ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

"PROPUESTA DE UN SISTEMA AUTOMATIZADO PARA CONTROLAR EL ACCESO VEHICULAR EN LA ESPOCH MEDIANTE EL USO DE TECNOLOGÍAS INALÁMBRICAS"

TRABAJO DE TITULACIÓN: **PROPUESTA TÉCNOLÓGICA**

Presentado para optar al Grado Académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: OMAR DARÍO DELGADO BRITO

TUTORA: Ing. Mónica Andrea Zabala M.Sc.

Riobamba-Ecuador

2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: El trabajo de investigación: Tipo Proyecto Técnico **"PROPUESTA DE UN SISTEMA AUTOMATIZADO PARA CONTROLAR EL ACCESO VEHICULAR EN LA ESPOCH MEDIANTE EL USO DE TECNOLOGÍAS INALÁMBRICAS"**, de responsabilidad del señor Omar Darío Delgado Brito, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

DR. JULIO SANTILLAN

VICEDECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA _____ _____

ING. FRANKLIN MORENO

DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA, TELECOMUNICACIONES Y REDES _____ _____

ING. MÓNICA ZABALA

DIRECTOR DEL TRABAJO DE TITULACIÓN _____ _____

ING. FRANKLIN MORENO

MIEMBRO DEL TRABAJO DE TITULACIÓN _____ _____

Yo, Omar Darío Delgado Brito, soy responsable de las ideas, criterios, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo.

Omar Darío Delgado Brito

DEDICATORIA

A Dios por haberme guiado por día a día y brindarme salud, sabiduría y la disciplina para poder alcanzar los objetivos que me propuse, día a día por bendecirme en todo lo que logrado.

A mis padres, Galo Delgado por haberme brindado la oportunidad de estudiar y superarme como persona, Eda Brito que ha estado en todo momento brindándome su apoyo incondicional, dándome concejos para ser mejor persona día a día, su compromiso ya que sin su ayuda nunca hubiera llegado a ser la persona que soy.

A mis hermanos Marlon y Freddy que están incondicionalmente apoyándome ayudándome a tomar la mejor decisión en las circunstancias a lo largo de mi vida tanto personal como profesional.

A todos los ingenieros que he conocido a lo largo de la carrera que gracias a su docencia he podido adquirir los conocimientos que poseo ahora, y a mis amigos que son un soporte extra en mi vida dándoles las gracias por todos los momentos compartidos en mi etapa de formación como estudiante.

AGRADECIMIENTO

A la Escuela Superior politécnica de Chimborazo, por brindarme la oportunidad de alcanzar mi objetivo un logro más, convirtiéndome en un profesional gracias a los valores éticos y morales que son pilares de la institución necesarios para formar no solo profesionales sino también personas de bien.

A mis docentes con los cuales he compartido no solo sus clases impartidas, sino experiencias muy valiosas ya que no solamente dictaban su clase sino también se daban tiempo para guiarme dándome concejos como sobrellevar el ámbito laboral y cotidiano, un especial agradecimiento a la Ing. Mónica Zabala quien fue un gran soporte durante todo el proceso ayudándome en cada etapa, resolviendo de la mejor manera mis dudas e inquietudes.

A cada una de las personas que estaban presentes en todo el proceso maestros, familiares, amigos que me apoyaron de alguna manera para que pueda realizar el presente Trabajo de titulación, ya que sin su apoyo incondicional no hubiese sido posible su ejecución.

TABLA DE CONTENIDO

ÍNDICE DE ABREVIATURAS

ESPOCH: Escuela Superior Politécnica de Chimborazo

FIE: Facultad de Informática y Electrónica

TIC: Tecnologías de la Información y la Comunicación

PNUD: Programa de las Naciones Unidas para el Desarrollo

ONU: Organización de las Naciones Unidas

CEDATOS: Centro de Estudios y Datos

USA: Estados Unidos de América

TX: Transmisor

RX: Receptor

IAN: International Article Number - (Asociación Internacional de Numeración de Artículos)

RFID: Radio Frequency Identification - (Identificación por Radiofrecuencia)

VHF: Very High Frequency - (Muy Baja Frecuencia)

LF: Low Frequency - (Baja Frecuencia)

MF: Medium Frequency - (Frecuencia Mediana)

HF: High Frequency - (Alta Frecuencia)

VHF: Very High Frecuency - (Muy Alta Frecuencia)

UHF: Ultra High Frecuency - (Ultra Alta frecuencia)

Hz: Hertz - (Hercio)

KHz: Kilo Hertz

MHz: Mega Hertz

GHz: Giga Hertz

IEEE: Institute Electrical and Electronics Enginners - (Instituto de Ingeniería Eléctrica y Electrónica)

bps: Bits por Segundo

Mbps: Mega Bits por Segundo

KB: Kilo Byte

MB: Mega Byte

GB: Giga Byte

LED: Light Emitting Diode (Diodo Emisor de Luz)

V: Voltio

E/S: Entrada y Salida

SS: Spread Spectrum - (Espectro Espandido)

Wi-Fi: Wireless Fidelity - (Fidelidad Inalámbrica)

WiMax: Worldwide Interoperability for Microwave Access - (Interoperabilidad Mundial de Acceso por Microondas)

Km: Kilometro

Qos: Quality of Service - (Calidad de Servicio)

OSI: Open Source Initiative – (Software de Código Abierto)

APL: Arduino Programming Language – (Lenguaje de Programación de Arduino)

IDE: Integrated Development Environment – (Entorno de Desarrollo Integrado)

