipo propuesto.

2.1 Concepción general del prototipo

2.1.1 Concepción general del sistema de control de acceso y registro de usuarios

La concepción general del sistema de control de acceso, registro y automatización es esquematizada en la Figura 1-2, donde de muestra que está constituido por 3 etapas: nodo de control de acceso, nodo de registro y nodo de control de eventos físicos.

El funcionamiento del sistema inicia con la ejecución de la aplicación NFC en cada uno de los teléfonos de los usuarios, que en este caso serían los profesores, esta aplicación servirá como interfaz entre los teléfonos y el circuito controlador para la apertura de la puerta, si la contraseña es correcta y se encuentra dentro de su horario de clases establecido, de manera automática se registrada cada uno de los accesos en la base de datos que será visualizada y administrada por el encargado o administrador.

También por medio de esta misma aplicación podrá cada maestro controlar los dispositivos dentro del laboratorio como: luces, proyector u otros elementos que estén conectados en el nodo de control de eventos físicos mediante el controlador como se muestra en la Figura 1-2.

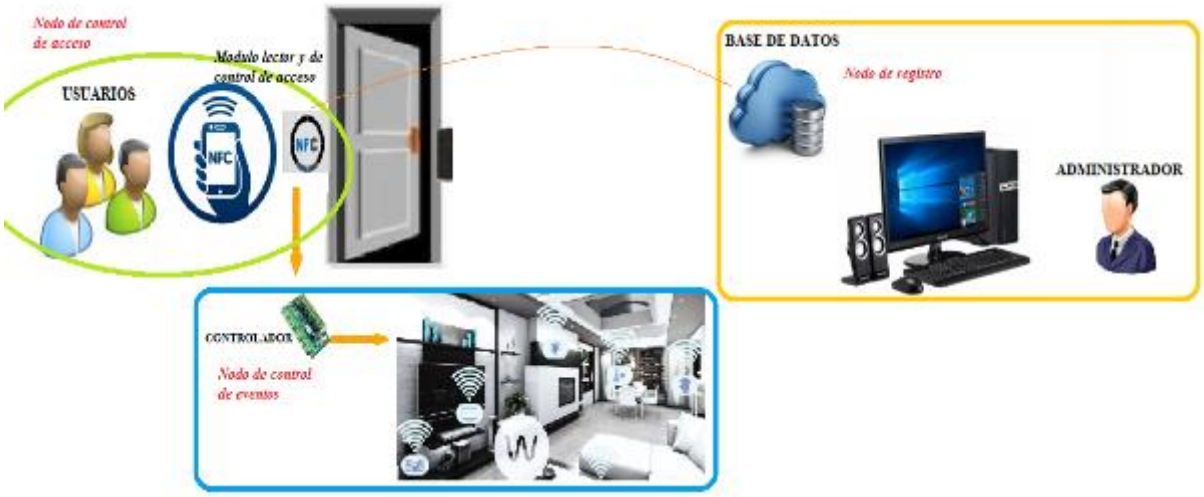


Figura 1-2: Concepción general del sistema de control de acceso, registro y automatización de eventos físicos.
Realizado por: VÁSQUEZ, Christian 2018

Para este sistema cada uno de los usuarios debe de realizar un registro previo de forma manual con el administrador o encargado de los laboratorios, donde se solicitará una clave a cada uno de los usuarios, la cual permitirá el acceso a cada uno de los laboratorios o aulas en horarios de clases establecidos

2.1.2 Concepción general de la automatización de eventos físicos

El control de eventos físicos que se pretende realizar a los dispositivos, equipos y elementos de electrónicos de las aulas y laboratorios se puede apreciar en la Figura 2-2, estos controles domóticas van hacer generados con la misma aplicación del control de acceso, integrando ciertos botones para el manipular de una forma cómoda y confortable, mediante la tecnología NFC, aprovechando el controlador del control de acceso ESP8266 NODE MCU, para la transmisión de estas instrucciones utilizando la red inalámbrica que genera el dispositivo.

El enfoque de comunicación NFC-WIFI garantizara la correcta manipulación de los dispositivos y equipos del aula o laboratorio, siendo manipulados solo cuando el usuario adecuado este dentro de dicho recinto en un horario establecido de clases y no de los exteriores, como se puede realizar con la tecnología wifi o bluetooth.

Figura 2-2: Nodo de control de eventos físicos
Realizado por: VÁSQUEZ, Christian 2018

2.2 Arquitectura y requerimientos hardware del sistema

2.2.1 Nodo de control de acceso

Según el diagrama de bloques que se aprecia en la Figura 3-2, nos habla sobre el funcionamiento general, donde el bloque de procesamiento es ejecutado por el dispositivo ESP8266 NODE MCU, encargado de la lectura de códigos y la transmisión de datos a la web para validar su respuesta el bloque de control.

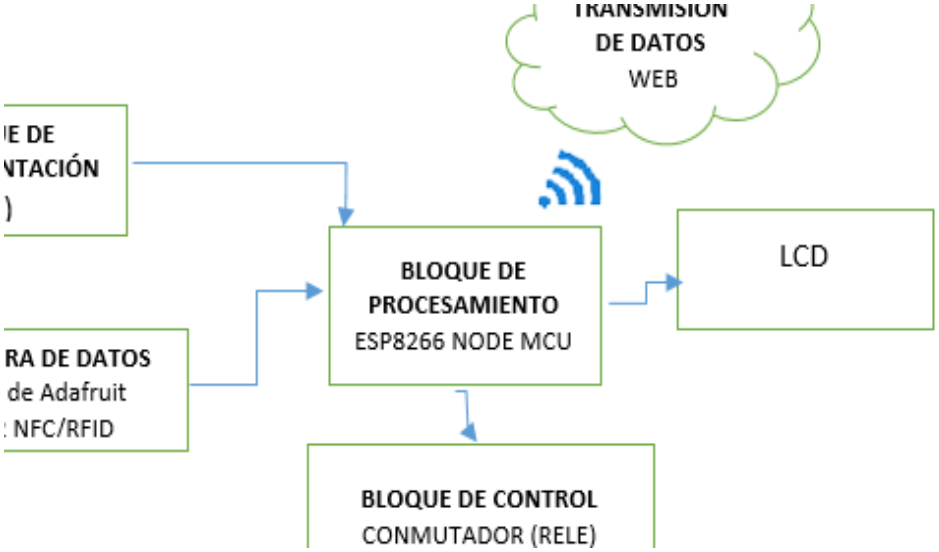


Figura 3-2: Diagrama de bloques del control de acceso
Realizado por: VÁSQUEZ, Christian 2018

En el bloque de recepción de datos el dispositivo que se utiliza es Shield de Adafruit PN532 NFC/RFID, captando los datos del Smartphone del usuario para enviarlos al NODE MCU, que

interpreta los datos y los envía vía WIFI hacia el servidor donde se validara la información, y se ejecutara los resultados en el bloque de control, dando pulsos on/off al relé.

2.2.2 Nodo de automatización de eventos físicos

Similar al nodo de control de acceso, los cambios se dieron en el bloque de control por un módulo de redes y la eliminación del bloque del LCD como se muestra en la figura 4-2. El bloque de lectura está enfocado a captar datos NFC a ser ejecutados en los actuadores relés una vez que el bloque de procesamiento, asigne señales off / on a los pines D5, D6, D7 y D8.

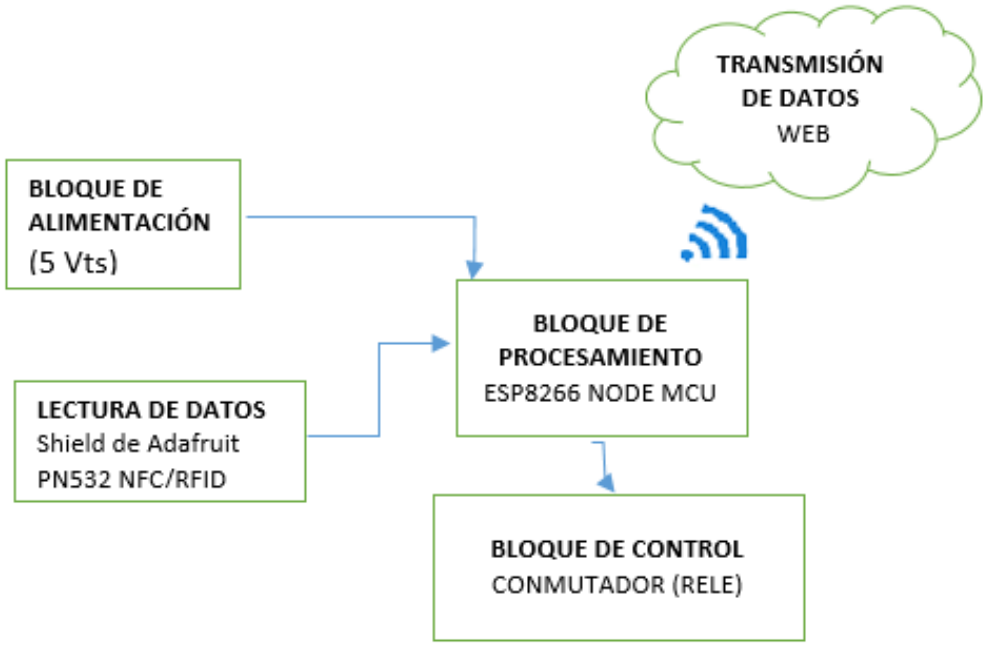


Figura 4-2: Diagrama de bloques del control de eventos físicos
Realizado por: VÁSQUEZ, Christian 2018

2.2.3 Descripción de dispositivos utilizados

2.2.3.1 ESP8266 NODE MCU

Es un microcontrolador de código abierto que se desarrolló de la evolución ESP8266 que brinda una solución de red inalámbrica autónoma, sirviendo como interfaz entre el actuador y el elemento controlador.

En la Figura 5-2 se presenta la tarjeta de desarrollo, también viene incluido en este dispositivo un conector usb y varios pines denominados GPIO, fácil de conectar, flasear y configurar en la IDE

de arduino. (Anonymous, 2017, p 1)**.** El datasheet sus especificaciones y su configuración previa en la interfaz de arduino se puede ver en el Anexo 1.

Figura 5-2: Tarjeta de desarrollo ESP8266 NodeMCU WiFi
Realizado por: VÁSQUEZ, Christian 2018

2.2.3.2 Shield de Adafruit PN532 NFC/RFID

Es un módulo que utiliza un grupo de chips PN532 este modelo es prácticamente es el mismo que componente que incorporan en los Smartphone que trabajan con la tecnología NFC, este elemento se puede observar en la Figura 6-2, que es considerado uno de los mejores en el mercado por su gran funcionalidad al momento de escribir y leer en tags, tarjetas y etiquetas, ideal para los sistemas de pagos mediante la comunicación con teléfonos (Adafruit, 2018)**.**

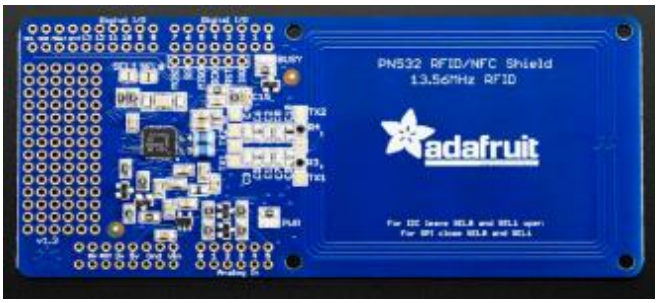


Figura 6-2: Módulo PN532 NFC/ RFID de ADAFRUIT
Fuente: https://cdn-shop.adafruit.com/970x728/789-03.jpg

Las especificaciones técnicas del dispositivo NFC se pueden observar en la Tabla 1-2 se identifican las características principales del elemento PN532 NFC,

Tabla 1-2: Especificaciones del PN532

Voltaje de funcionamiento	**5V**
Frecuencia	13,56 Mhz
Rango de antena	5cm
Ancho	53,3 mm
Largo	117.7
Espesor	1.1 mm
Peso	9 gr

Fuente:(Lara and Vallejo, 2016; Adafruit, 2018)

2.2.3.3 Relé

Es un dispositivo que funcionan como un interruptor cuando recibe una pequeña corriente en la bobina, el cual se imanta y atrae a uno de sus contactos para dar paso a través de ellos a una corriente mucho mayor (platea.pntic, 2008, p 1).

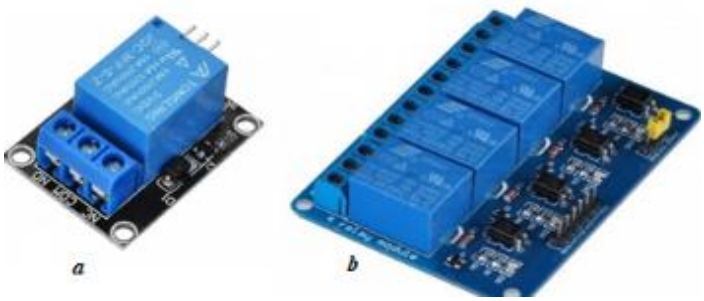


Figura 7-2: Conmutador a 5Vts
Fuente: http://img.dxcdn.com/productimages/sku_448813_1.jpg

En la **Figura 7-2 a** se observa el elemento utilizado para el control de acceso que permitirá la habilitación de la puerta. En la **Figura 7-2 b** se ve el elemento utilizado en el nodo de control de eventos físicos que van conectados los diversos equipos para el encendido automático.

2.2.3.4 LCD

Es una pantalla electrónica de cristal líquido, es un dispositivo muy básico utilizado como periférico de salida para el control de ejecuciones y resultados, son muy económicas (Kushagra, 2015, p 1). El display utilizado para la visualización de mensajes en el control de acceso, es un LCD 16 x2 permitiéndonos mostrar 32 caracteres repartidos en 2 filas es decir 2 filas y 16 columnas. El dispositivo se puede apreciar en la Figura 8-2.

Figura 8-2: Pantalla de cristal líquido 16 x 2
Fuente: http://www.orientlcd.com/v/vspfiles/photos/AMC1602AR-B-B6WTDW-2.jpg

2.2.3.5 I2C

Es un nuevo protocolo que se ha implementado para el control de varios esclavos mediante un controlador maestro, para su funcionamiento, I2C utiliza 2 vías de comunicación llamadas SDA

(Serial Data) y SCL (Serial Clock), SDA permite la comunicación maestro esclavo mientras que SCL la señal de reloj (Morales. Michel, 2017). En la Figura 9-2 se puede visualizar el dispositivo.

Figura 9-2: Conector I2C para LCD
Fuente: https://powergie.com.mx/wp-content/uploads/2017/09/Adaptador-pantalla-LCD-16×2-Serial-I2C-PCF8574.jpg

2.2.3.6 Conexión del LCD 16 X 2 y el I2C

La conexión entre estos dos elementos es muy sencilla ya que son dispositivos creados de forma estándar respecto a la ubicación de los pines del I2C con el LCD, fáciles de conectar y soldar los 16 pines que tienen en común, la información es procesada por el I2C en las 2 salida SDA y SCL, en la Figura 10-2. Se aprecia la unión de estos dos dispositivos.

Figura 10-2: LCD con I2C
Fuente: https://www.makerlab-electronics.com/my_uploads/2016/06/16x2-i2c-lcd-blackgreen-02.jpg

2.3 Esquema de conexión del control de acceso

A continuación, se destalla la conexión de cada uno de los componentes con el controlador central Esp8266 Node MCU, el cual es considerado el elemento electrónico más importante ya que establece la comunicación con los diversos elementos.

2.3.1 Conexión de ESP8266 Node MCU con Adafruit PN532 nfc/rfid

En la Figura 11-2 se observa de forma general la conexión de comunicación y la conexión de alimentación con el dispositivo NFC mediante el NODE MCU, las cuales son detallada a continuación de forma específica en las tablas (Tabla 1-2, Tabla 1-2), diseñosy los datasheets del ESP8266 NODE MCU y NP532 NFC ubicados en el Anexo A y Anexo D donde nos muestra el manejo de pines GPIO XX o D XX.

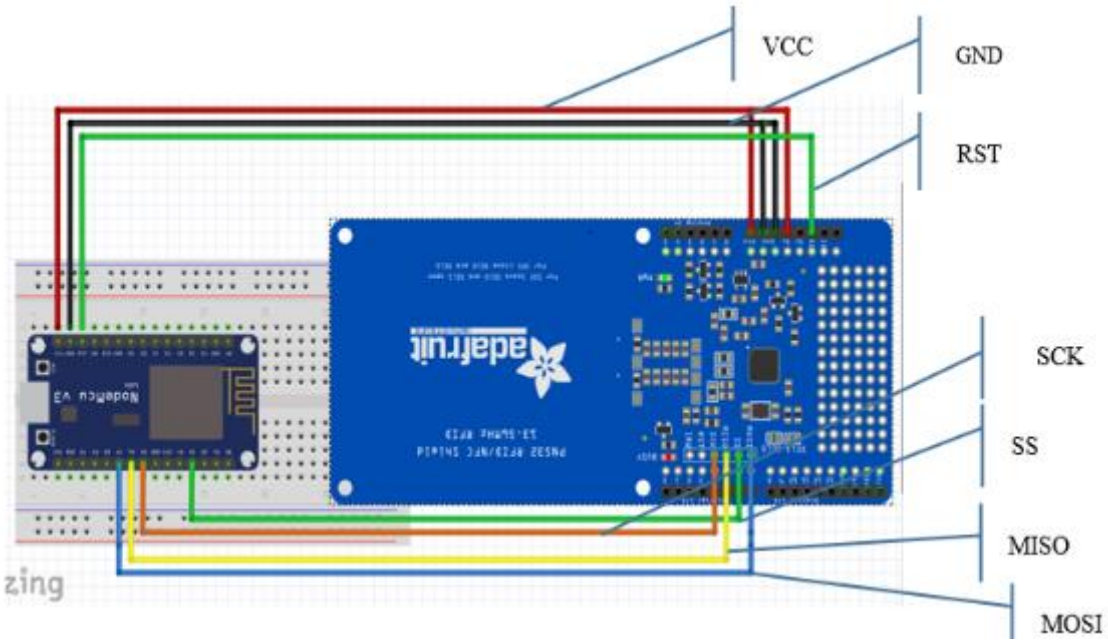


Figura 11-2: Conexión ESP8266 Node MCU con Adafruit PN532 nfc/rfid
Realizado por: VÁSQUEZ, Christian 2018

2.3.1.1 Comunicación SPI

Adafruit pn532 nfc/rfid tiene dos tipos de comunicación para su funcionamiento (I2C y SPI), se hizo uso de la comunicación SPI, para habilitarlo se debe cerrar el circuido de conexión soldando SEL1 y SEL2, como se muestra en la Figura 12-1.