INTEL: Integrated Electronics - (Electrónica Integrada)

SO: Operating System - (Sistema Operativo)

IoT: Internet of Things - (Internet de las Cosas)

LUA: Extensible Programming Language - (Lenguaje de Programación Extensible)

RAM: Random Access Memory - (Memoria de Acceso Aleatorio)

ROM: Read Only Memory - (Memoria Solo de Lectura)

EEPROM: Electricaly Eresable Programmable Read Only Memory – (Memoria Solo de Lectura Programable y Borrable Eléctricamente)

SGBD: Data Base Management Systems - (Sistema Gestor de Bases de Datos)

GPL: General Public License – (Licencia Pública General)

CERN: Concejo Europeo para la Investigación Nuclear

WWW: World Wide Web - (Red Informática Mundial)

RISC: Reduced Instruction Set Computer – (Ordenador con Conjunto Reducido de Instrucciones)

ARM: Advanced RISC Machine – (Maquina Avanzada RISC)

SD: Secure Digital - (Seguridad Digital)

mA: Miliamperio

mm: Milimetro

ms: Milisegundo

PHP: Hypertext Processor – (Procesador de Hipertexto)

SDA: Serial Data Input/Output - (Interfaz serial para la entrada o salida de datos)

SCK: Serial Clock - (Reloj Serial)

MOSI: Master Output Slave Input - (Maestro Salida Esclavo Entrada)

MISO: Master Input Slave Output - (Maestro Ingreso Esclavo Salida)

IRQ: Interrupt request - (Requerimiento de Interrupción)

GND: Ground - (Tierra)

RST: Reset - (Reiniciar)

LCD: Liquid Crystal Display - (Pantalla de Cristal Líquido)

DTIC: Departamento de Tecnologías de la Información y Comunicación)

VPN: Virtual Private Network - (Red Virtual Privada)

USD: Dólar Estadounidense

SAVEO: Sistema de Control de Acceso Vehicular por Omar

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

En la presente investigación se desarrolló la propuesta de un sistema de control de acceso vehicular para la Escuela Superior Politécnica de Chimborazo a través de tecnologías inalámbricas de corto y largo alcance para la identificación y conectividad del sistema. El sistema denominado Sistema de Acceso Vehicular en la ESPOCH por Omar (SAVEO) cuenta con tres etapas: entrada, control y salida, el cual basa a partir de su funcionamiento en la tecnología de identificación por radiofrecuencia (RFID), autoriza o deniega el acceso a la institución mediante etiquetas que tienen almacenado un código identificador único, la transmisión de datos se realiza a través de placas electrónicas NodeMCU, con la ayuda de un servidor web apache se envían los registros que son almacenados en una base de datos que es gestionada por phpMyAdmin, procesados por la tarjeta de desarrollo Raspberry pi. De las pruebas realizadas se obtuvo que la lectura máxima de las etiquetas utilizando tarjetas es de 3,5cm y utilizando llaveros es 2.5cm, el tiempo de retardo de petición es de 0.43seg para los llaveros, en la tarjeta es de 0.21seg y para el almacenamiento de los datos se tiene un retardo 1.125seg, cuando se realiza más de una lectura simultánea se insertó un retardo de 0.8seg en cada NodeMCU para no tener perdida de información. A través del análisis económico y técnico de la propuesta, el sistema cumple con los requerimientos propuestos, es viable para su implementación, el mismo contribuirá con la seguridad vehicular del personal que labora en la institución. Se recomienda para trabajos futuros tener la posibilidad de trabajar con monitorización, cámaras de video o un circuito cerrado de televisión en cada acceso de la institución.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <TELECOMUNICACIONES>, <COMUNICACIONES INALÁMBRICAS>, <CONTROL VEHICULAR>, <IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID)>, <TARJETAS DE DESARROLLO>.

SUMMARY

In the present research was developed a proposal for an access vehicles control system to the Escuela Superior Politecnica de Chimborazo through online technologies short and long range of the connectivity and identification system. The system called Sistema de Acceso Vehicular en la ESPCOH for Omar (SAVEO) consists of three stages: Entrance, Control, and, Exit which based draw from its operation in the identification technology by radiofrequency (RFID) authorize or refuse the access to the institution through tags that have stored an identifying unique code, the data transmission realized through electronic boards NodeMCU, with a help of Apache web server send the register that is storing in a data-based managed by phpMyAdmin, processes by the develop card Raspberry pi. From the tests performed getting the maximum reading from the tags using cards of 3,5 cm and using keys 2,5 cm, the request delay time is 0,43 seconds for the keys and in the card 0,21 seconds and to the storage of the date has a delay of 1.125 seconds when is used more than one at the same time reading a delay was inserted 0,8 seconds in each NodeMCU to avoid data loss. Through the economic and technical analysis of the proposal, the system meets the requirements proposed, it is feasible to its implementation which will contribute to the vehicle security of the staff work in the institution. It is recommended for futures research has the possibility to work with monitoring, video cameras, television closed circuit on each entrance of the institution.

KEY WORDS: <ENGINEERING AND TECHNOLOGY SCIENCE>, <TELECOMMUNICATIONS>, <WIRELESS COMMUNICATION>, <VEHICLES CONTROL>, <IDENTIFICATION BY RADIOFREQUENCY (RFID)>, <DEVELOPMENT BOARDS>.

INTRODUCCIÓN

Los avances científicos y tecnológicos que se han producido a lo largo de los años han dado como resultado las Tecnologías de la Información y la Comunicación (TIC) que poco a poco aportan de manera positiva a la vida cotidiana de las personas, ayudando en áreas encaminadas a la innovación, interconexión y automatización.

Donde es posible mejorar procesos que favorecen las actividades que desarrollan las personas de manera habitual, secundando los problemas de interés común, lo que ha provocado una modificación en las actividades realizadas a diario en donde los sistemas automatizados han tomado un mayor apogeo en numerosas aplicaciones (Belloch, 2010, p.1).

Los sistemas automatizados estimulan la aparición de nuevas herramientas y aplicaciones que asisten en áreas militares, industriales, de la educación entre otras, debido a la gran utilidad que ofrecen ayudan para mejorar u optimizar la operatividad de procesos o actividades cotidianas, combinando con los avances tecnológicos de la actualidad dan como resultado mejor rendimiento y control vehicular. (Asensi, 1995, p. 67)

Un sistema automatizado que controle el acceso vehicular a espacios concurridos tanto públicos como privados constituye un gran aporte de seguridad y confiabilidad para las personas que convergen con sus vehículos; es una prioridad por ello hay que poner especial interés, gracias a la tecnología que se cuenta hoy en día es posible hacerlo.

ANTECEDENTES

Según el informe Programa de Desarrollo de la ONU (PNUD), la inseguridad se ha convertido en un reto e impedimento compartido para el progreso tanto social como económico de los países de América Latina.

Las medidas que se han tomado contra el delito no son suficientes para reducir la inseguridad de manera duradera, PNUD recomienda utilizar políticas que ayuden a la prevención del delito encaminadas hacia la mejora de la calidad de vida de la población (UNDP, 2017).

En el Ecuador la problemática de la inseguridad ciudadana aumentado de manera considerable en los últimos años, según un estudio de opinión realizado por el Centro de Estudios y Datos (CEDATOS); de los encuestados la primera inquietante de sufrir algún delito, el 51% contesto que ha sido víctima de robos o asaltos; otra inquietante es que tan seguros se sienten y el 36% han respondido no sentirse nada seguros en la ciudad.

La situación es causa de preocupación para las autoridades y habitantes que sugieren acciones para mejorar la seguridad ciudadana, por tal motivo las empresas exploran diferentes alternativas de seguridad para satisfacer esta necesidad (UNDP, 2017).

En la ciudad de Riobamba el número de vehículos ha crecido exponencialmente saturándola, pues la ciudad no fue diseñada para un masivo tráfico vehicular. De la misma manera, en la Escuela Superior Politécnica de Chimborazo las infraestructuras viales fueron concebidas para la circulación de un bajo volumen de tráfico muy diferente a la realidad actual.

Según las transparencias del 2017 menciona que la institución alberga a 1671 personas entre docentes, empleados, personal administrativo sin contar con los estudiantes y vehículos particulares que ingresan a la institución por diversas actividades (LOTAIP, 2017).

Tomando en consideración el problema que se vive debido a la inseguridad ciudadana, crecimiento vehicular; el avance de la tecnología plantea grandes soluciones a la hora de llevar un control sobre el acceso vehicular hacia una institución pública o privada.

Este es el caso de los sistemas automatizados que se han convertido en una herramienta de gran utilidad realizando el control de acceso vehicular de manera rápida y segura, brindado un mayor grado de seguridad y confiabilidad para las personas que conforman la institución.

FORMULACIÓN DEL PROBLEMA

¿Es propicio tener un sistema automatizado para controlar el acceso vehicular en la ESPOCH basándose en tecnologías inalámbricas?

SISTEMATIZACIÓN DEL PROBLEMA

Para dar solución al problema planteado, es necesario ir respondiendo durante el desarrollo del trabajo las siguientes interrogantes:

- ¿Es necesario restringir el acceso vehicular en la ESPOCH?
- ¿Qué tecnologías son utilizadas en los sistemas de control de acceso vehicular?
- ¿Qué análisis se deben realizar a la situación actual de la ESPOCH para que sea factible implementar la propuesta?
- ¿Qué tipo de tecnología inalámbrica es provechosa utilizar para implementar el sistema de control vehicular?
- ¿Bajo qué supuestos se debe realizar la implementación de un prototipo del sistema?
- ¿Qué tipos de pruebas se deben realizar para validar la operatividad del sistema?

JUSTIFICACIÓN TEÓRICA

Con el paso de los años los avances tecnológicos son cada vez más notorios y comunes en la vida cotidiana de la mayoría de personas entre las que han tenido un mayor auge están la innovación, interconexión y automatización; los sistemas de control de acceso vehicular han permitido tener mayor seguridad, fiabilidad y confiabilidad para los usuarios que estén accediendo a la institución.

Actualmente, los sistemas de control vehicular que se usan en los países de primer mundo, tienen independencia total de algún personal encargado, al contrario de países como el nuestro, la labor se realiza sin un control acertado de los vehículos que ingresan. Adicionalmente si por algún motivo el personal encargado se ausenta el sistema se vuelve vulnerable causando incomodidad e inseguridad.

Los sistemas de control de acceso vehicular son empleados para contrastar el volumen de tráfico en los espacios tanto privado como público, esto permite tener el mando de que vehículo se le permite el ingreso y se le restringe al que no esté autorizado. Actualmente existe una gran variedad de sistemas, desde los más simples y sencillos hasta los robotizados.

Es importante modernizar los sistemas que controlan el acceso vehicular a instituciones tanto públicas como privadas, siendo el caso de la ESPOCH así se lograría tener un control de las personas con vehículo que ingresen a la institución.