Figura 12-2: Comunicación SPI en Shield Adafruit PN532
Realizado por: VÁSQUEZ, Christian 2018

La comunicación SPI usa un bus de 3 líneas, dos de ellas son utilizadas para el intercambio de datos (recepción y trasmisión full dúplex) y la otra línea es la señal de reloj, permitiendo que los dispositivos funcionen de forma Maestro – Esclavo.

Donde el maestro genera señales de control y reloj iniciando con la transferencia de datos, el dispositivo de adafruit PN532 realiza esta acción mediante el pin SS y las 3 líneas denominadas MISO, MOSI y SCK como se aprecia en Figura 12-2.

Tabla 2-2: Pines de conexión Adafruif PN532 – Esp8266 node mcu

ADAFRUIF PN532	ESP8266 NODEMCU
SDA/SS	GPIO 00 D3 Verde
SCK	GPIO 14 D5 Naranja
MOSI	GPIO 13 D7 Azul
MISO	GPIO 12 D6 Amarillo

Realizado por: VÁSQUEZ, Christian 2018

La forma adecuada para la conexión se indica en la Tabla 2-2 siguiendo las especificaciones como:

1. SS o también llamado SDA va conectado al D3 identificado con el cable verde
2. SCK va conectado al D5 identificado con el cable Naranja
3. MOSI va conectado al D7 identificado con el cable Azul
4. MISO va conectado al D6 identificado con el cable Amarillo

2.3.1.2 Alimentación de la Shield PN532

Las conexiones realizadas en cada uno de los pines se encuentran especificados en la Tabla 3-2, donde los pines (5V y VIN) van al pin VIN de node mcu y los pines negativos con sus similares del otro dispositivo, con cable verde se visualiza cada la conexión con los pines RST.

Tabla 3-2: Conexión Pines

ADAFRUIF PN532	ESP8266 NODEMCU
RST(verde)	RST
5V (rojo)	VIN
GND (negro)	GND
GND (negro)	GND
VIN (rojo)	VIN

Realizado por: VÁSQUEZ, Christian 2018

2.3.2 Conexión del ESP8266 Node MCU con el conmutador (rele)

En la Figura 13-2 se muestra la conexión entre el dispositivo controlador con el rele a 5 voltios mediante el pin D4 del esp8266 node mcu hacia el pin del relé que está identificado como señal de entrada con el cable azul, y la conexión respectiva con los cables de alimentación VIN y GND.

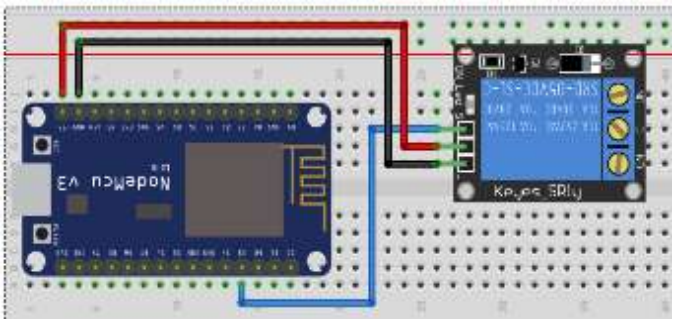


Figura 13-2: Conexión entre ESP8266 NODE MCU y Rele
Realizado por: VÁSQUEZ, Christian 2018

2.3.2.1 Conexión del ESP8266 Node MCU entre LCD 16x 2 con I2C

En la Figura 14-2 se puede observar la conexión de entre el controlador y el componente I2C que está en comunicación directa con la pantalla de cristal líquido, los pines que se utilizan se especifican en la Tabla 4-2 por medio de esto se interpreta.

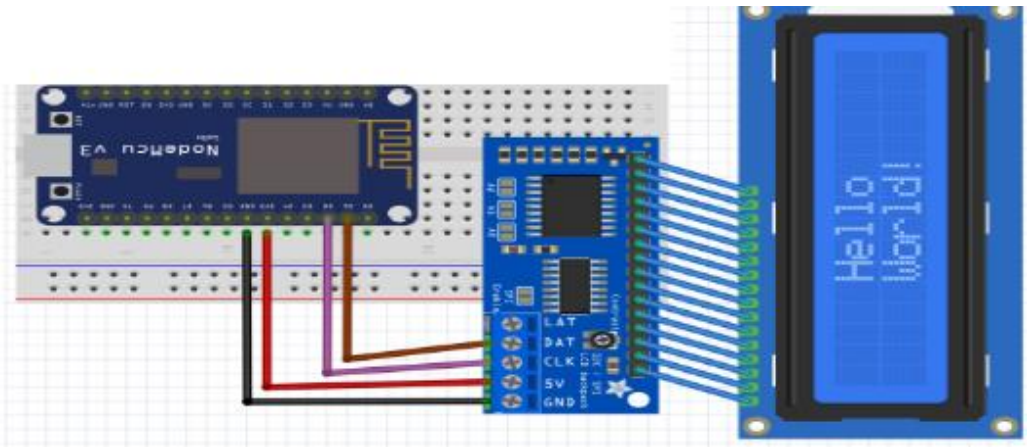


Figura 14-2: Conexión entre ESP8266 NODE MCU y LCD con I2C
Realizado por: VÁSQUEZ, Christian 2018

Las conexiones correctas se detallan en la Tabla 4-2

1. El pin GND en el LCD se conecta al pin GND del NodeMCU
2. El pin VCC en el LCD se conecta al pin VIN del NodeMCU.
3. El pin SDA en el LCD se conecta al pin D2 del NodeMCU.
4. El pin SDL en el LCD se conecta al pin D1 del NodeMCU.

Tabla 4-2: Pines entre LCD con I2C y esp8266 NODE MCU

LCD con I2C	ESP8266 NODEMCU
SDA	D2
SDL	D1
VIN	3.3 V(rojo)
GND	GND (negro)

Realizado por: VÁSQUEZ, Christian 2018

La conexión de todos estos dispositivos mencionados y vistos en los diseños anteriores con el controlador esp8266 node mcu da como resultado el diseño que se puede apreciar en la Figura 15-2, que muestra el diseño final del nodo de control de acceso. Que incorpora el regulador de voltaje lm7805 que proveerá el voltaje necesario a cada dispositivo.

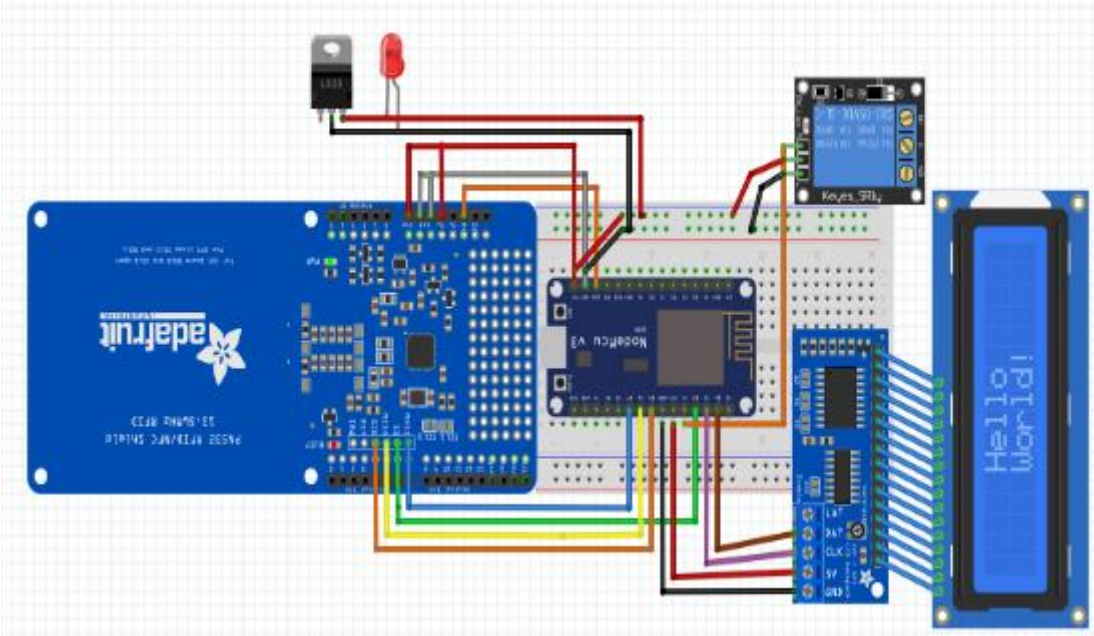


Figura 15-2: Diseño de conexión final del controlador de acceso
Realizado por: VÁSQUEZ, Christian 2018

2.3.3 Esquema de conexión del control de eventos físicos

El diseño de este nodo no posee una compleja estructura ya que este nodo se encarga de la generación de la red inalámbrica y recepción de instrucciones mediante la tecnología wifi, para la habilitación de los puertos D5, D6, D7 y D8, en caso de existir más elementos a conectar se procede a la habilitación de los diversos puertos libres como se observa en la Figura 16-2.

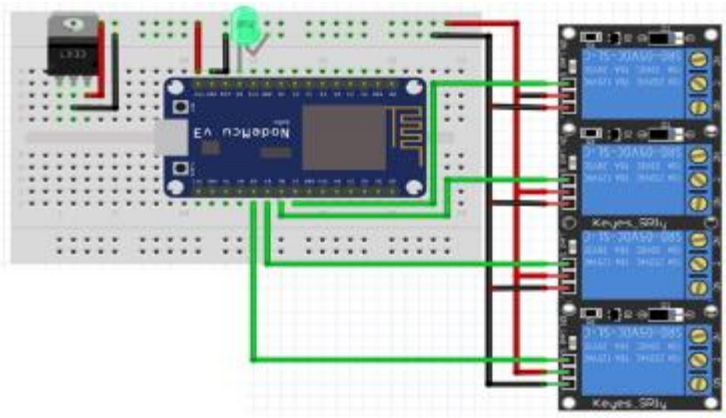


Figura 16-2: Diseño de conexión de node MCU con el módulo relé
Realizado por: VÁSQUEZ, Christian 2018

La conexión se aprecia en la Tabla 5-2 desde las señales del relé hacia el ESP8266 NODE MCU:

1. D5 conectado a la señal 1 del relé
2. D6 conectado a la señal 2 del relé
3. D7 conectado a la señal 3 del relé
4. D8 conectado a la señal 4 del relé

Tabla 5-2: Conexión Pines

MODULO RELÉ	ESP8266 NODEMCU
D1	D5
D2	D6
D3	D7
D4	D8
GND (negro)	GND
VIN (rojo)	VV

Realizado por: VÁSQUEZ, Christian 2018

2.4 Requerimientos de Software

2.4.1 IDE De Arduino

Es una plataforma de software libre diseñado para varios sistemas operativos y una amplia gama de usuario de nivel corporativo y estudiantes, está enfocada en una placa de desarrollo que posee varios pines de entrada/salida, analógicos o digitales y un microcontrolador en el cual se almacena la programación de comandos he instrucciones para la ejecución de componentes y elementos que son identificados mediante el uso de librerías (Baeza y Pomares, 2009,p 9).

Requerimientos para el ESP8266 NODE MCU

Para la utilización de la IDE de arduino con el ESP8266 NODE MCU es necesario descargar he instalar el componente para el reconocimiento de las placas ESP, para ello seguimos los siguientes pasos:

1. Una vez abierto la IDE de arduino damos clic en **Archivo**, se despliega un menú en el cual escogemos **Preferencias**, damos clic y se despliega una nueva ventana que se puede ver en la Figura 17-2, en la cual debemos colocar el siguiente link: **http://arduino.esp8266.com/stable/package_esp8266com_index.json,http://arduino.esp8266.com/stable/package_esp8266com_index.json**, finalmente damos clic en **OK.** Esto se realiza para dar a conocer al programa la ruta de donde debe descargarse las librerías para más información se amplía en el Anexo B.

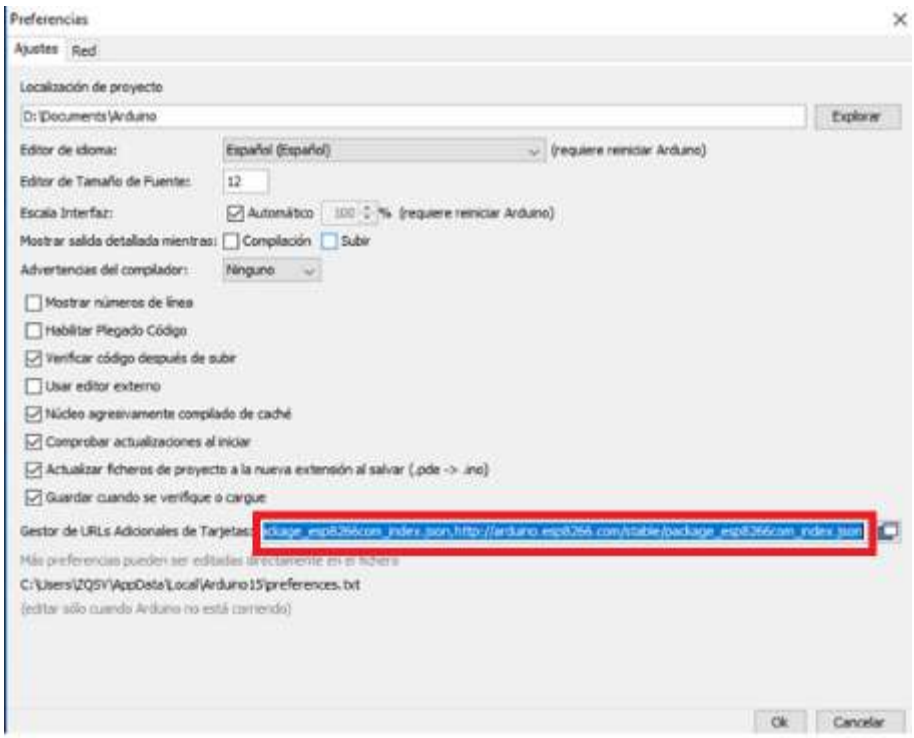


Figura 17-2: Configuración de la url para esp8266
Realizado por: VÁSQUEZ, Christian 2018

2. Damos clic en **Herramientas** se despliega un menú donde escogemos **Placa** dentro de placa escogemos **Gestor de Tarjetas** tal como se puede observar en la Figura 18-2.

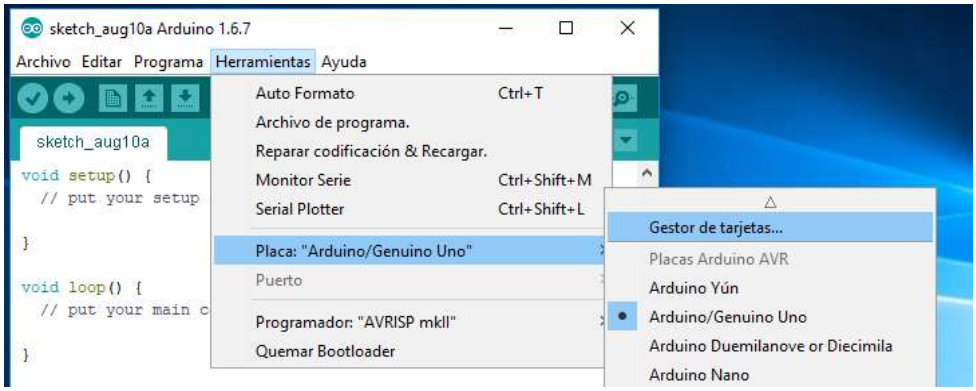


Figura 18-2: Configuración para descarga de la placa NODE MCU
Realizado por: VÁSQUEZ, Christian 2018

3. La nueva ventana que se despliega se puede apreciar en la Figura 19-2 donde debemos escribir **ESP8266**, escogemos he instalamos la primera opción se despliega una vez instalado cerramos la ventana.

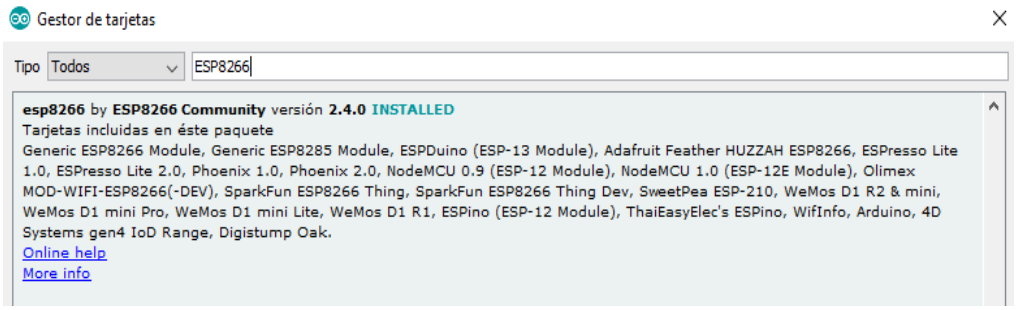


Figura 19-2: Instalación de la placa y librerías ESP8266
Realizado por: VÁSQUEZ, Christian 2018

4. En la Figura 20-2 se puede apreciar la interfaz de la IDE de arduino cargada con todos los posibles componentes de la familia ESP8266, en el caso de nuestro proyecto se va a utilizar la placa **NodeMCU 1.0 (ESP-12E Module)**.

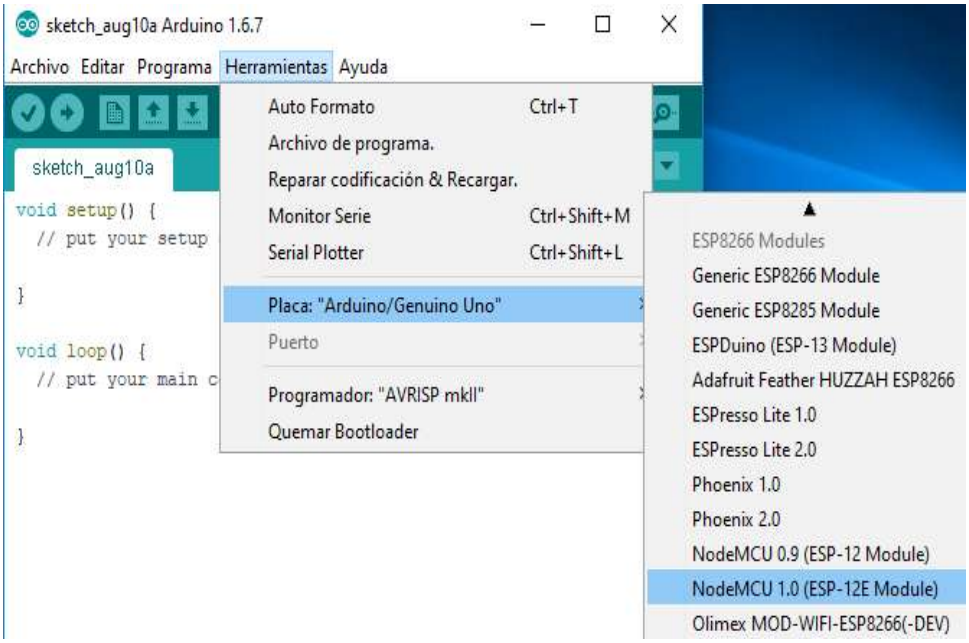


Figura 20-2: Interfaz de IDE de Arduino
Realizado por: VÁSQUEZ, Christian 2018

2.4.1.1 Librerías

Para la elaboración del sketch es necesario establecer librerías las cuales permitan la comunicación, funcionamiento e interacción entre los dispositivos mencionados anteriormente. Estas librerías se presentan en la Tabla 6-2, donde se detallan cada uno de las funciones y en los dispositivos con los cuales fueron empleados, adicional a esto se menciona la fuente de donde se obtuvieron cada una de las librerías externas.

Tabla 6-2: Librerías para el funcionamiento del sistema

DISPOSITIVO	LIBRERÍA POR DEFECTO	LIBRERÍA EXTERNA	URL EXTERNA	DESCRIPCIÓN
IDE ARDUINO	<SPI>	-	-	Permite comunicarse con dispositivos SPI, con el Arduino como dispositivo maestro
	<wire.h>	-	-	Permite comunicarse con dispositivos I2C / TWI.
Adafruit PN532 NFC/RFID	-	<PN532_SPI.h>	https://github.com/adafruit/Adafruit_NFCShield_I2C	Permite la lectura escritura de NFC con el modo SPI
	-	<Snep.h>	https://github.com/don/NDEF	Permite la comunicación para el Shield NFC y los dispositivos externos.
	-	<Ndefmessage.h>	https://github.com/don/NDEF	Facilita la creación y encapsulación de tramas NDEF.
ESP8266 NODE MCU	-	<ESP8266WiFi.h>	http://arduino.esp8266.com/stable/package_esp8266com_index.json	Permite la comunicación entre la placa esp y los dispositivos WIFI
	-	<WiFiClient.h>	http://arduino.esp8266.com/stable/package_esp8266com_index.json	Habilitar la conexión como clientes a las diferentes redes WIFI
	-	<ESP8266WebServer.h>	http://arduino.esp8266.com/stable/package_esp8266com_index.json	Permite que el dispositivo actué como un servidor
LCD CON I2C	-	<LiquidCrystal_I2C.h>	https://github.com/marcoschwartz/LiquidCrystal_I2C	Permite la comunicación I2C

Realizado por: VASQUEZ, Christian 2018

2.4.1.2 Código para conectarse a una red

Para conectarse a una red wifi utilizamos las librerías ESP8266WiFi.h y WiFiClient.h, estas librerías permiten la ejecución de funciones soft-AP o WiFi.begin, en este caso como modo cliente se establece configuraciones y parámetros como:

- SSID: Se denomina así a la cadena de caracteres o nombre de la red wifi (máximo 63 caracteres).
- PASSWORD: Es la contraseña establecida en la red wifi.

En la Figura 21-2 se muestra la configuración con la IDE de arduino en el esp8266 node mcu, donde se coloca el nombre de la red y la contraseña, también la IP del servidor de la base de datos en donde se autenticará las credenciales del usuario. Para garantizar la conexión a la red colocamos en el ciclo while la sentencia que permitirá pasar a la siguiente instrucción caso contrario permanecerá de forma indefinida dentro del ciclo hasta que se conecte.

```
//DECLARACION DE VARIABLES PARA LA CONEXION A LA RED
const char* ssid = "LAB4";
const char* password = "0987654321";
const char* host = "192.168.43.199";
```

Figura 21-2: Redes Inalámbricas de FIE-ESPOCH
Realizado por: VÁSQUEZ, Christian 2018

2.4.1.3 Lectura de datos del ADAFRUIT PN532 NFC- RFID

Para la lectura del NFC mediante el celular utilizamos las librerías PN532_SPI.h, NdefMessage.h, y snep.h, donde vamos a recibir el mensaje y procesarlo con la función NfcReceive, adquiriendo y almacenando datos dentro de la variable payloadAsString, que retornara una respuesta de la función, como se puede ver en la Figura 22-2.

```
String nfcReceive()
{
    int msgSize = nfc.read(ndefBuf, sizeof(ndefBuf));

    if (msgSize > 0)
    {
        NdefMessage msg  = NdefMessage(ndefBuf, msgSize);
        NdefRecord record = msg.getRecord(0);
        int payloadLength = record.getPayloadLength();
        byte payload[payloadLength];
        record.getPayload(payload);
              int startChar = 0;
        if (record.getTnf() == TNF_WELL_KNOWN && record.getType() == "T")
        { // text message
          // skip the language code
          startChar = payload[0] + 1;
        } else if (record.getTnf() == TNF_WELL_KNOWN && record.getType() == "U")
        {
          startChar = 1;
        }
        payloadAsString = "";
        for (int c = startChar; c < payloadLength; c++)
        {
          payloadAsString += (char)payload[c];
        }
    }
```

Figura 22-2: Función para la recepción del mensaje NFC
Realizado por: VÁSQUEZ, Christian 2018

2.4.1.4 Envió de datos al servidor

La variable payloadAsString posee la información almacenada del NFC, esta información es transformada a datos enteros en la variable identificador, utilizando el código que se muestra en la Figura 23-2 se envía los datos al servidor de manera inalámbrica (wifi) mediante el método GET.

```
Serial.println(payloadAsString);
//delay(3000);
int identificador=payloadAsString.toInt();
Serial.println("El identificador que imprime es ");
Serial.println(identificador);

client.print(String("GET /nfccontrol/prueba_1.php?pass_acceso=") +
         identificador  + " HTTP/1.1\r\n" +
        "Host: " + host + "\r\n" +
        "Connection: close\r\n" +
        "\r\n"
       );
```

Figura 23-2: Código para el envio de datos al servidor
Realizado por: VÁSQUEZ, Christian 2018

2.4.1.5 Recepción de datos del servidor

Para recibir los datos provenientes del servidor se utiliza el código de la Figura 24-2 donde, la variable **line** almacena toda la información que recibe el puerto serial. Para poder extraer el dato especifico a utilizar se realiza una condición donde solo se extrae los datos que están contenidos entre un asterisco y un guion (*****puertaon**-**).

```
cepcion datos del servidor_____________________________

nile (client.connected())

     if(client.available())
     {

          String line = client.readStringUntil('\n');
          Serial.println(line);

     }
```

Figura 24-2: Código para la recepción de datos del servidor
Realizado por: VÁSQUEZ, Christian 2018

El diagrama de flujo de el Gráfico 1-2 muestra el funcionamiento del programa cargado en la placa esp8266 node mcu, para el control de acceso, donde intervienen cada uno de los códigos como:

- Conexión a la red
- Lectura de datos nfc
- Envió de datos al servidor
- Recepción de datos del servidor

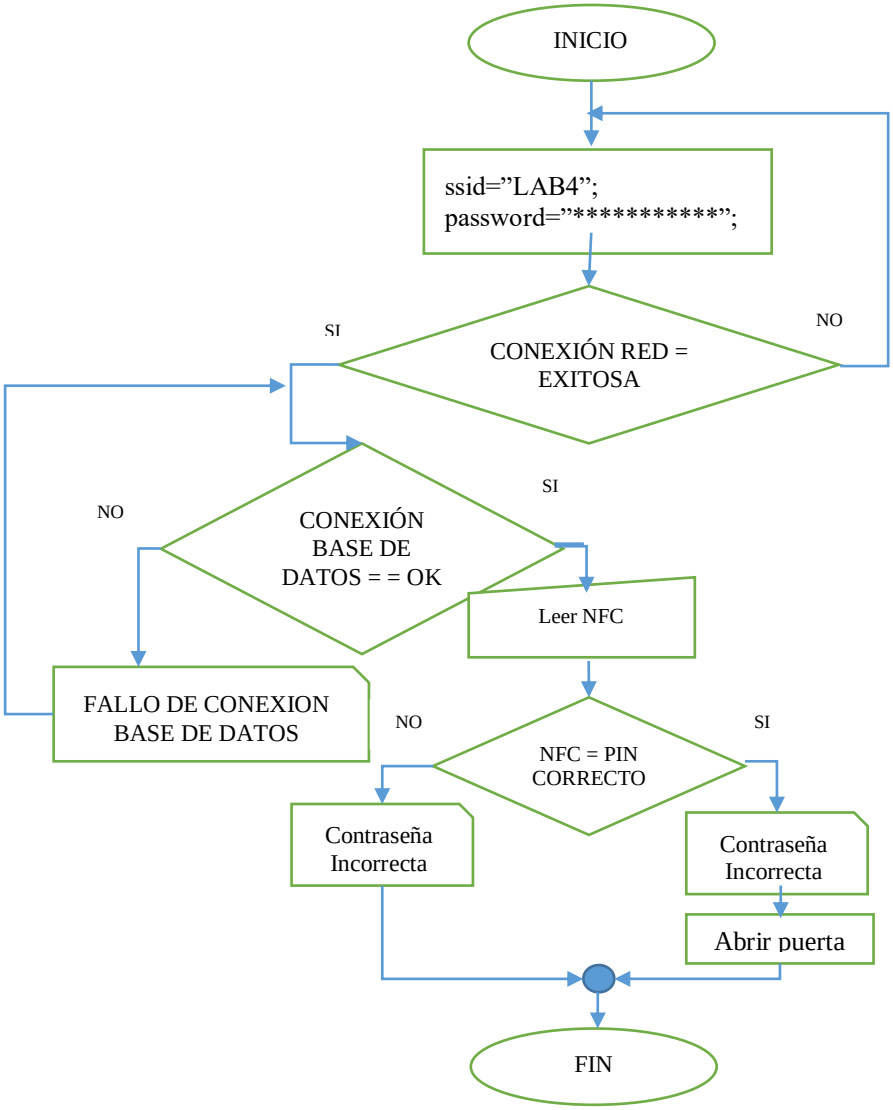


Gráfico 2-1: Diagrama de flujo del control de acceso
Realizado por: VÁSQUEZ, Christian 2018

2.4.1.6 Código para el control de eventos físicos

La **función nfcReceive** nos devuelve un valor en la variable petición, esta es comparada y ejecutada en una de las condiciones para el encendido o apagado de unos de los elementos, el código utilizado se aprecia en la Figura 25-2.

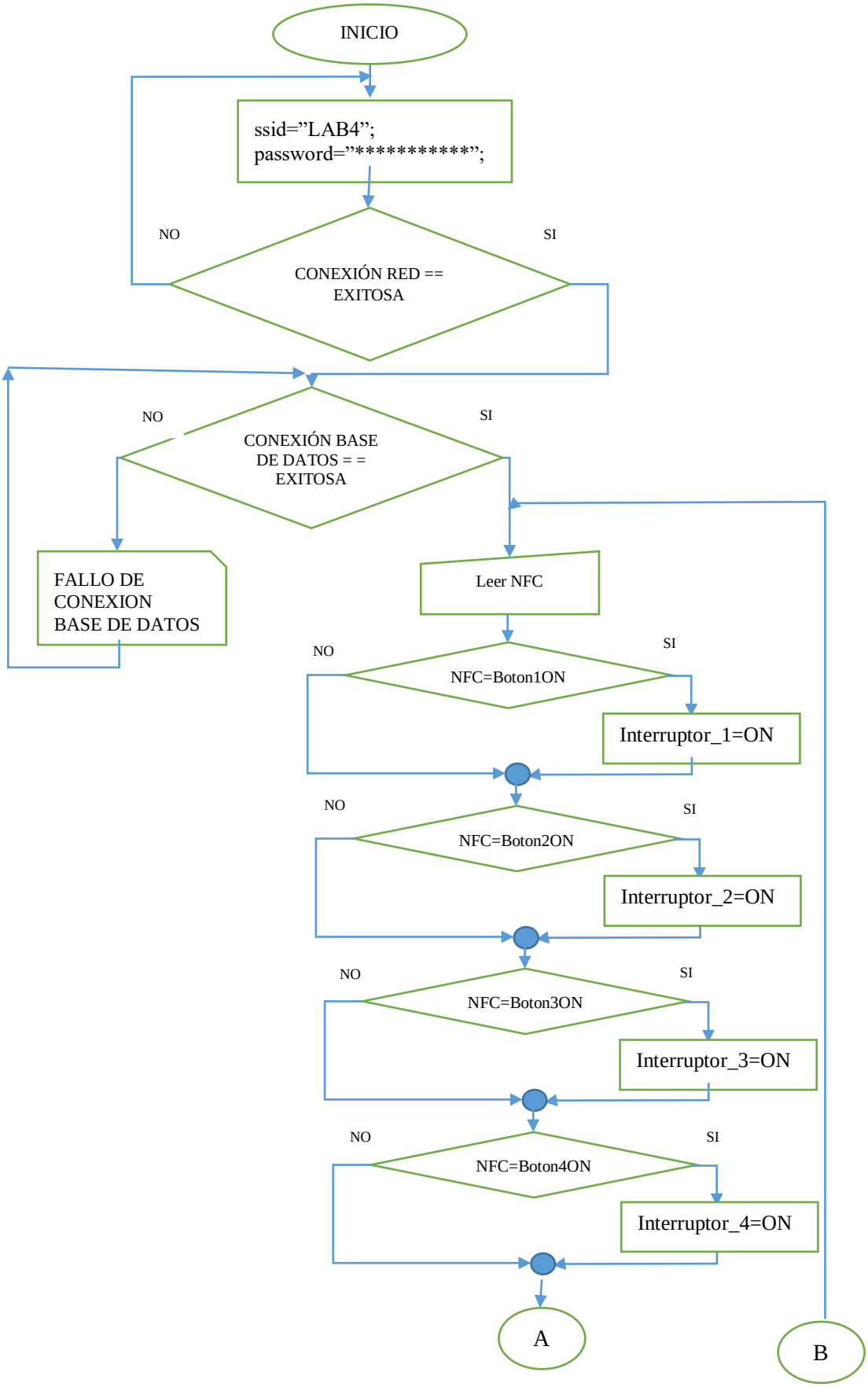
```
String peticion=payloadAsString;
//_____________-Boton 1_____________________
if(peticion=="1on")
{
   Serial.println("boton1 Enciende ");
   digitalWrite(16, LOW);//Prende GPIO15 (D0)
}
if(peticion=="1off")
{
   Serial.println("boton 1 Apaga");
   digitalWrite(16, HIGH);//Prende GPIO15 (D0)
}
//_____________Boton 2_____________________
if(peticion=="2on")
{
   Serial.println("boton 2 Enciende ");
   digitalWrite(5, LOW);//Prende GPIO15 (D1)
}
if(peticion=="2off")
{
   Serial.println("boton 2 Apaga");
   digitalWrite(5, HIGH);//Prende GPIO15 (D1)
}

//_____________Boton 3_____________________
if(peticion=="3on")
{
   Serial.println("boton 3 Enciende ");
   digitalWrite(4, LOW);//Prende GPIO15 (D2)
}
if(peticion=="3off")
{
   Serial.println("boton 3 Apaga");
   digitalWrite(4, HIGH);//Prende GPIO15 (D2)
}
//_____________Boton 4_____________________
if(peticion=="4on")
{
   Serial.println("boton 4 Enciende ");
   digitalWrite(2, LOW);//Prende GPIO15 (D4)
}
if(peticion=="4off")
{
   Serial.println("boton 4 Apaga");
   digitalWrite(2, HIGH);//Prende GPIO15 (D4)
}
peticion=" ";
```

Figura 25-2: Recepción de códigos ON/OFF

Realizado por: VÁSQUEZ, Christian 2018

En el Grafico 2-2 se puede observar el diagrama de flujo del programa que se carga en la placa esp8266 node mcu, para la administración de los eventos físicos.