La ESPOCH tiene la problemática que no existe un control que limite el acceso no autorizado de personas ajenas a la institución, es decir cualquier vehículo puede ingresar y salir exponiendo la integridad de los estudiantes, docentes, personal administrativo y empleados.

JUSTIFICACIÓN APLICATIVA

Actualmente la ESPOCH no cuenta con un sistema de control vehicular que limite el acceso a vehículos ajenos a la institución, en nuestro país son pocas las instituciones de educación superior públicas que tienen un sistema automatizado de control de acceso vehicular la mayoría de empresas que ofrecen este servicio son privadas siendo esta la razón de no existir suficiente documentación.

El presente Trabajo de Titulación pretende establecer una base para que los sistemas de control de acceso vehicular sean implementados en otras universidades y determinar los requerimientos necesarios que permitan el diseño, posteriormente la implementación de un prototipo de un sistema automatizado de control de acceso vehicular que permita tener un control y registro de los vehículos que ingresen a la institución.

La propuesta del sistema automatizado de control de acceso vehicular constituye una herramienta útil que ayudara a mejorar la seguridad y confort para las personas que conforman la institución de este modo cuidando la integridad y bienestar tanto a docentes, personal administrativo y estudiantes.

OBJETIVOS

OBJETIVO GENERAL

- Formular una propuesta de un sistema automatizado para controlar el acceso vehicular en la ESPOCH mediante el uso de tecnologías inalámbricas.

OBJETIVOS ESPECIFICOS

- Realizar el estudio de factibilidad de cada etapa propuesta del sistema automatizado.
- Examinar las tecnologías que son utilizadas para el control y verificación de ingreso y salida de vehículos.
- Analizar las características de tecnologías inalámbricas que se ajusten a los requerimientos del sistema.
- Demostrar la operatividad del sistema mediante la implementación de un prototipo.

A continuación se muestra el desarrollo del Trabajo de Titulación que consiste en tres capítulos, donde el Capítulo I Marco Teórico comprende el estudio y análisis de sistemas de control vehicular, tecnologías de comunicación, identificación, tarjetas de desarrollo, módulos inalámbricos y base de datos.

Cuya información es necesaria para iniciar el Capítulo II Marco Metodológico donde se detalla el diseño del sistema de control vehicular, los requerimientos tanto *hardware* como *software* además de las tablas comparativas y ponderación de las tecnologías de comunicación, tarjetas de desarrollo y módulos inalámbricos, así como también la viabilidad, costos y propuesta,.

Acto seguido el Capítulo III Marco de Pruebas y Resultados se ejecutan pruebas, mediciones *hardware* y *software* en los escenarios propuestos por los supuestos a los que se rige el sistema propuesto para finalmente concluir con las respectivas conclusiones y recomendaciones del Trabajo de Titulación.

CAPÍTULO I

1. MARCO TEÓRICO

En este capítulo se estudian las características de los sistemas y tecnologías de control vehicular, se específica también los sistemas de identificación, las tecnologías inalámbricas, módulos inalámbricos, base de datos, gestión de base de datos y servidores.

1.1. Automatización de sistemas

Las tareas de producción, control entre otras realizadas por un operario encargado se trasfieren a un grupo tecnológico, el sistema automatizado consta de dos partes una parte de mando y una parte operativa (Acevedo y Perez, 2009, p. 37).

La parte de mando debe trabajar de manera independiente es decir autómata esto se logra a través de tecnología programable (tarjetas de desarrollo), también debe ser capaz de comunicarse con cada una de las partes que conforma el sistema ya sea de manera alámbrica o inalámbricamente.

La parte operativa es aquella en la que el sistema realiza la operación deseada, aquí actúan los dispositivos finales (relevadores, motores, indicadores etc.) estos dispositivos son conocidos como actuadores o accionadores (Acevedo y Perez, 2009, p. 38).

1.1.1 *Tecnologías de la automatización*

En la automatización las tecnologías usadas se pueden dividir en dos grupos, la tecnología cableada en la cual todas las conexiones realizadas entre los diferentes elementos que conforman el sistema se lo realiza de manera física como mecánica, neumática, hidráulica y eléctrica.

La tecnología programable en la cual asistida por tarjetas de desarrollo se realiza la programación del sistema para que cumpla una tarea especificada en su código como: ordenadores, microcontroladores y tarjetas de desarrollo (Uniovi, 2002, p. 2).

1.2 Control vehicular

Busca regular las actividades de un vehículo con el fin de lograr un funcionamiento predeterminado, el control de acceso vehicular se implementa donde afluyen personas a lugares que pueden ser públicos o privados que deban garantizar seguridad ciudadana.
Con el paso del tiempo han surgido distintas tecnologías de identificación vehicular asegurando el acceso al vehículo que esté autorizado y denegando el acceso al vehículo que no esté autorizado (Rios, 2011, p. 17).

1.2.1 Tecnologías inmersas en el control vehicular

La industria automovilística de Estados Unidos de América (USA - United States of America) empezó a tener un auge a finales de la década de 1950, la industria creció rápidamente es por ello que el volumen vehicular fue incrementando.

Por esta razón surge la necesidad de tener un control sobre el volumen vehicular en distintas zonas pobladas, donde la primera solución a esta problemática fue colocar guardias que se encarguen de esta labor, poco a poco los avances tecnológicos fueron modificaron la manera de controlar el acceso (Isolve, 2002, p. 14), entre las tecnologías para el control vehicular más utilizadas actualmente tenemos:

Reconocimiento de placas

Figura 1-1: Reconocimiento de placas

Fuente: Nektrom Technologies, 2014

Su control total lo realiza el identificador de las placas del vehículo, su virtud es reconocer propiamente la placa así se tiene la información del propietario del vehículo, el inconveniente es el descuido de acceso debido a que el vehículo es el autorizado mas no la persona, a esto se le debe sumar los altos costos que tienen sus dispositivos.