INICIO
ssid=”LAB4”;
password=”**********”;
NO
SI
CONEXIÓN RED == EXITOSA
NO
SI
CONEXIÓN BASE DE DATOS = = EXITOSA
FALLO DE CONEXION BASE DE DATOS
Leer NFC
NO
SI
NFC=Boton1ON
Interruptor_1=ON
NO
SI
NFC=Boton2ON
Interruptor_2=ON
NO
SI
NFC=Boton3ON
Interruptor_3=ON
NO
SI
NFC=Boton4ON
Interruptor_4=ON
A
B

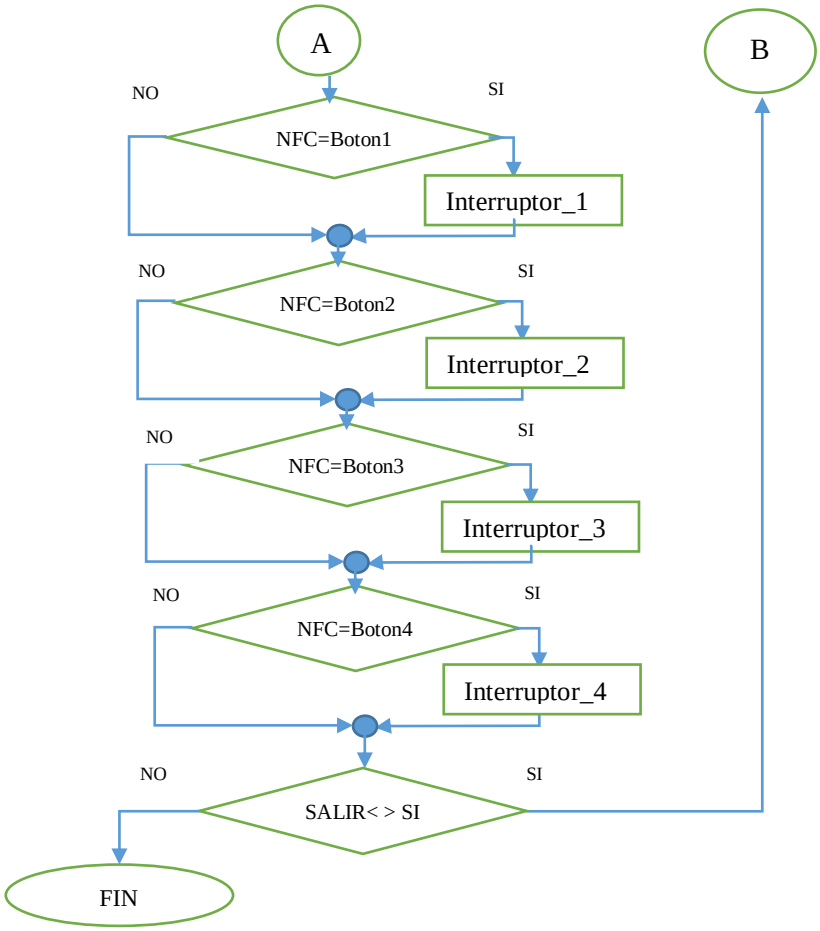


Gráfico 2-2: Diagrama de flujo de la automatización de eventos físicos
Realizado por: VÁSQUEZ, Christian 2018

2.4.2 MYSQL

Para la creación de la base de datos se ha utilizado una herramienta de software libre con licencia GNU, que contiene interpretes para varios lenguajes como script PHP y servidor web, permitiendo un manejo eficiente y muy intuitivo para la administración de una base de datos.

Figura 26-2: Estructura de la base de datos del control de acceso
Realizado por: VÁSQUEZ, Christian 2018

En este software creamos una base de datos con el nombre **db_control_acceso**, para el proyecto se requirió crear **8 Tablas** las cuales se pueden apreciar en la Figura 26-2, cada una de estas tablas fueron utilizadas para:

- **datos_admin:** Se almacena los datos solo de administradores y encargados de laboratorios teniendo campos como: (id, fecha, apellidos, nombres, ci, pass_admin, pass_user, privilegio).
- **tbacceso:** Se registra los ingresos de usuarios en los campos (id_acceso, hora, id_chip, pin).
- **tbdías:** Están almacenados todos los días laborables (id_dia, descripción_dia)
- **tbhorario:** Están almacenadas todas las horas desde la mañana hasta la noche (id_hora, inicio, fin, descripción_hora).
- **tblaboratorios:** Se encuentran guardados los laboratorios existentes en el edificio de la FIE y en el modular antiguo de electrónica (id_lab, código_lab, nombre_lab, ubicación_lab, foto_lab).
- **tblogin:** Se guarda toda la información de los usuarios (id, cedula, nombre, email, password y privilegio)
- **tbmaterias:** Se almacena toda la información de cada una de las materias (id_materia, código_mat, monbre_mat, semestre y paralelo)
- **tbregistros:** Se almacena todas las reservaciones de los laboratorios (id_registro, id_lab, id_hora, id, id_materia y id_hora).

2.4.2.1 Diagrama identidad-relación del sistema de registros de usuarios para el control de acceso

En la Figura 27-2 se observa las múltiples relaciones que se utilizaron en el sistema de control de acceso registro y automatización de eventos físicos, donde se utilizan 8 Tablas, una de estas tablas **datos_admin** no está relacionado con las otras tabas esta funciona de forma independiente sin necesidad de relacionarse a las demás, ya que solo los administradores pueden realizar el ingreso al sistema de registros.

Para poder relacionar las otras tablas se tuvo que crear la tabla tbregistros con el campo clave o primary key de cada una de las tablas, con lo se consiguió correlacionar cada uno de los campos para ejecutar las distintas instrucciones como comparaciones, condiciones, inserciones, modificaciones, actualizaciones y eliminaciones en la base de datos.

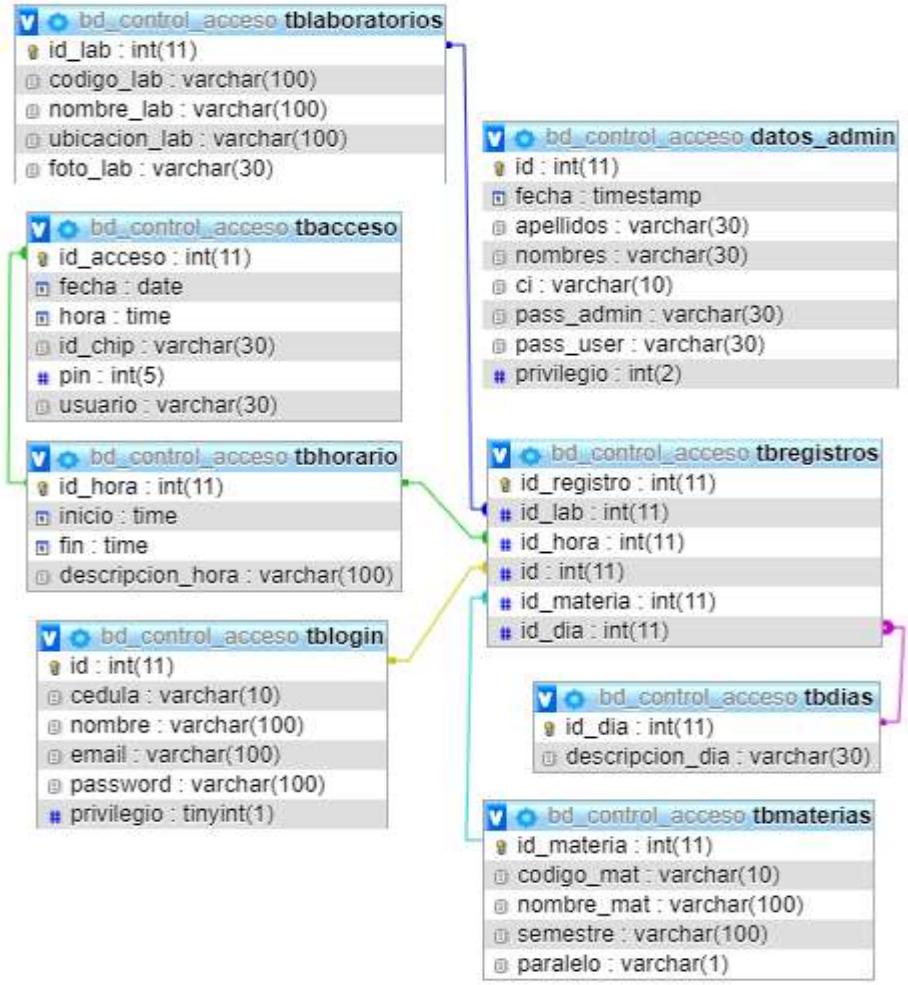


Figura 27-2: Diagrama entidad relación de control de accesos
Realizado por: VÁSQUEZ, Christian 2018

2.4.3 Sublime Text

Es un editor de código multiplataforma utilizado para la creación de scripts en HTML y PHP, siendo utilizado como interprete entre el código fuente a un método gráfico de administración para el sistema de registros. El código observado en la Figura 28-2, trata sobre la relación entre cada una de las tablas y campos mediante su clave primaria en la tabla TBREGISTROS.

```
require 'conexion.php';

$query="SELECT * FROM tbregistros INNER JOIN tblaboratorios ON tbregistros.id_lab=tblaboratorios.id_lab
                                  INNER JOIN tbhorario ON tbregistros.id_hora = tbhorario.id_hora
                                  INNER JOIN tblogin ON tbregistros.id=tblogin.id
                                  INNER JOIN tbmaterias ON tbregistros.id_materia = tbmaterias.id_materia
                                  INNER JOIN tbdias ON tbregistros.id_dia = tbdias.id_dia";


/* Nombre de La Tabla */
```

Figura: 28-2 Código para Script del menú principal con Sublime Text
Realizado por: VÁSQUEZ, Christian 2018

2.4.3.1 Algoritmo para la gestión de la página web

Para la gestión de la base de datos el administrador debe ingresar sus credenciales, si estas son correctas le presenta la página del menú principal del sistema de registros de usuarios y laboratorios. Dentro de la página web puede realizar el escogimiento pertinente para gestionar los Usuarios, Laboratorios Materias y Reservaciones de Laboratorios como se aprecia en el flujograma de el Gráfico 3-2.

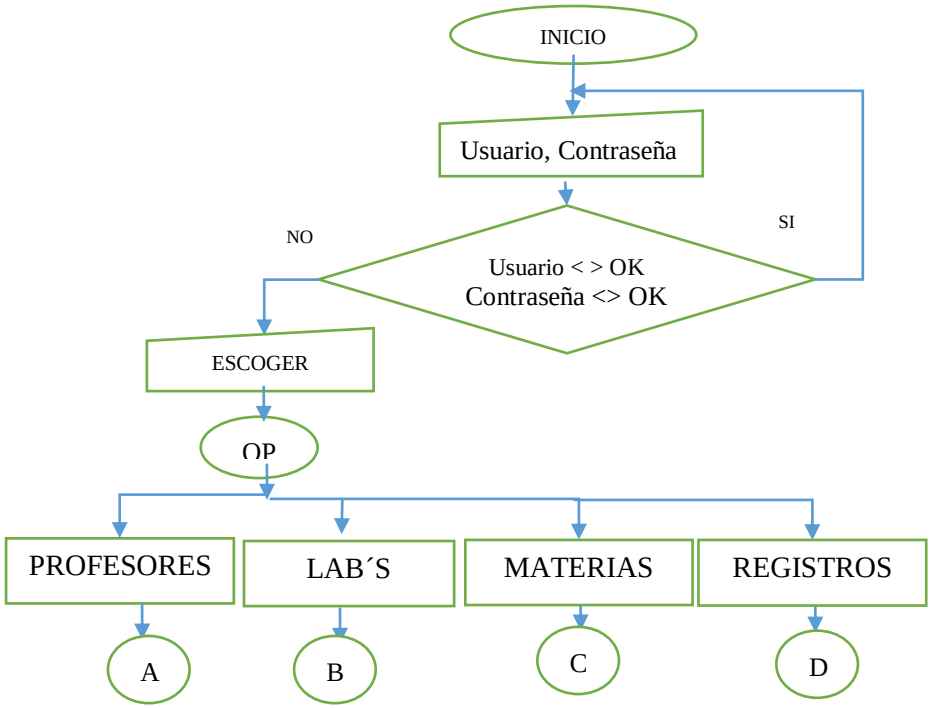


Gráfico 2-3: Flujograma para el menú principal del proyecto
Realizado por: VÁSQUEZ, Christian 2018

El proceso de funcionamiento al escoger cualquiera de las opciones del menú principal se detalla a continuación:

2.4.3.2 Algoritmo para administrar la tabla Profesores

Al seleccionar la opción PROFESORES, el proceso que se realiza está visualizado en el diagrama de flujo del Gráfico 4-2, donde se despliegan las opciones de ingresos, eliminaciones y modificaciones en cada uno de los campos, al dar clic en **Nuevo Usuario** podrá añadir a un usuario (Profesor) completando los campos solicitados, también si presionamos la opción modificar podemos corregir datos que ingresaron mal, o tomar la decisión de eliminarlo permanentemente de la base de datos y como última opción se puede retornar al menú principal.

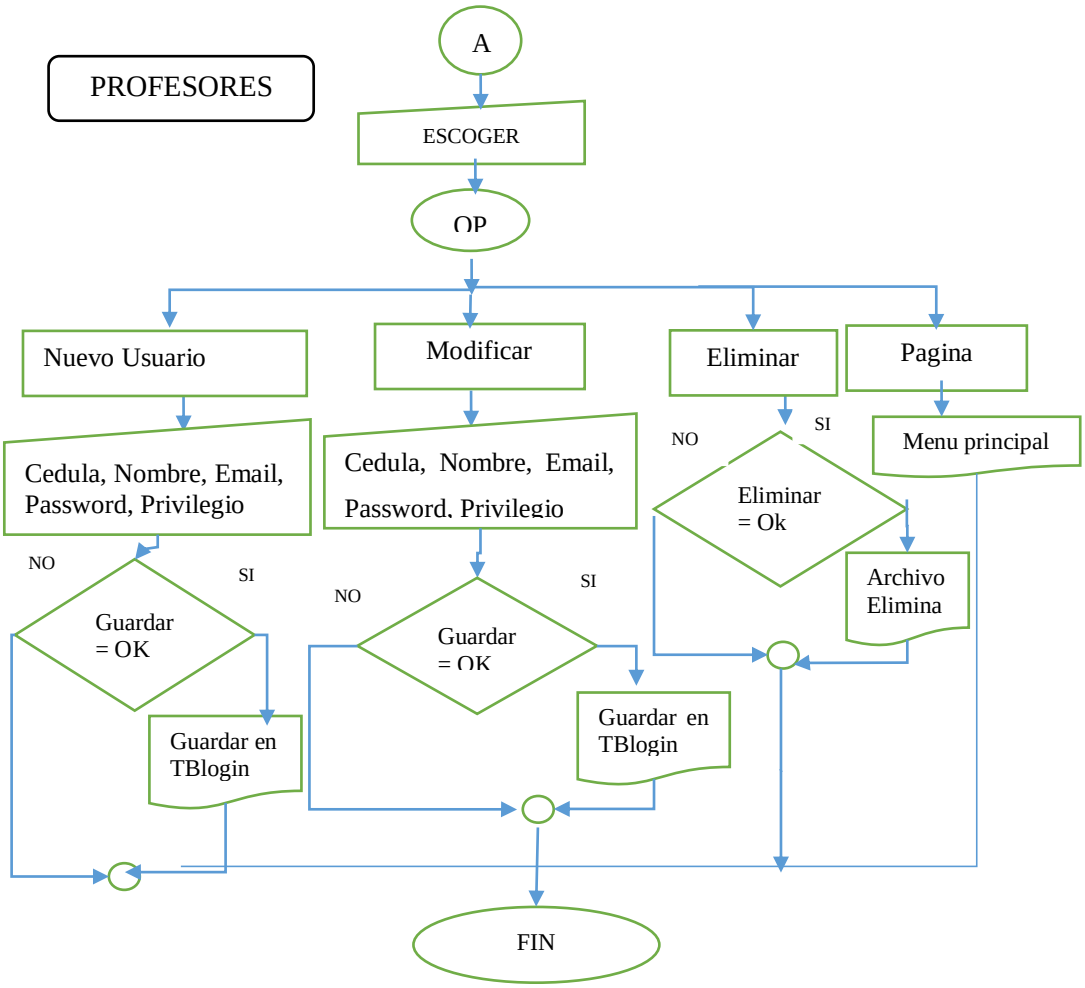


Gráfico 2-4: Diagrama de flujo al escoger la opción de Usuarios
Realizado por: VÁSQUEZ, Christian 2018

2.4.3.3 Algoritmo para administrar la tabla Laboratorios

Cuando se escoge la opción de LAB´S de manera similar que el anterior se despliegan las opciones de: **Nuevo Laboratorio**, **modificar**, **eliminar**, **página principal**, dentro de cada una de ellas se despliegan a otras ventanas, en el caso de Nuevo Laboratorio se abrirá una nueva

ventana con los campos de (Cod_lab, nombre_lab, ubicación_lab), una vez llenos se toma la decisión de guardar si los datos están bien, o regresar a la página anterior. También cuenta con las opciones de eliminar o modificar, como se en el flujograma del Gráfico 5-2.

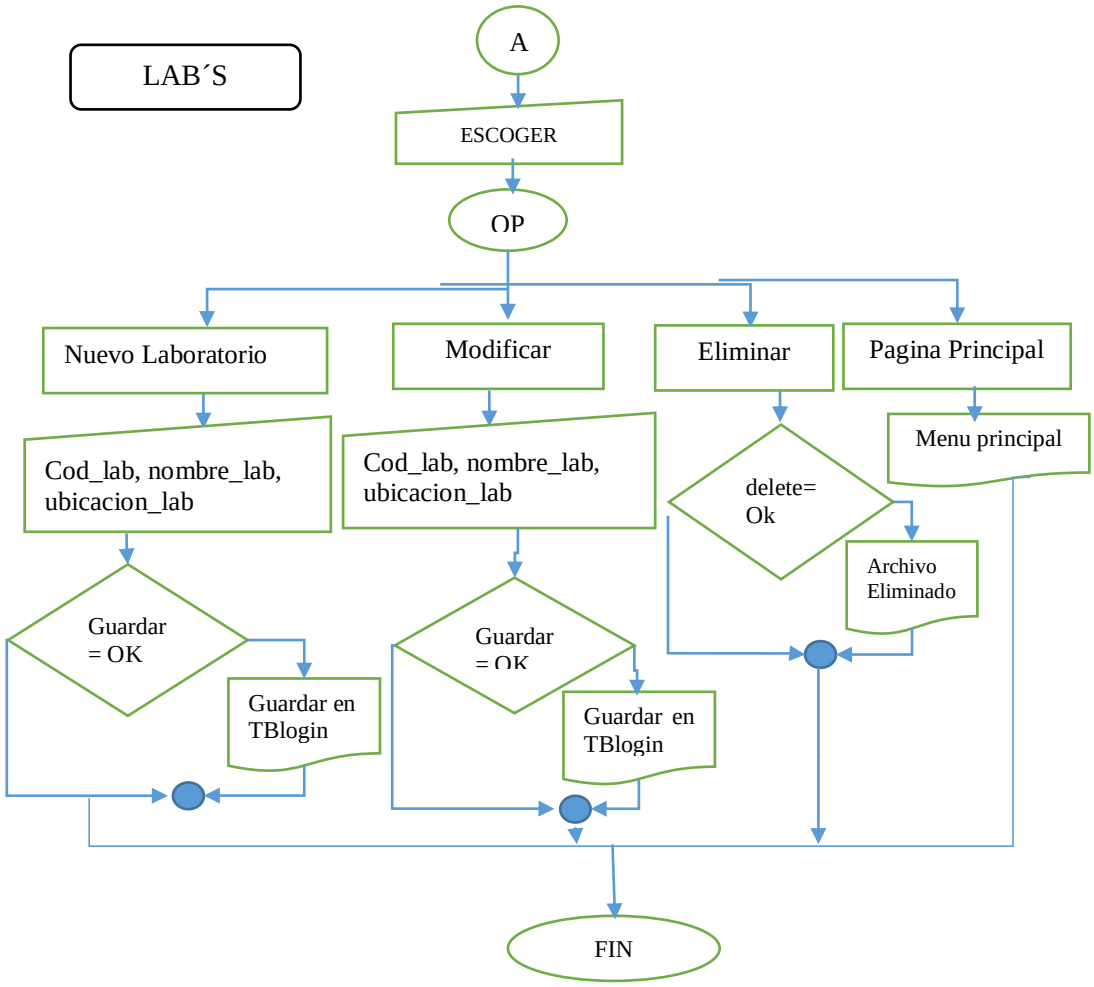


Gráfico 2-5:Diagrama de flujo al escoger la opción de LAB´S
Realizado por: VÁSQUEZ, Christian 2018

2.4.3.4 Algoritmo para administrar la tabla Materias

En la opción Materias ocurre un proceso similar a los descritos en los apartados anteriores, este flujograma puede ser observado en la Figura 6-2, donde se detallan los procesos secuenciales de las opciones tales como: nueva asignatura, modificar, eliminar, página principal, enlazándose a nuevas ventanas

Las cuales realizan cambios en la información, así como solicitudes de confirmaciones, cancelaciones, retornos o simplemente el de guardar o borrar el campo. Mientras que en la opción **Nueva asignatura** se debe completar la información requerida de forma adecuada en cada uno de los campos como son: código, materia, semestre, paralelo.

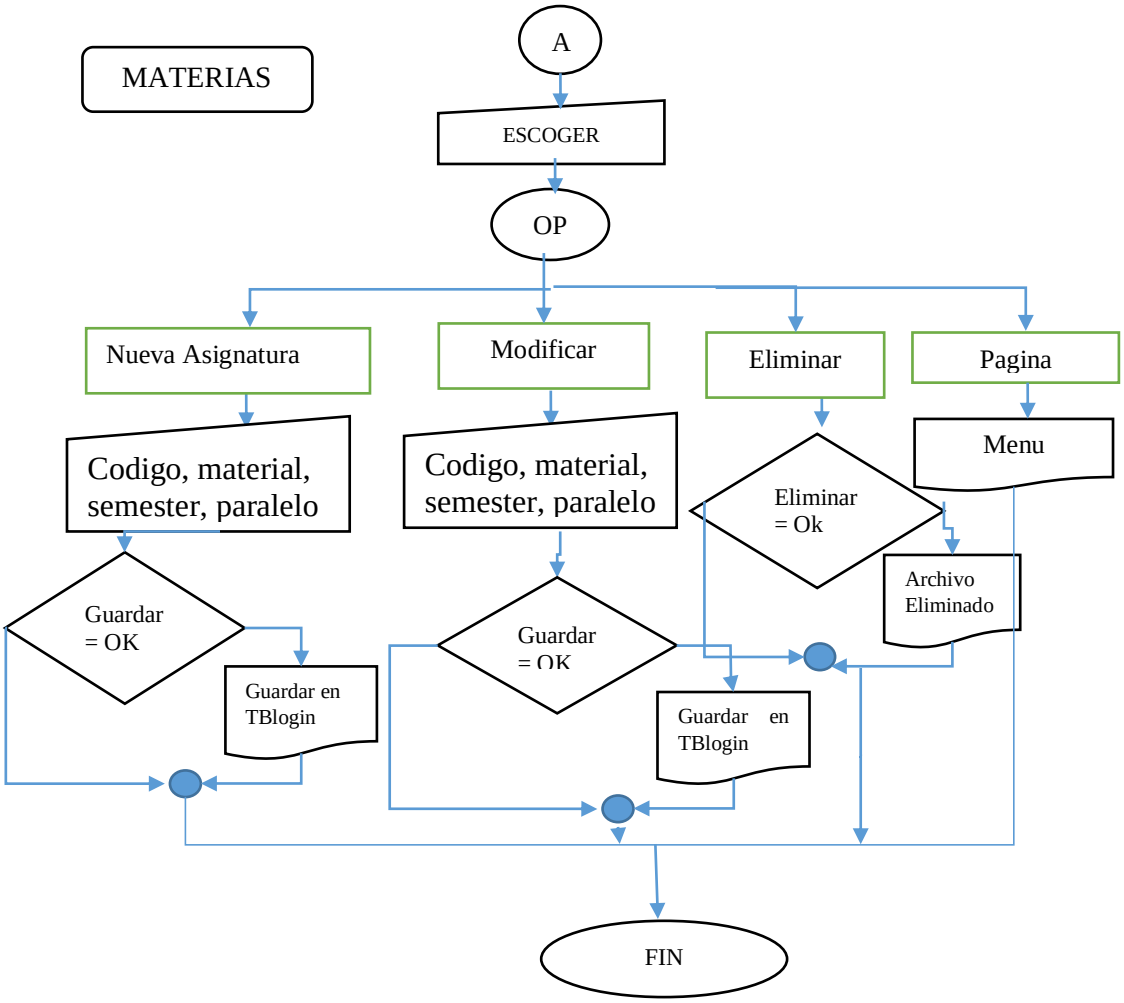


Gráfico 2-6: Diagrama de flujo al escoger la opción de Materias
Realizado por: VÁSQUEZ, Christian 2018

2.4.3.5 Algoritmo para Reservación de Laboratorios

En la opción "RESERVAR LABORATORIO" se puede mencionar que también cuenta con las opciones de gestión de base de datos mencionadas anteriormente como: modificar eliminar he ingresar. Esta opción es una de las partes principales del proyecto porque empiezan a interactuar con todos los registros de la base de datos.

El proceso para el control de acceso a cada uno de los laboratorios comienza en la disponibilidad de los laboratorios en los distintos horarios, dando una prioridad esencial a las tablas **laboratorios** y **horas**. Al momento de presionar el botón "**reservar laboratorio"** se visualiza una pantalla para seleccionar los datos como: Laboratorio, Día, Horario, Maestro, Asignatura, como se aprecia en el Gráfico 7-2, si los datos son correctos y el laboratorio se encuentra libre no mostrara ningún error y se reservara el laboratorio.

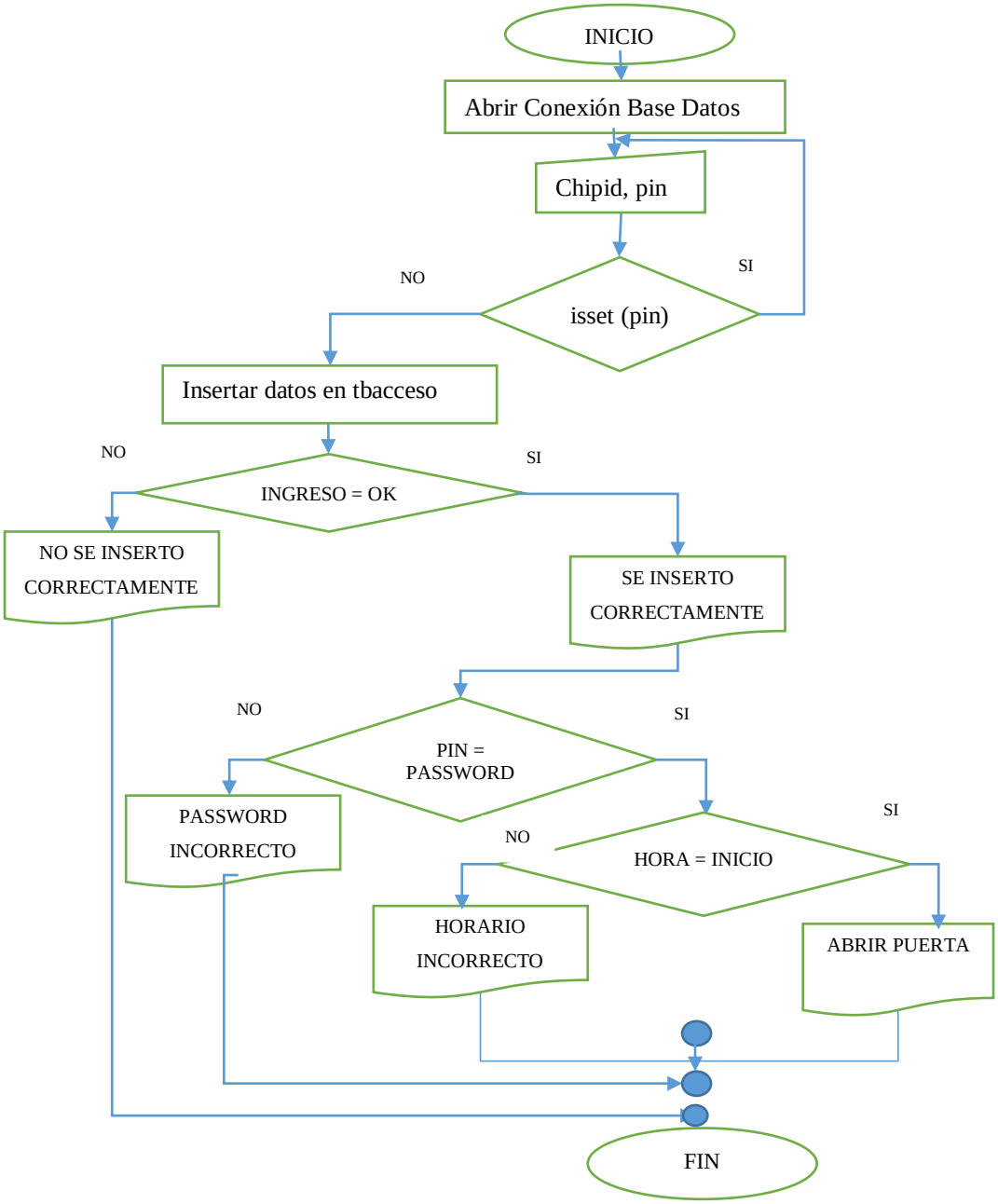


Gráfico 2-7: Recepción de control de password y horario
Realizado por: VÁSQUEZ, Christian 2018

2.4.4 APP INVENTOR

Es una herramienta de software libre basado en una plataforma web, para la creación de aplicaciones móviles con sistema operativo Android, la programación en este lenguaje se realiza mediante bloques basado como piezas en un juego de construcción.

2.4.4.1 Construcción de bloques para el control de acceso

La construcción de bloques inicia con la sincronización del reloj entre la aplicación y el dispositivo, seguido del almacenamiento de datos ingresado por el usuario y el posterior envio de la variable **texts_pass** mediante nfc. El procedimiento a seguir se puede observar en la Figura 29-2.

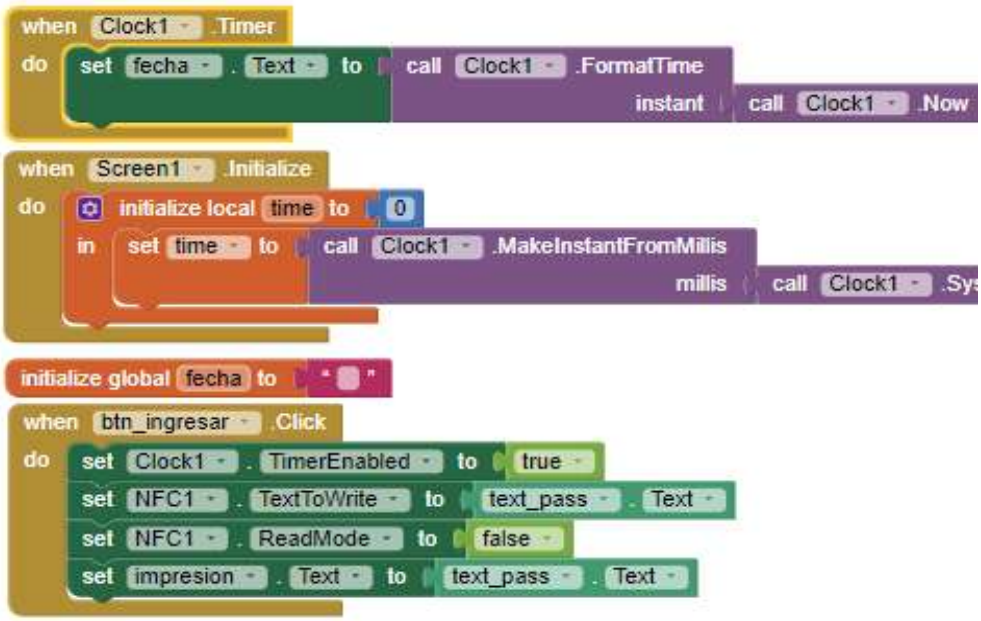


Figura 29-2: Diagrama de flujo del envió de password en la aplicación.
Realizado por: VÁSQUEZ, Christian 2018

El envio de la contraseña mediante tecnología nfc hacia el dispositivo de control de acceso solo permite ingreso de datos numéricos, el ingreso de otros datos tales como alfanuméricos no permite el correcto funcionamiento del distintivo.

2.4.4.2 Construcción de bloques de automatización de eventos físicos

El desarrollo de cada botón se diseñó para controlar el encendido y apagado de la iluminación (4 focos) o 4 dispositivos diferentes que estén conectados a las salidas del relé.

En la Figura 30-2 se puede observar el procedimiento y condiciones para la ejecución de cada uno de los botones en la aplicación, existen 4 botones que están en funcionamiento cada uno con un código único. Para el funcionamiento de los eventos físicos, el usuario debe estar dentro del laboratorio.

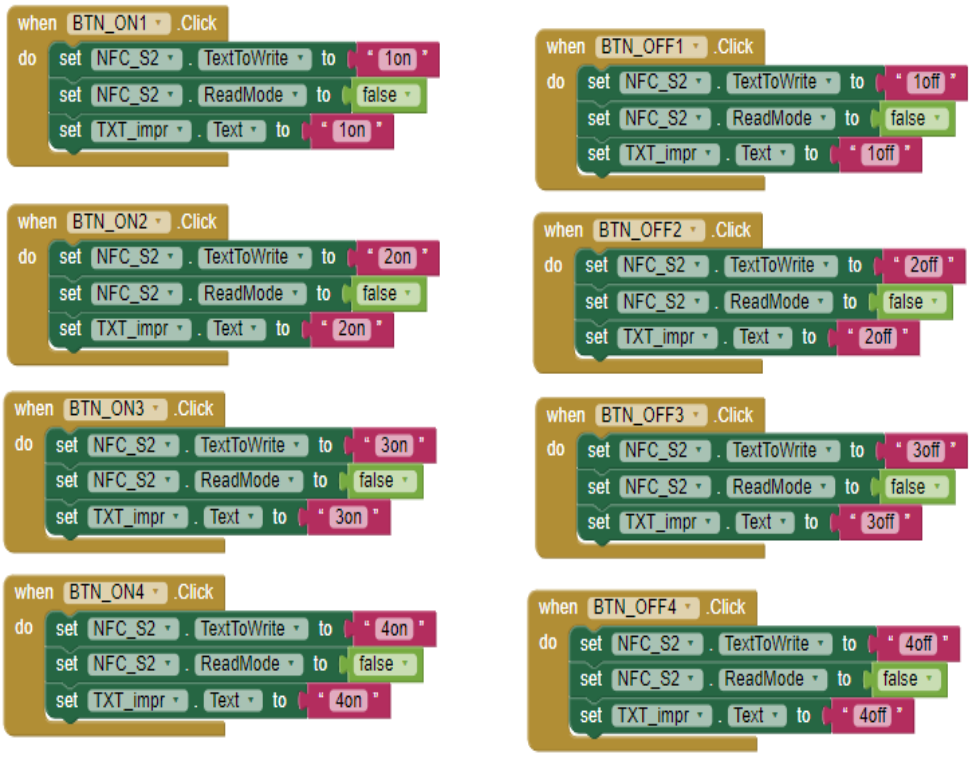


Figura 30-2: Diagrama de flujo del envió de códigos ON/OFF
Realizado por: VÁSQUEZ, Christian 2018

BOTÓN 1

Al seleccionar este botón 1 encendido estamos enviando el código "**on1**" y al seleccionar el botón 1 apagado estamos enviando "**off1".**

BOTÓN 2

Al seleccionar este botón 2 encendido estamos enviando el código "**on2**" y al seleccionar el botón 1 apagado estamos enviando "**off2".**

BOTÓN 3

Al seleccionar este botón 3 encendido estamos enviando el código "**on3**" y al seleccionar el botón 1 apagado estamos enviando "**off3".**

BOTÓN 4

Al seleccionar este botón 4 encendido estamos enviando el código "**on4**" y al seleccionar el botón 1 apagado estamos enviando "**off4".**

CAPITULO III

3 PRUEBAS Y ANÁLISIS DE RESULTADOS DEL SISTEMA

Culminado el proceso de implementación del prototipo se procede a las pruebas de funcionamiento, análisis comparativos y análisis de costos resultantes en los dispositivos desarrollados. A nivel hardware se identificará parámetros de alimentación a los dispositivos, distancia de funcionamiento NFC, tiempo de operación de NFC, también pruebas a nivel de software para comprobar el correcto funcionamiento del registro en la base de datos, la página web y la aplicación móvil.