Acceso vehicular por radiofrecuencia

Figura 2-1: Acceso vehicular por radiofrecuencia

Fuente: Hackster.io, 2018

Gravita su funcionamiento en tecnología inalámbrica de corto o largo alcance dependiendo la frecuencia que se maneje, la distancia es un factor fundamental, cada usuario tiene una tarjeta con un identificador propio y único

Barreras vehiculares automáticas

Figura 3-1: Barreras vehiculares automáticas

Fuente: planetamexico, 2016

Esta tecnología basa su funcionamiento en las lecturas de sensores de proximidad es decir detecta un vehículo cercano y las barreras se accionan automáticamente, su desventaja es que cualquier vehículo autorizado o no autorizado tiene acceso.

Brazos electromecánicos

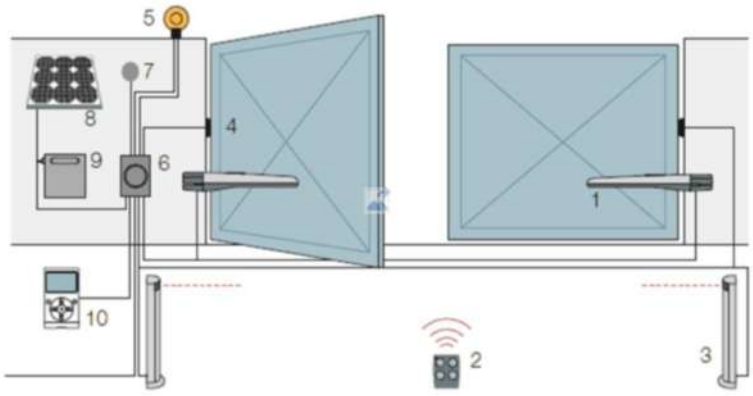


Figura 4-1: Control vehicular electromecánico

Fuente: Dointech Sas, 2015

Su desempeño se apoya en sensores de proximidad es decir detecta el vehículo y se activa, en este caso activara los brazos que tienen parte mecánica y parte electrónica, nuevamente al igual que el anterior su principal inconveniente es la falta de seguridad que brinda.

1.3 Tecnologías para la identificación

Con el avance de la tecnología se ha podido emplear sistemas que son utilizados para la identificación de objetos y personas, así logrando el manejo de la información que proporciona el objeto o persona identificada.

Para realizar la identificación se requiere de dos partes fundamentales un elemento que contenga la información ya sea codificada o no y otro elemento que sea capaz de reconocer esta información.

En la vida cotidiana se puede realizar el proceso de identificación de personas u objetos para acceder a diferentes servicios, tarjetas de crédito, control de asistencia, acceso a una zona,

también el costo, precio, stock de un producto, la ubicación de una persona u objeto entre las características más relevantes (Medina César, 1994).

1.3.1 Sistema de código de barras

Los códigos de barras fueron establecidos por la Asociación Internacional de Numeración de Artículos (IAN), este fue el sistema más difundido por disponibilidad, fue aplicado hace alrededor de 20 años aproximadamente con éxito.

Figura 5-1: Código de Barras
Fuente: Omar Delgado, 2018

Su funcionamiento se basa en un código binario que comprende una serie de líneas paralelas verticales y espacios blancos, ambos de diferentes anchos cuya secuencia que emplea tiene forma numérica o alfanumérica, la lectura se realiza por una luz láser proveniente de un escáner óptico que se basa en la reflexión de la luz de las barras (blancas y negras).

Los usos más comunes se da en la identificación de los productos donde en su información guarda sus características o datos técnicos como lo son origen, stock, precio, marca entre otras (Monsó, 1994, p. 18).

1.3.2 Sistema de tarjetas magnéticas

Son tarjetas plásticas que en una parte de la tarjeta tiene una pista negra que es usada para leer y grabar datos, los estándares utilizados son ISO 1 (79 caracteres alfanuméricos con densidad de codificación de 210bpi) ISO 2 (40 caracteres alfanuméricos con densidad de codificación de

75bpi) ISO 3 (107 caracteres alfanuméricos con densidad de codificación de 210bpi), y por último la norma ISO 7811 es que define las características de la tarjeta plástica.

Figura 6-1: Sistema de tarjetas magnéticas

Fuente: https://www.indiamart.com/nirmalpravidyainfotech/swipe-machine.html

El registro o la escritura se realizan a través de un pequeño electroimán que transforma la energía eléctrica empleada en un campo magnético que contiene la información codificada. Los usos más comunes que tienen este tipo de sistema son para el acceso a un determinado lugar o zona en específico, tarjetas de crédito, ingreso a un hotel, parking entre los más conocidos (Monsó, 1994, p. 119).

1.3.3 Sistema biométrico

Actualmente este sistema basa la identificación en el reconocimiento de diversas características huellas dactilares, iris, y rostro cada una de ellas posee ventajas y desventajas a la hora de realizar la identificación.

Figura 7-1: Sistema Biométrico

Editado por: Omar Delgado, 2018

Identificación por huella dactilar

La lectura de la huella dactilar generalmente el dedo pulgar, que ha tenido un auge en la tecnología de identificación debido que satisface los requerimientos de evidencia e identificación propiamente, los dibujos que aparecen en la epidermis son perennes es decir son originales y diversiformes (Monsó, 1994, p. 121).