3.1 Pruebas a nivel de hardware

3.1.1 Carcaza para el dispositivo control de acceso

El dispositivo de control de acceso posee las dimensiones de 14.2 cm de largo x 8.5cm de ancho x 6 cm de alto, como se muestra en la Figura 1-3, en la que vemos una vista 3D de la parte interior y exterior de la caja.

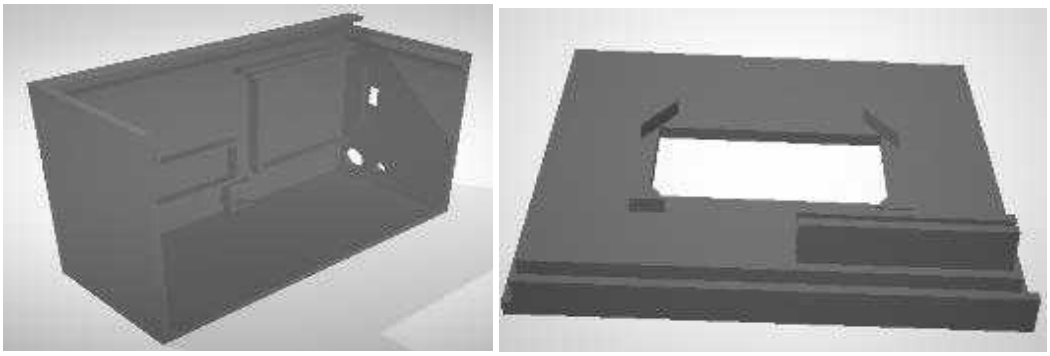


Figura 1-3: Diseño interno y externo de la caja y tapa del control de acceso.
Realizado por: VÁSQUEZ, Christian 2018

3.1.2 Dispositivo de control de acceso

En la Figura 2-3 se pude apreciar la parte interna del sistema de control de acceso, donde cada uno de los elementos electrónicos están correctamente ubicados y sujetados en el interior debido a las llanuras diseñadas previamente en la caja.

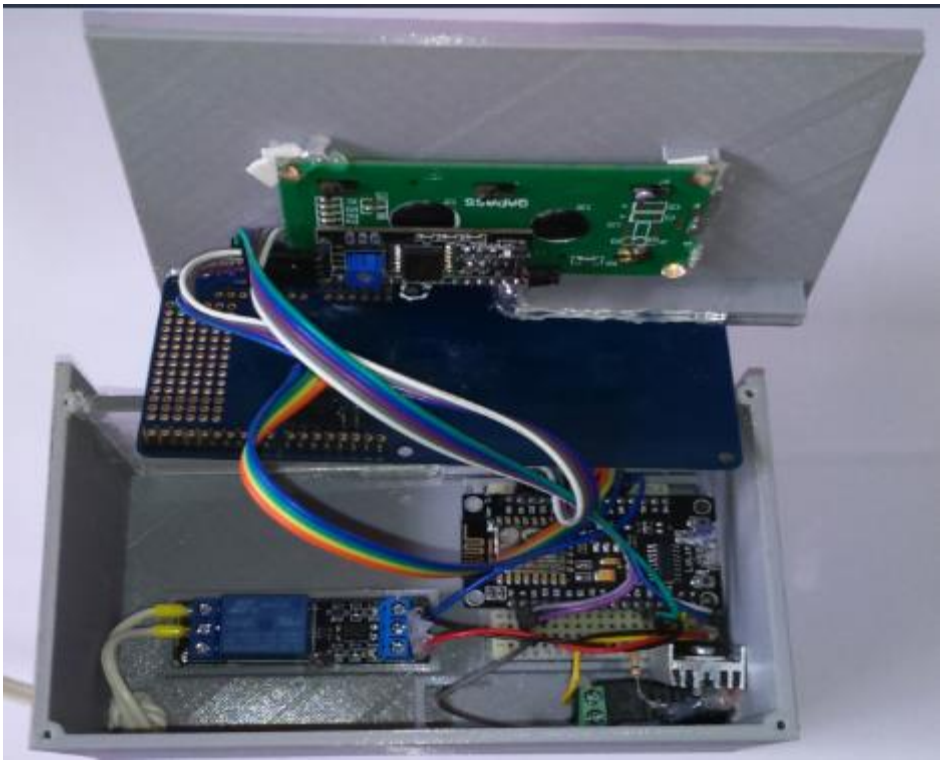


Figura 2-3: Parte interna del dispositivo control de acceso.
Realizado por: VÁSQUEZ, Christian 2018

Mientras que en la Figura 3-3 se observa la parte externa del dispositivo después de realizar las conexiones y ensamblaje de los elementos electrónicos en la caja, con la cobertura de la tapa para brindar la protección necesaria.

Figura 3-3: Parte interna del dispositivo de control de acceso.
Realizado por: VÁSQUEZ, Christian 2018

3.1.3 Dispositivo de Control de Eventos Físicos

El dispositivo de control de eventos físicos tiene una dimensión de 8,2cm de ancho x 10cm de largo y 5.5cm de alto. El mismo se puede apreciar en la Figura 4-3 donde están contenido la parte externa e interna del dispositivo de control de eventos.

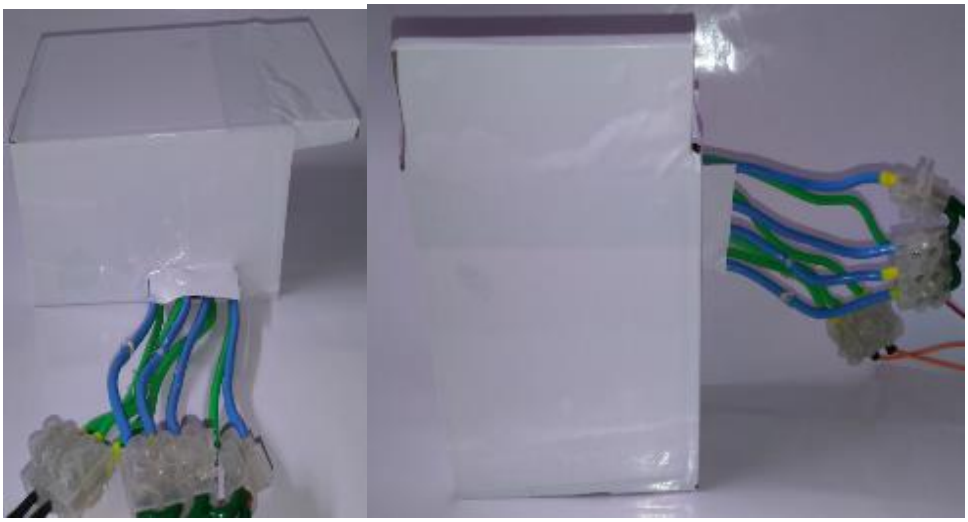


Figura 4-3: Diseño interno y externo de la caja de control de eventos físicos.
Realizado por: VÁSQUEZ**,** Christian 2018

3.1.4 Rango de operación de NFC en los dispositivos controladores

Mediante las mediciones de distancias tomadas en la Tabla 1-3 se concluyó que los lectores NFC de los dispositivos de control de acceso y automatización de eventos, entra en funcionamiento en un rango de distancia menor o igual a 1 centímetro estableciendo la trasferencia de datos de 424kbit/s, mientras que en distancias mayores a 1 cm los dispositivos no pueden entrar en funcionamiento.

Tabla 1-3: Rango de operación de la tecnología NFC

RANGO DE OPERACIÓN NFC	CONTROL DE ACCESO	CONTROL DE EVENTOS FÍSICOS
0 cm	Existe transferencia de datos	Existe transferencia de datos
1 cm	Recepción de señales electromagnéticas	Recepción de señales electromagnéticas
2 cm	Capta señales electromagnéticas mínimas de NFC	Capta señales electromagnéticas mínimas de NFC
3 cm	No capta señales	No capta señales

Realizado por: VÁSQUEZ, Christian, 2018

Para que pueda existir un nivel alto de comunicación nfc entre el Smartphone y Shield PN532 deben estar en una distancia entre 0 a 1 centímetro, caso contrario la comunicación será regular y a mayor distancia seria nula como se aprecia en la Figura 5-3.

Figura 5-3: Rangos de funcionamiento NFC.
Realizado por: VÁSQUEZ, Christian 2018

El sistema de comunicación completa la trasferencia de datos solo cuando el Smartphone entra en contacto con la superficie del dispositivo y una vez que se comunican estos, se debe retirar.

3.2 Pruebas del software del prototipo

3.2.1 Aplicación móvil

La aplicación fue realizada en **MIT App Inventor,** cuenta con una interfaz gráfica amigable que se puede apreciarse en la Figura 6-3, la primera pantalla nos solicita la contraseña que sebe ser enviada presionando el botón INGRESAR, acercarlo al dispositivo de control de acceso y retirarlo.

La contraseña enviada es almacenada en la tabla TBACCESOS junto con la fecha, la hora, el id chip, pin usuario. Para el funcionamiento de la aplicación se debe activar NFC en cada uno de los dispositivos.

Figura 6-3: Primera ventana de la aplicación
Realizado por: VÁSQUEZ, Christian, 2018

3.2.2 Página web

El ingreso a la página web se realiza colocando http://localhost/public_html/index.php, donde se solicita las credenciales del administrador, como se aprecia en la Figura 7-3.

Figura 7-3: Ingreso de credenciales para el Sistema de control de acceso y registro de usuarios para la FIE-ESPOCH
Realizado por: VÁSQUEZ, Christian, 2018

Si las credenciales son correctas se visualizará la imagen de la Figura 8-3 donde el administrador puede gestionar los diferentes formularios.

Figura 8-3: Pantalla Principal del Sistema de registro de usuarios y laboratorios
Realizado por: VÁSQUEZ, Christian, 2018

Las pruebas de funcionamiento de cada uno de los formularios se muestran a continuación al presionar GESTIONAR.

3.2.2.1 Profesores

Al seleccionar la opción PROFESORES, el proceso que se realiza está visualizado en la Figura 9-3, donde se despliegan las opciones de ingresos, eliminaciones y modificaciones en cada uno de los campos,

Figura 9-3: Pagina de administración de usuarios
Realizado por: VÁSQUEZ, Christian, 2018

Al dar clic en **Nuevo Usuario** podrá añadir a un usuario (Profesor) completando los campos solicitados como se observa en la Figura 10-3

Figura 10-3: Ingreso de un usuario nuevo
Realizado por: VÁSQUEZ, Christian, 2018

3.2.2.2 Laboratorios

Cuando se escoge la opción de LAB´S de manera similar que el anterior se despliegan las opciones de: **Nuevo Laboratorio**, **modificar**, **eliminar**, **página principal**, como se observa en la Figura 11-3 en cada opción se despliegan otras ventanas como modificar y eliminar.

Figura 11-3: Pagina de administración de Laboratorios
Realizado por: VÁSQUEZ, Christian, 2018

Al presionar Nuevo Laboratorio se abrirá una nueva ventana con los campos de (Cod_lab, nombre_lab, ubicación_lab), una vez llenos se toma la decisión de guardar si los datos están bien, o regresar a la página anterior. Esta ventana se muestra en la Figura 12-3.

Figura 12-3: Ingreso de un laboratorio nuevo
Realizado por: VÁSQUEZ, Christian, 2018

3.2.2.3 Materias

En la opción Materias se detallan cada una de las materias ingresadas y también cuenta con opciones tales como: nueva asignatura, modificar, eliminar, página principal, enlazándose a nuevas ventanas como se aprecia en la Figura 13-3

Figura 13-3: Pagina de administración de Asignaturas
Realizado por: VÁSQUEZ, Christian, 2018

En la opción **Nueva asignatura** se debe completar la información requerida de forma adecuada en cada uno de los campos como son: código, materia, semestre, paralelo como se ve en la Figura 14-3.

Figura 14-3: Ingreso de una nueva asignatura
Realizado por: VÁSQUEZ, Christian, 2018

3.2.2.4 Reservación de Laboratorios

El proceso para el control de acceso a cada uno de los laboratorios comienza en la disponibilidad de los laboratorios en los distintos horarios, dando una prioridad esencial a las tablas **laboratorios** y **horas**. Todos los datos ingresados se pueden visualizar en la Figura 15-3.

Figura 15-3: Registro de reservación de laboratorios
Realizado por: VÁSQUEZ, Christian, 2018

Al momento de presionar el botón "**reservar laboratorio"** se visualiza una pantalla para seleccionar los datos como: Laboratorio, Día, Horario, Maestro, Asignatura, como se aprecia en la Figura 16-3, si los datos son correctos y el laboratorio se encuentra libre no mostrara ningún error y se reservara el laboratorio.

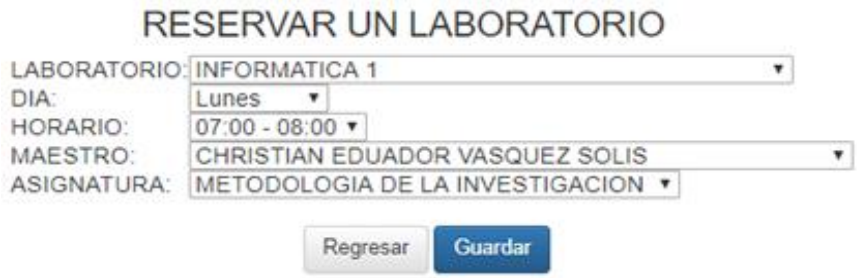


Figura 16-3: Nueva reservación de laboratorios
Realizado por: VÁSQUEZ, Christian, 2018

3.2.3 Funcionamiento del dispositivo

Todas las partes que conforman el prototipo implementado junto con del sistema de registros de laboratorios y usuarios, se puede apreciar en la Figura 17-3. Se realizó las pruebas necesarias y se comprobó el adecuado funcionamiento del prototipo, cumpliendo con requerimientos establecidos en la implementación.

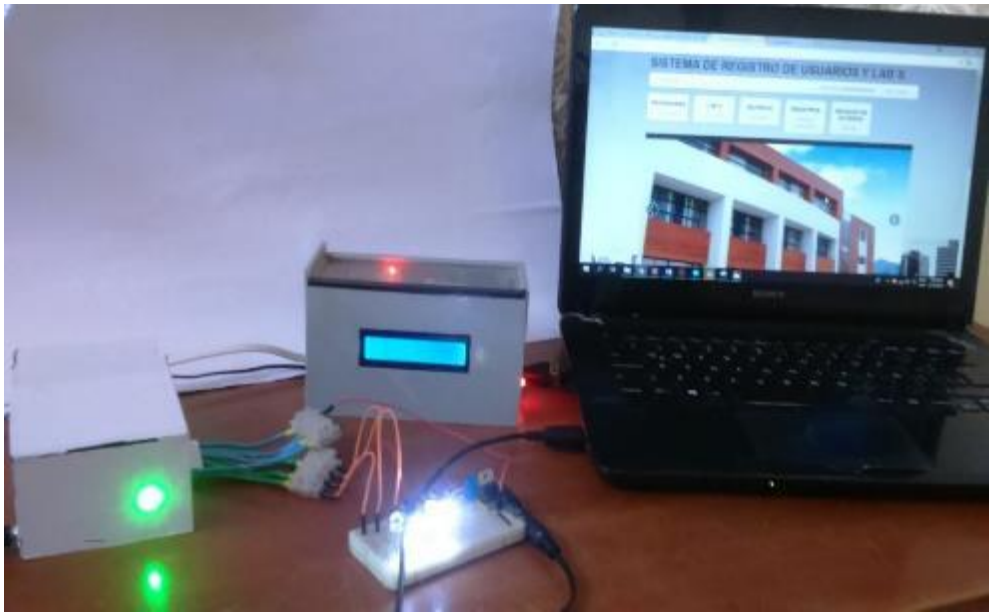


Figura 17-3: Partes del Prototipo Implementado
Realizado por: VÁSQUEZ, Christian, 2018

3.3 Tiempos de respuesta

Para realizar el análisis de funcionamiento determinamos el tamaño de la muestra mediante la fórmula de poblaciones infinitas.

$$n = \left(\frac{Z * S}{e}\right)^2$$

Donde se asumió datos estadísticos como:

$Nivel\ de\ significancia \rightarrow \propto = 0{,}05$
$Nivel\ de\ confianza \rightarrow Z = 95\% \rightarrow 1.96$
$Varianza \rightarrow S$
$Error \rightarrow e = 0{,}05$

Muestra piloto de 10 datos

Tabla 2-3: Parámetros de nivel de confianza

NIVEL DE CONFIANZA	Z alfa
99.70%	3
99%	2.58
98%	2.33
96%	2.05
95%	1.96
90%	1.645
80%	1.28
50%	0.674

Realizado por: VÁSQUEZ, Christian, 2018

Mediante el software R COMMANDER se pudo determinar el tamaño de la muestra aplicando la varianza de los 10 datos de la muestra piloto, el nivel de confianza al 95%, y un error del 0,05, donde se obtuvo un resultado de: 45 y 47 que se puede observar en la Figura 18-3. De los valores obtenidos se debe tomar el valor máximo como el tamaño de la muestra para los campos, pero para este caso se redondeará a una muestra de 50, ya que mientras más datos mejor.