Identificación de iris

Analiza el patrón al azar del iris de una persona (el iris regula el tamaño de la pupila, controlando la cantidad de luz que ingresa al ojo), en un individuo aunque sus iris sean muy semejantes su estructura es distinta, debido a ello permite realizar la distinción; el reconocimiento de iris y el reconocimiento de la retina son proceso parecidos pero distintos ya que su identificación se basa en patrones diferentes (Monsó, 1994, p. 124).

Identificación facial

Este sistema no es tan nuevo como aparenta desde la década de 1960 se ha ido realizando pruebas, siendo la automatización de manera parcial teniendo en gran parte intervención humana.

En la actualidad la intervención humana se ha reducido siendo nula para mejorar los cálculos matemáticos, procesos y programación siendo utilizados para identificar de manera cuidadosa y precisa a distintos tipos de personas aportando en gran medida en la seguridad, hay que tomar en cuenta que esta tecnología no es intrusiva (Monsó, 1994, p. 126).

1.3.4 Sistema de identificación por radiofrecuencia

Sistema de identificación por radiofrecuencia (RFID - Radio Frecuency Identification), es una tecnología que se remite a los inicios de la radio, en 1860 se empieza a estudiar la comunicación por radiofrecuencia, de origen militar fueron las primeras aplicaciones de RFID, teniendo más auge en el desarrollo de la segunda guerra mundial en donde se les colocaba una etiqueta (tag) a los aviones para identificarlo si es amigo o enemigo (Hunt y Puglia, 2017, p. 1).

Aunque no es una tecnología nueva, las mejores que tiene como alcance, seguridad, velocidad de lectura, almacenamiento representan una importante reducción en los costes como en cadenas de producción y logística.

El fundamento básico de esta tecnología es la identificación de objetos o personas a distancia sin necesidad de tener una línea de vista propia y contacto propio, una solución básica en la cual se basa RFID se compone de una o más antenas, etiquetas de identificación (tags), y un software que realice el procesamiento de la información recolectada por los lectores.

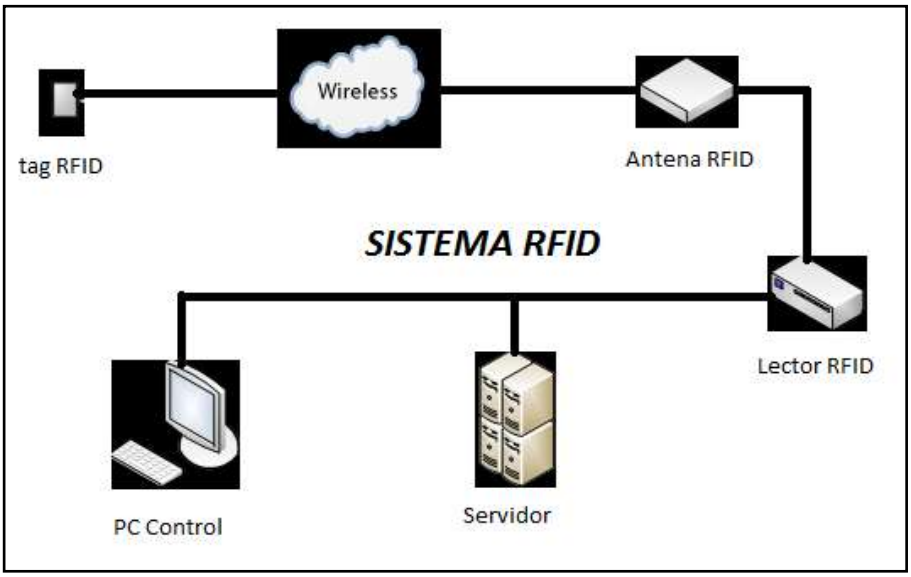


Figura 8-1: Sistema de identificación por radiofrecuencia

Realizado por: Omar Delgado, 2018

RFID es una tecnología que con el paso del tiempo ha ido tomando cada vez mayor importancia a la hora de identificar una persona o un objeto de cualquier tipo ya que de manera inalámbrica permite la obtención de los datos de forma automática; una tecnología bastante versátil que tiene un mercado muy amplio en aplicaciones desde trazabilidad, control de inventario, seguimiento de personas, la seguridad y control de accesos.

Su funcionamiento gravita en la emisión ondas de radiofrecuencia que son captadas por el tag que tiene almacenado un código u información, estas ondas activan el microchip que tiene integrada la etiqueta el cual emite la información al lector (Hunt y Puglia, 2007, p. 3).

Existen varios organismos que regulan en menor o mayor medida la estandarización de la tecnología RFID, la organización internacional de estandarización define los estándares comerciales e industriales a nivel mundial y la comisión internacional electrotécnica promueve la estandarización en los campos de la electrónica y las tecnologías.

- Estándar ISO 1423 contiene la estructura del código de identificación por radiofrecuencia para animales, detalla el interfaz aire entre el lector y el transponder basando en la condición de compatibilidad.
- Estándar ISO 15693 define las características físicas, el interfaz de aire e inicialización, protocolos anti-colisión y de trasmisión de tarjetas inteligentes.
- Estándar ISO 10374 especifica los requisitos de usuario para la identificación automática de contenedores de carga, codificación de datos, criterios de seguridad y rendimiento.
- Estándar ISO 15963 para las técnicas de identificación automática y adquisición de datos para gestión de objetos, incluyendo los protocolos, interfaz y reglas de codificación.
- Estándar ISO series 1800 de q a 6 definen los parámetros para el interfaz aire en las frecuencias aceptadas para su funcionamiento: 125Khz, 13.56Mhz, 2.45Ghz y 5.8Ghz centra los métodos de rendimiento de tags y lectores así como también la conformidad de los dispositivos.