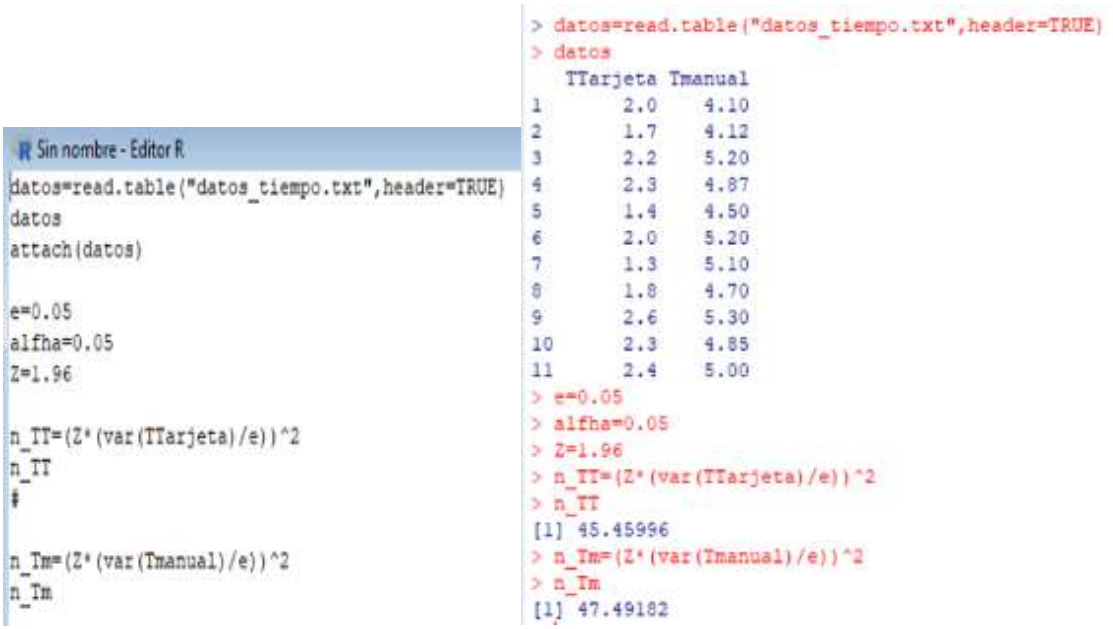


Figura 18-3: Datos de la muestra piloto
Realizado por: VÁSQUEZ, Christian, 2018

Tiempos de respuesta de NFC (ESP 8266 NODE MCU con el Smartphone)

Para el análisis de tiempos de respuestas entre el Smartphone y el ESP8266 NODE MCU, se tomo una muestra de 50 datos de los dispositivos (control de acceso y automatización de eventos), donde se obtuvo datos que se aprecia en la Tabla 3-3, dando como resultado un tiempo de respuesta promedio de1.19 a 1.46 segundos para la trasferencia de datos mediante la tecnología NFC.

Tabla 3-3: Tiempos de respuesta en los dispositivos nfc

NFC Control de acceso	NFC Control de eventos
1.58 sg	0.84 sg
1.88 sg	1.00 sg
0.94 sg	1.32 sg
1.18 sg	0.83 sg
1.76 sg	0.91 sg
1.09 sg	1.23 sg
1.90 sg	1.12 sg
1.78 sg	1.43 sg
1.83 sg	1.47 sg
0.99 sg	1.12 sg
1.40 sg	1.20 sg
1.39 sg	1.21 sg
1.82 sg	0.87 sg
1.55 sg	1.09 sg
1.70 sg	1.22 sg
1.86 sg	1.02 sg
1.15 sg	0.86 sg
1.40 sg	0.98 sg
1.55 sg	1.45 sg
1.04 sg	1.46 sg
1.04 sg	1.47 sg
1.70 sg	1.17 sg
1.77 sg	1.40 sg
1.32 sg	1.08 sg
1.46 sg	1.38 sg
1.83 sg	1.41 sg
1.44 sg	0.87 sg
1.22 sg	1.46 sg
1.03 sg	1.08 sg
1.73 sg	1.13 sg
0.98 sg	1.03 sg
1.88 sg	1.25 sg
1.50 sg	1.45 sg
1.58 sg	1.44 sg
1.51 sg	1.40 sg
1.55 sg	1.18 sg
1.82 sg	1.02 sg
1.36 sg	1.17 sg
1.02 sg	1.42 sg
1.32 sg	1.10 sg
1.28 sg	0.97 sg
1.11 sg	0.94 sg
1.35 sg	1.18 sg
1.50 sg	1.04 sg
1.64 sg	1.43 sg
1.26 sg	1.29 sg
1.88 sg	1.47 sg
1.34 sg	1.50 sg
1.14 sg	0.90sg
1.81 sg	1.18 sg
1.46 sg	**1.19 sg**

Promedio

Realizado por: VÁSQUEZ, Christian, 2018

Para el grupo de datos correspondiente al Control de Acceso se obtuvo una media poblacional de 1.46 segundos, mientras que para la automatización de eventos físicos la media poblacional fue de 1.19 segundos.

Con estos los valores obtenidos de las medias poblacionales se puede evidenciar que el dispositivo de control de acceso permite una transmisión de datos NFC más rápida que el dispositivo de automatización de eventos, debido a que no realiza condiciones en el script del php.

3.4 Análisis de pruebas de funcionamiento del sistema

3.4.1 Tiempos de respuesta del sistema de control de acceso registro y automatización

Para el análisis de tiempos de respuesta de todo el sistema se obtuvieron los datos que se muestran en la Tabla 4-3, donde se realizaron 50 pruebas con cada uno de los dispositivos, obteniendo 50 mediciones de tiempos en segundos.

Con estos datos se llegó a determinar como resultado final, que cada uno de los dispositivos entran en funcionamiento en un rango de tiempo de 1.2 a 3 segundos desde que se ingresa la contraseña en el Smartphone

Tabla 4-3: Tiempos de respuesta del sistema

# Prueba	Control de acceso	Automatización de eventos
1	3	1.2
2	2.4	2.0
3	2.7	2.1
4	2	2.0
5	2.6	1.8
6	1.8	0
7	2	2.1
8	1.3	2.0
9	1.2	1.4
10	2	2.8
11	1.5	1.0
12	2	1.7
13	0	2.2
14	1.4	1.4
15	2	2.2
16	1.3	1.4
17	2	2.0
18	2.3	1.3
19	2.2	2.3
20	1.6	1.8
21	1.4	2.1
22	1.4	1.8
23	1.9	0
24	1.6	2.5
25	2	2.4
26	2.1	0
27	1.7	2.0
28	1.4	2.1
29	2	0
30	1.3	2.0
31	1.4	1.4
32	2	1.4
33	1.3	2.5
34	1.8	2.1
35	2.6	2.5
36	2.3	1.5
37	2.7	1.8
38	1.6	2.6
39	2	2.0
40	2.1	2.0
41	1.6	1.6
42	2	2.4
43	2.1	1.8
44	1.5	1.3
45	1.8	2.1
46	2.6	2.1
47	2.1	2.5
48	1.8	1.5
49	2.6	1.8
50	2.3	2.6
Promedio	1.95 sg	1.81 sg

Realizado por: VÁSQUEZ, Christian, 2018

También en la Tabla 4-3 se pueden identificar los promedios de tiempos para los dispositivos, donde:

El tiempo en que se demoran en el envio y recepción de información desde el Smartphone hacia la base de datos y de la base de datos hasta el relé. Esto para el dispositivo de control de acceso, obteniendo un tiempo de 1,95 segundos para su funcionamiento.

Mientras que, para la conexión a la base de datos y el envio de información para el caso del dispositivo de automatización de eventos físicos, tarda un tiempo de 1.81 segundos en promedio.

Llegando a la conclusión que el dispositivo de automatización de eventos físicos se demora menos segundos en la transferencia de datos que el dispositivo de control de acceso, esto es debido a que no realiza envio y recepción de datos.

3.4.2 Análisis de pruebas exitosas y fallidas del sistema de control de acceso registro y automatización

3.4.2.1 Pruebas de funcionamiento en el dispositivo de control de acceso

En la muestra realizada con el dispositivo de control de acceso se tuvo 1 intento fallido, donde no se registró la contraseña ingresada, mientras que los otros intentos fueron correctos, este dato nos muestra un porcentaje de éxitos del 98% y un porcentaje de error del 2 %, como se muestra en el Figura 19-3.

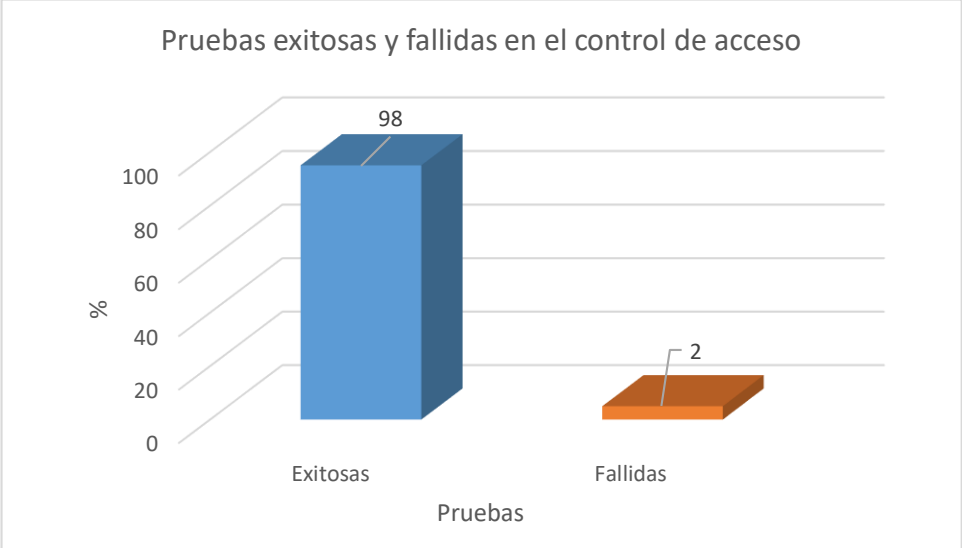


Gráfico 3-1: Porcentaje de éxito y error en el dispositivo de control de acceso
Realizado por: VÁSQUEZ, Christian, 2018

3.4.2.2 Pruebas de funcionamiento en el dispositivo de automatización de eventos físicos

En el dispositivo de automatización de eventos físicos se tuvo 3 datos erróneos, mientras que el resto de pruebas fueron correctas, los porcentajes se pueden observar en el Figura 20-3, donde se obtuvo un 95% de éxito.

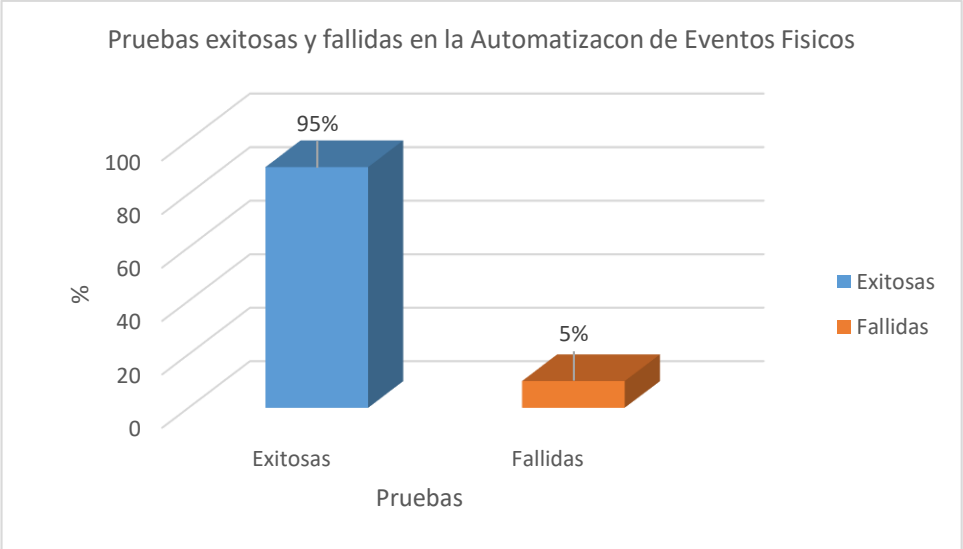


Gráfico 3-2:Porcentaje de éxito y error en el dispositivo de control de eventos
Realizado por: VÁSQUEZ, Christian, 2018

3.5 Pruebas de acceso por el método tradicional (con llaves)

Según las pruebas realizada con el método tradicional (con llaves) una persona tarda entre 3 a 8 segundos en la apertura de una puerta, los datos están ubicados en la Tabla 5-3 donde también se obtienen un promedio de 5 segundos en el acceso a un recinto.

Tabla 5-3: Tiempos de respuesta con el método tradicional

# Prueba	Control de acceso manual
1	5.1
2	4.44
3	5
4	4.64
5	4.59
6	5.25
7	4.36
8	4.39
9	5.18
10	5.35
11	4.18
12	4.14
13	4.36
14	5.29
15	4.4
16	4.21
17	4.9
18	5.5
19	5.46
20	4.67
21	5.31
22	5.17
23	5.3
24	5.32
25	5.17
26	5.22
27	4.82
28	4.52
29	4.1
30	4.71
31	5.25
32	5.18
33	4.72
34	4.46
35	4.43
36	4.13
37	4.63
38	5.49
39	4.18
40	4.11
41	5.33
42	5.21
43	4.34
44	5.36
45	4.61
46	5.36
47	5.05
48	5.15
49	5
50	4.4

Realizado por: VÁSQUEZ, Christian, 2018

Para el análisis de las muestras obtenidas se aplicará la Normalidad con el diseño de diferencias para muestras pareadas, ya que se realizó el mismo experimento al mismo ente pareado (la misma puerta). Los tiempos que se estudia en la normalidad son los datos de la tarjeta, así como la forma manual.

Para determinar si los datos estadísticos se distribuyen de normalmente se utilizó el método estadístico del Test de Shapiro–Wilk que es ideal para contrastar la normalidad de un conjunto de datos mayores a 30 provenientes de una población normalmente distribuida. Como podemos ver en la figura 19-3, los valores obtenidos denominados **P-Valores** son menores a 0,05 lo cual nos indica que los valores se distribuyen normalmente.

```
> attach(muestra_pareada)
> shapiro.test(X3.0)

        Shapiro-Wilk normality test

data:  X3.0
W = 0.92383, p-value = 0.003635

> shapiro.test(X5.10)

        Shapiro-Wilk normality test

data:  X5.10
W = 0.91086, p-value = 0.001268
```

Figura 19-3: Valores de normalidad por el método de Shapiro Wilk
Realizado por: VÁSQUEZ, Christian, 2018

En la figura 20-3 se puede apreciar la aplicación de un test de varianza, donde elegimos el contraste de hipótesis para igualar las medias de 2 muestras pareadas y normales, realizada con el estadístico T-student. Donde el **P-valor** del test de varianza es mayor a 0.05, por lo que no existe diferencia significativa en varianza.

```
> t.test( X3.0,X5.10, paired = TRUE, alternative = "less", var.equal=TRUE)

        Paired t-test

data:  X3.0 and X5.10
t = -30.628, df = 48, p-value < 2.2e-16
alternative hypothesis: true difference in means is less than 0
95 percent confidence interval:
      -Inf -2.797909
sample estimates:
mean of the differences
                  -2.96
```

Figura 20-3: Prueba de hipótesis
Realizado por: VÁSQUEZ, Christian, 2018

Por lo que se concluye que la media de los tiempos de la apertura de la puerta de forma manual es mayor que, la media de los tiempos de la apertura por medio de la tarjeta con un nivel de confianza del 95%, donde se puede identificar que, con el dispositivo de control de acceso implementado, realiza un acceso rápido al recinto, y un registro del usuario al momento de enviar la contraseña.

3.5.1 Análisis de Costos

En la Tabla 6-3 se puede apreciar cada uno de los elementos del hardware con sus respectivos costos que se utilizó para la construcción del prototipo, dando un costo total de $ 139.94 dólares americanos.

Tabla 6-3: Costos de materiales

CANTIDAD	DESCRIPCION	UNIDAD	TOTAL
2	Esp8266 nodemcu	$11.00	$22.00
2	Adafruit PN532	$35.00	$70.00
12	Terminales eléctricos amarillos	$0.02	$0.24
2	Cables de conexión	$2.00	$4.00
2	reguladores lm7805	$0.70	$1.40
2	disipadores	$0.50	$1.00
3	metros de cable Numero 15	$0.70	$2.10
2	diodos (verde y rojo)	$0.10	$0.20
1	relé relay 5V 1 canal	$2.00	$2.00
1	módulo de relé 5V 4 canal	$8.00	$8.00
1	Lcd 16 x 2 con i2c	$9.00	$9.00
1	caja negra	$4.00	$4.00
1	caja diseñada	$15.00	$15.00
2	Conectores Hembras DC para arduino	$0.50	$1.00
	total	$88.52	$139.94

Realizado por: VÁSQUEZ, Christian, 2018

El precio del prototipo implementado sigue siendo de muy bajo costo en comparación a sistemas similares como **CONTROL ACCESO RFID USA TAG HC-05 DHT11 L298 RC522 YL-69,** que se puede apreciar en la Figura 21-3

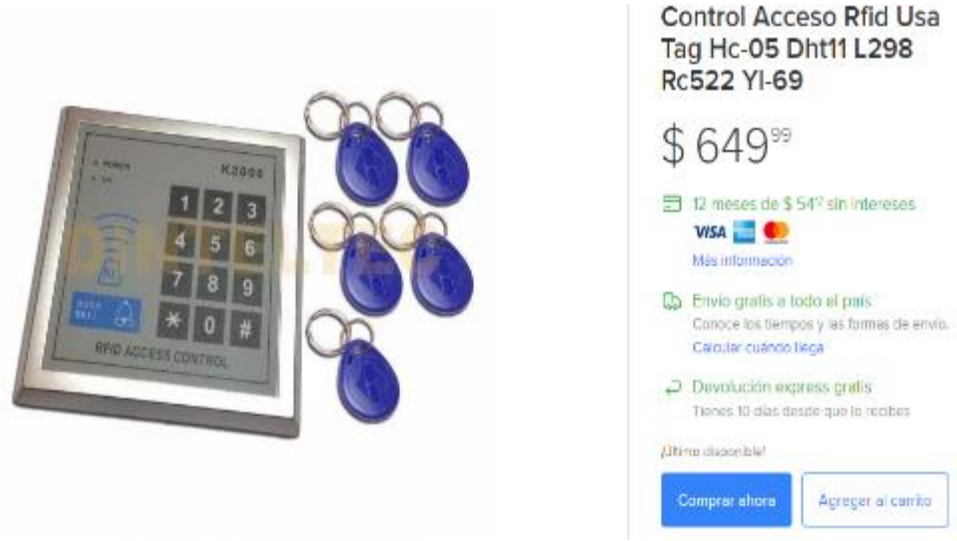


Figura 21-3: Sistema de control de acceso RFID Usa Tag Hc-05 Dht11 L298
Fuente: https://articulo.mercadolibre.com.mx/MLM-565234439-control-acceso-rfid-usa-tag-hc-05-dht11-l298-rc522-yl-69-_JM.

En la tabla 7-3 de puede observar las características de cada dispositivo, donde se tiene algunas mejoras en precio, consumo de energía y número de usuarios.

Tabla 7-3: Comparación entre el prototipo implementado Sistema de control de acceso RFID Usa Tag Hc-05 Dht11 L298

DISPOSITIVOS / CARACTERÍSTICAS	Prototipo Implementado	Control Acceso RFID K2000
Precio	$139.94	$649.99
Número de usuarios	ilimitados	250
Voltaje de funcionamiento	5	12
Sensibilidad	1 cm de distancia	5 cm de distancia
Fácil de usar	si	si
Tipo de tags	activos	pasivos
Salidas relevador NA-C-NC	1 modificable a 3	1

Realizado por: VÁSQUEZ, Christian, 2018

CONCLUSIONES

- Se implementó un prototipo, cuya operatividad se basa en 3 nodos denominados control de acceso, automatización de eventos físicos y registro, que trabaja con una aplicación móvil con tecnología NFC, ligado una base de datos local, que en conjunto permite el acceso a recintos, también el encendido y apagado de equipos.

- Con el estudio de la tecnología NFC se concluyó que el modo activo NFC es la tecnología inalámbrica con mayor seguridad para la trasferencia de datos, debido a su corto alcance.

- Los dispositivos más utilizados son los Smartphone, que posee tecnología NFC, BLUETOOTH y WIFI permitiendo una interconectividad una amplia gama de dispositivos (ESP NODE MCU) mediante aplicaciones y base de datos.

- Se diseñó una aplicación para el ingreso de códigos de acceso y control de dispositivos o equipos dentro del recinto, gestionando de encendido y apagado.

- Se construyó los dispositivos de control de acceso y control de eventos físicos con elementos electrónicos modernos (Shield Adafruit PN532 NFC, ESP8266 NODE MCU) con gran sensibilidad y múltiples usos, bajo una interfaz de programación amigable.

- La nueva tarjetas de desarrollo (ESP8266 NODE MCU) permite crear redes de sensores inalámbricos con diversos dispositivos de lectura/escritura mediante comunicaciones I2C y SPI, para enlazarlos a la WEB mediante el estándar IEEE 802.11.

RECOMENDACIONES

1. Se recomienda utilizar la tecnología NFC en futuras investigaciones, así como en la implementación de la domótica y las IoT.

2. Utilizar el dispositivo ESP8266 NODE MCU en el proceso de desarrollo de las IoT, especialmente en el proceso de adquisición y almacenamiento de datos de una red de sensores inalámbricos.

3. Establecer la velocidad de configuración del ESP8266 NODE MCU en 115200 baudios para evitar fallos al cargar el código.

4. Desconectar la alimentación externa del dispositivo de control de acceso al momento de cargar el código en la placa, si se utiliza los métodos de comunicación SPI e I2C en conjunto.

5. Ampliar las funcionalidades del prototipo con la tecnología NFC.

BIBLIOGRAFÍA

ABADÍA, A. *Introducción a las redes WiFi*. Mexico, 2010, p. 28.

BAEZA, J.P. y POMARES, J. *¨Manual de arduino revision. manual de Arduino¨* [en línea], 2009, pp. 1-8. Disponible en: https://rua.ua.es/dspace/bitstream/10045/11833/1/arduino.pdf.

BUENO DELGADO, M.V., PAVÓN MARIÑO, P. y DE GEA GARCIA, A. *¨La tecnología NFC y sus aplicaciones en un entorno universitario¨. Revista de la ETSIT-UPCT*, 2011.

CAMPA RUIZ, A. *Desarrollo de una aplicación de pago a través de la tecnología NFC.* 2011. pp. 42-44.

CÁRDENAS, G. y GÓMEZ, S. "*Diseño e implementación de una Tarjeta de Desarrollo con profundización en desarrollo de aplicación de Touch Sensing"* [en línea]. (tesis). (Pregado). Cancun. Mexico. 2013. pp. 1-10. [Consulta: 30 noviembre 2017]. http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP157.pdf

CAVOUKIAN, A. *Mobile Near Field Communications (NFC) " Tap ' n Go " Keep it Secure & Private. PbD*, 2011. pp. 2.

CHAVARRÍA ANTONIO *¨Tecnología de comunicación de campo cercano (nfc) y sus aplicaciones¨* [en línea] (tesis). (Pregado) Universidad de Costa Rica. San Jose. Costa Rica. 2011. p [Consulta: 20 noviembre 2017]. P. 50 Disponible en: http://eie.ucr.ac.cr/uploads/file/proybach/pb2011/pb2011_012.pdf.

COBOS, M. y ORTIZ, M. *Implementación de un prototipo de una red inalambrica de sensores para la identificación de personas y acceso a historias clínicas basadas en tarjetas de desarrollo.* [En línea] (tesis). (Pregado) ESPOCH. Riobamba. Ecuador. 2017. p. 146 [Consulta: 23 noviembre 2017]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/6869.

COLLIGAN, P. *Raspberry Pi.* [en línea] 2018. [Consulta: 2 mayo 2018]. Disponible en: https://www.raspberrypi.org/blog/.

COSENTINO, L. *Control de Acceso: conceptos, historia y esquema básico. .Datatécnica* [en línea], 2013. pp. 156. [Consulta: 13 diciembre 2017]. Disponible en: http://www.rnds.com.ar/articulos/045/RNDS_152W.pdf.

DIARIO EL COMERCIO, ECUADOR. *Uso de 'smartphones' ganó mercado durante el 2016 | El Comercio. [en línea]. 18 febrero.* 2016. pp. 10. [Consulta: 10 octubre 2017]. Disponible en: http://www.elcomercio.com/actualidad/smartphon-celular-mercado-ventas-crecimiento.html.

DOMÍNGUEZ, H.M. y SÁEZ, F. *Domótica: Un enfoque sociotécnico* [en línea]. 2006. [Consulta: 23 mayo 2018]. Disponible en: https://www.mendeley.com/viewer/?fileId=59311669-e39c-33cf-26a3-a2b28ac1747c&documentId=5da8602d-cc63-391c-a521-a24ca2eade58.

ELECTRONILAB. *NodeMCU – Board de desarrollo con módulo ESP8266 WiFi y Lua - Electronilab.* [en línea] California-USA, 2016, [Consulta: 23 mayo 2018]. Disponible en: https://electronilab.co/tienda/nodemcu-board-de-desarrollo-con-esp8266-wifi-y-lua/.

FALKE, O., RUKZIO, E. y DIETZ, U. *Mobile services for near field communication.* [en línea], *Germany*, 2007, [Consulta: 23 mayo 2018], Disponible en: http://www.mmi.ifi.lmu.de/pubdb/publications/pub/falke2007mobileServicesTR/falke2007mobileServicesTR.pdf.

FERNÁNDEZ, M. *Instalación eléctrica y domótica para una vivienda unifamiliar.* Barcelona-España, 2012, p. 281.

FERNÁNDEZ, R., et. al. Sapiens. *Redes inalámbricas de sensores: teoría y aplicación práctica*. Madrid. España. 2009, pp 40-45.

FUENTES, C. *Redes inalámbricas y Estándares de conexión*. [en línea] Cuenca, 2015, [Consulta: 21 mayo 2018]. Disponible en: http://slideplayer.es/slide/5473520/#.

HERNÁNDEZ BALIBREA, R. *Tecnología domótica para el control de una vivienda .Madrid,* 2012, pp. 16-18.

HERRERA M. *Bandas ISM.* [en línea]. Mexico, 2016, [Consulta: 5 octubre 2017]. Disponible en: https://es.slideshare.net/maoherrera1/bandas-ism.

HUIDOBRO, J.M., et. nb. Sapiens. *La Domótica Como Solución de Futuro* [en línea] 2007. [Consulta: 1 octubre 2017], Disponible en: www.fenercom.com.

IGOE, T., ., et. al. Sapiens. *Beginning NFC : near field communication with Arduino, Android, and PhoneGap*. O'Reilly Media. Washington. 2014. p. 20.

IHS MARKIT. *M2M, IoT y conectividad - Tecnología IHS.* [en línea]. 2016, [Consulta: 2 agosto 2017]. Disponible en: https://technology.ihs.com/Categories/453325/m2m-iot-connectivity.

JIMÉNEZ, R. *Redes de Area Personal o PAN (Personal Area Net- work) Redes de Area Local o LAN (Local Area Network).* [en línea], 1994. pp. 13-37. Disponible en: http://www.bdigital.unal.edu.co/4234/2/299696.2011_pte_2.pdf.

JURADO, A. y SALAZAR, B. *Diseño y construcción de un sistema prototipo para el control de vehículos por medio de dispositivos tag con identificación rfid (radio frecuency identification) para la dirección de control del tránsito y seguridad vial de la policia nacional.* [en línea] (tesis). (Pregado). Escuela Politecnica Nacional. Quito. Ecuador. 2013. p. 176. [Consulta: 10 octubre 2017]. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/5805/1/CD-4707.pdf.

KUSHAGRA. *16 x 2 LCD Datasheet | 16x2 Character LCD Module PINOUT.* [en línea] 2015, [Consulta: 2 junio 2018]. Disponible en: https://www.engineersgarage.com/electronic-components/16x2-lcd-module-datasheet.

LARA, D. y VALLEJO, J. *"Desarrollo de un sistema de comunicación con nfc para el acceso a información académica de los estudiantes de la fie-espoch"*. [en línea] (tesis). (Pregado). ESPOCH. Riobamba. Ecuador. 2016, pp. 54-56. [Consulta: 2 junio 2017]. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/6440/1/98T00129.pdf

MCGRAW-HILL INTERAMERICANA DE ESPAÑA. *Redes de ordenadores*. Madrid: 2018. p. 5.

MEDINA, J. *Ganado bovino mediante la lectura y escritura de etiquetas.* [en línea] (tesis). (Pregado). Francisco José de Caldas. Caldas. Colombia. 2017, [Consulta: 12 mayo 2018], Disponible en: http://repository.udistrital.edu.co/bitstream/11349/6545/1/MedinaDelgadoJavierLeonardo2017.pdf.

MOJICA, S. y GAMBA, C. *Control de acceso con verificación de identidad por medio de código de barras* [en línea] 2010, [Consulta: 12 mayo 2018], Disponible en: https://repository.javeriana.edu.co/bitstream/handle/10554/7043/tesis488.pdf?sequence=1.

MORALES. MICHEL. *Protocolo I2C - Fundamentos de aprendizaje. ¿Cómo funciona? - Clases TBem.* [en línea]. 2016, [Consulta: 2 junio 2018]. Disponible en: http://learn.teslabem.com/fundamentos-del-protocolo-i2c-aprende/2/.

NETWORK, P.A. Redes inalámbricas de area personal (wpan) introducción a las wpan. *redes inalámbricas*. Colorado, 2012 , pp. 31-62.

NFC FORUM. *Nfc data exchange format.* [en línea] 2006, [Consulta: 12 mayo 2018], Disponible en: http://www.lightpath.io/tarjetas-de-desarrollo/.

ORTIZ, S. *Is near-field communication close to success? Computer*, vol. 39, 2006. pp. 18-20.

PEÑA, M. *NFC y sus Principales Usos. Tendencias* [en línea] Mexico, 2012. pp. 60 y 61. Disponible en: http://www.nts-solutions.com/news/47.pdf.

PERALES, M.A., ., et. al. Sapiens. Análisis comparativo de distintas plataformas para la enseñanza de Sistemas Electrónicos Digitales. *TAEE 2016: XII Congreso de Tecnologías Aplicadas a la Enseñanza de la Electrónica: Libro de Actas*, 2016. pp. 26-33.

PORTILLO, GARCÍA., et. al. Sapiens. *Informe de vigilancia tecnológica: tecnologia de identificacion por radiofrecuencia (RFID)* [en línea]. 1 edicion. Madrid: 2008. Disponible en: http://www.tagingenieros.com/sites/default/files/vt13_rfid_0.pdf.

QUISPE, O. *Tarjetas Para Desarrollo De Hardware – Lightpath.* [en línea], 2017 [Consulta: 23 mayo 2018], Disponible en: http://www.lightpath.io/tarjetas-de-desarrollo/.

RF WIRELESS WORLD. *NFC A vs NFC B vs NFC F-Difference between NFC-A,NFC-B,NFC-F* [en línea]. NFC Forum. 2016, [Consulta: 18 enero 2018]. Disponible en: http://www.rfwireless-world.com/Terminology/NFC-A-vs-NFC-B-vs-NFC-F.html.

RIVERA, H., et. al. Sapiens.. *Conmutación y Enrutamiento de Redes de Datos* [en línea]. Madrid: 2016. [Consulta: 20 mayo 2018]. Disponible en: https://es.scribd.com/presentation/349690811/4-Tecnologias-Inalambricas.

RODRIGO, J. *ESP8266 y NodeMCU: la nueva generación de sistemas embebidos* [en línea] *Panama. Hitek.* 2016 [Consulta: 23 mayo 2018]. Disponible en: http://panamahitek.com/esp8266-y-nodemcu-la-nueva-generacion/.

ROHDE&SCHWARZ. *Principios básicos de NFC/RFID | Rohde & Schwarz.* [En línea] 2018 [Consulta: 18 abril 2018]. Disponible en: https://www.rohde-schwarz.com/es/tecnologias/conectividad-inalambrica/rfid-nfc/tecnologia-rfid-nfc/tecnologia-rfid-nfc_55704.html.

RUILOBA, J. y QUITO, K. *"Prototipo de telecontrol de una red inalámbrica de sensores para seguridad y acciones básicas del hogar, aplicado a personas con discapacidad motriz en extremidades inferiores, basado en tarjetas de desarrollo"*. [En línea (tesis). (Pregado). ESPOCH. Riobamba. Ecuador. *2017, p 25.* [Consulta: 7 abril 2018].

SABELLA, R. *The NFC Data Exchange Format (NDEF) - dummies.* [en línea] 2016, [Consulta: 19 enero 2018], Disponible en: http://www.dummies.com/consumer-electronics/nfc-data-exchange-format-ndef/.

SHOPNFC. *Teléfonos y Tabletas compatibles con las Etiquetas NFC - Shop NFC.* [en línea]. 2017, [Consulta: 9 enero 2018], Disponible en: https://www.shopnfc.it/es/content/7-telefonos-y-tabletas-compatibles-con-etiquetas-nfc.

SONY IMAGING PRODUCTS & SOLUTIONS INC. *Sony Global - FeliCa - About NFC - Relationship between NFC and FeliCa.* [en línea]. 2018, [Consulta: 27 abril 2018]. Disponible en: https://www.sony.net/Products/felica/NFC/forum.html.

TOLOSA BORJA, C.G.B. y ÁLVARO. *Sistemas Biométricos.* vol. 1, Quito, 2010, p. 39.

UNIVERSIDAD DE CÁDI. *Hardware y cable USB Especificaciones técnicas. Universidad de Cádiz* [en línea], 2009. pp. 1-7, [Consulta: 27 abril 2018], Disponible en: http://www.uca.es/recursos/doc/Unidades/Unidad_Innovacion/Innovacion_Docente/ANEXOS_2011_2012/22232441_310201212102.pdf.

VÁSQUEZ, SANTIAGO. *Diseño e implementación de un sistema electrónico para el registro de acceso y envío de información mediante tecnología nfc al personal administrativo y de soporte técnico de la empresa wisp airmaxtelecom soluciones tecnológicas*. (tesis). (Pregado). Universidad Tecnica del Norte. Ibarra. Ecuador. 2016. p. 293 [Consulta: 02 abril 2018], Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/7194/1/04%20RED%20102%20TRABAJO%20GRADO.pdf.

WAHID, H., AHMAD, S., NOR, M.A.M. y RASHID, M.A. *RFID Handbook Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. 3rd ed. London: 2017. WILEY. pp. 17-20.