1.3.4.1 Etiqueta RFID

Los tags tienen en su interior un pequeño chip, un bobinado (para realizar la comunicación), y una antena impresa, el chip tiene grabado un código de serie único para identificarlo de los demás, aparte contiene pequeños bloques de memoria para leer, escribir, guardar otros datos.

La banda de los 25KHz muy baja frecuencia (VLF - Very Low Frecuencia) era utilizada en los primeros lectores, las tarjetas modernas trabajan en alta frecuencia (HF) de 13,56 MHz (Hunt y Puglia, 2007, p. 6).

Figura 9-1: Etiqueta de identificación por radiofrecuencia

Fuente: http://www.ravirajtech.com/rfid-tags.html

Existen tres tipos de etiquetas activas, semipasivas y pasivas.
Los etiquetas pasivos no tienen ningún tipo de alimentación es decir no necesitan alimentación interna debido a que la lectura y envió de datos se los hace aprovechando el campo magnético provocado al bobinado, estas etiquetas no son programables.

Las etiquetas activas son lo que tienen una fuente de alimentación interna, tienen una fuente de poder interna que energiza los diferentes componentes chip, y el transmisor para poder establecer comunicación, estas etiquetas son programables.

Las etiquetas semipasivas son muy similares a las tags activas tienen un alimentador interno pero este solamente energiza al chip, la parte de lectura y transmisión de datos lo hace a través del bobinado, son semi programables de manera similar es decir se puede editar pocos bloques de memoria de la etiqueta.

1.3.4.2 Lector RFID

El lector la parte más importantes del sistema de identificación, debido a que cuenta con una

antena incorporada para comunicarse con la etiqueta del circuito que es la parte encargada de emitir las ondas de radiofrecuencia, que posteriormente serán replicadas con información de la etiqueta en un determinado rango de acción que viene delimitado por la frecuencia que se trabaje (Rios, 2011, p. 18).

Figura 10-1: Lector de identificación por radiofrecuencia

Fuente: Omar Delgado, 2018

1.3.4.3 Antena RFID

Existen antenas para la identificación utilizadas para transmitir y recibir las señales de radiofrecuencia, es decir de forma bidireccional otros sistemas utilizan una antena para él envió y otra para la recepción, es decir de manera unidireccional la cantidad y tipo de antena depende de los requerimientos de las aplicaciones que se vayan a utilizar; además del alcance corto alcance y largo alcance. (Rios, 2011, p. 19)

1.3.4.4 Tipos de sistemas RFID

Los sistemas que existen en la actualidad trabajan a baja frecuencia, alta frecuencia y ultra alta frecuencia las ondas de radiofrecuencia utilizadas por cada sistema operan de manera distinta por lo cual presentan ventajas y desventajas.

Tabla 1-1: Tipos de sistemas de identificación por radiofrecuencia

Sistema	Banda	Frecuencia	Rango	Característica
	LF	125Khz		Resiste bastante a

Baja Frecuencia	30 – 300Khz	o 134Khz	10 cm	interferencias externas.
Alta Frecuencia	HF 3 – 30Mhz	13,56Mhz	10cm – 1m	Utilizados comúnmente para ticketing.
Ultra alta Frecuencia	UHF 300Mhz - 3Ghz	860Mhz a 960Mhz	12m	Transmisión de datos rápida, pero sensible.

Realizado por: Omar Delgado, 2018

Fuente: (http://www.dipolerfid.es/es/blog/Tipos-Sistemas-RFID, s.f.)

Según la banda de frecuencia utilizada en la transmisión entre lector y antena se lo realiza a través de los acoplamientos de distinta forma:

- Acoplamiento inductivo se utiliza en comunicaciones de baja frecuencia (LF) y alta frecuencia (HF), donde la corriente que circula por la antena genera un campo magnético que al alcanzar la etiqueta conmuta la impedancia de carga para crear una modulación que permita la transmisión de los datos.
- Acoplamiento capacitivo usado en comunicaciones de muy alta frecuencia (UHF) y microondas donde el lector transmite una señal de radiofrecuencia, la etiqueta la recibe, modula y la refleja hacia el nuevo lector, y finalmente retransmiten la señal en respuesta.

1.4 Tecnologías inalámbricas

1.4.1 Bluetooth

Bluetooth es un protocolo IEEE 802.15 (Institute of Electrical and Electronics Engineers – Instituto de Ingeniería Eléctrica y Electrónica) que permite él envió de datos de manera inalámbrica a corto alcance a una serie de dispositivos electrónicos para el intercambio de información entre ellos que requiera un poco ancho de banda (BW - Bandwidth).

Esta tecnología es pionera y vino a reemplazar a su sucesor infrarrojo, que su mayor debilidad era que para el intercambio de información los dispositivos debían estar totalmente pegados y

no debían moverse hasta que finalice la transferencia, la tecnología bluetooth trabaja en la banda de 2,4Ghz esta tecnología es capaz de atravesar paredes (Huang y Rudolph, 2007, p. 67).

Existen 5 tipos de versiones de esta tecnología donde los rangos de frecuencias que utilizan influyen directamente la velocidad de transmisión de datos que van desde 1Mbps a 24Mbps. La tecnología Bluetooth está dividida en tres clases 1,2 y 3 a medida que la clase disminuye la potencia y el alcance aumenta, siendo la clase 2 la más comercial.

- Pequeña escala
- Bajo Costo
- Baja Complejidad
- Corto alcance
- Baja transferencia de datos

1.4.2 ZigBee

El protocolo ZigBee (IEEE 802.15.4) versión 1.0 está diseñada para la comunicación inalámbrica de largo alcance y con una tasa de transferencia baja, opera en las bandas libres 2.4Ghz y en la banda 858Mhz para Europa y 915Mhz para USA, utiliza la técnica SS (Spread Spectrum – Espectro Expandido) para el envío de la información (Wexler, 2007, p. 2).

- Escalable
- Bajo Costo
- Complejo
- Mediano alcance
- Baja transferencia de datos

1.4.3 Wi-Fi

Esta tecnología llego a ser una solución inalámbrica de baja capacidad en el hogar y en las industrias como son la domótica y la automatización industrial, debido a la velocidad de transmisión de datos ofrece una baja expectativa siendo ideal en aplicaciones que tengan un bajo consumo.

Wireless Fidelity (Wi-Fi) es la tecnología que más se ha difundido a lo largo del tiempo debido a que ofrece una mayor cantidad de beneficios al costo más bajo, es económica y su punto más

fuerte es la interoperabilidad con los diferentes fabricantes de equipos que utilizan el estándar IEEE 802.11.

Esta tecnología utiliza la técnica de espectro expandido que permite que la señal se pueda propagar dentro de un intervalo de bandas de frecuencias permitidas al público (Carballar, 2010, p. 1).

Wi-Fi 802.11, opera en las bandas de frecuencias libres de 2.4Ghz y 5Ghz, esta tecnología ha ido evolucionando y mejorando su tasa de transferencia con las distintas versiones IEEE 802.11 a, IEEE 802.11 b, IEEE 802.11 g, y por ultima su actual versión IEEE 802.11 n cuya tasa máxima de transferencia bordea los 600Mbps que se impone en el mercado.

- Escalable
- Bajos costos
- Interoperable
- Alcance medio
- Alta tasa de transferencia

1.4.4 WiMax

Worlwide Interoperability for Microwave Access (WiMax) la tecnología estandarizado bajo el protocolo IEEE 802.16 e, es considerada el hermano mayor de Wi-Fi debido a que promete mayor alcance, mayor ancho de banda y más potencia también introdujo mejoras para tener mejor soporte (velocidades de 120Km) de movilidad (Taylor et al., 2006, p. 149).

WiMax y WiFi son totalmente diferentes debido a que fueron diseñados para diferentes ámbitos, además WiMax usa tecnología completamente diferente ya que usa frecuencias licenciadas como exentas, también se antepone a que incorpora QoS (Servicio de Calidad).

- Gran escalabilidad
- Costoso
- Complejo
- Gran alcance
- Tasa de transferencia alta

1.5 Tarjetas de desarrollo

Una tarjeta de desarrollo es una herramienta útil para el mejoramiento de los procesos de diseño de sistemas digitales y analógicos debido a que ofrece una solución y a la vez un producto final, facilitan la creación de aplicaciones que son de gran utilidad para la sociedad, brindando una gran compatibilidad con dispositivos y sensores.

1.5.1 Arduino

Es una plataforma *Software* de Código Abierto (OSI - Open Source Initiative) enfocada a la elaboración de prototipos electrónicos que se basa tanto en *hardware* como en *software* libre que son sencillos de usar.

Arduino puede interactuar y ejecutar acciones con sus puertos de salida analógicos y digitales, cuenta con un microcontrolador en el cual se programan las diferentes actividades que sean requeridas mediante el uso del Lenguaje de Programación de Arduino (APL - Arduino Programming Language), gracias a su Entorno de Desarrollo Integrado (IDE - Integrated Development Environment) (Caicedo, 2017, p. 5).

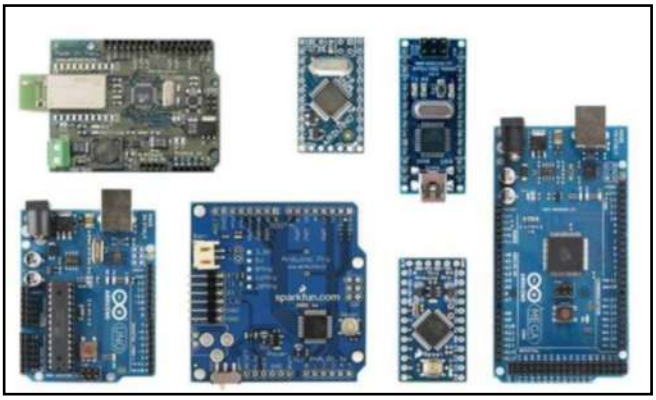


Figura 11-1: Tarjeta de desarrollo Arduino

Fuente: Omar Delgado, 2018

- Bajo costo
- Multiplataforma
- Entorno de programación simple
- Código abierto y *hardware* y *software* extensible

1.5.2 Galileo

Es una placa de desarrollo de la empresa Electrónica Integrada (Intel - Integrated Electronics) sirve para la creación de rápidos y simples proyectos que son a la vez interactivos, trabaja bajo la arquitectura de Intel pero al ser multiplataforma es compatible con la familia Arduino, siendo un sistema capaz de funcionar con el sistema operativo Windows y versiones de Linux, es una herramienta bastante interesante para el campo de la domótica (Intel, 2017).

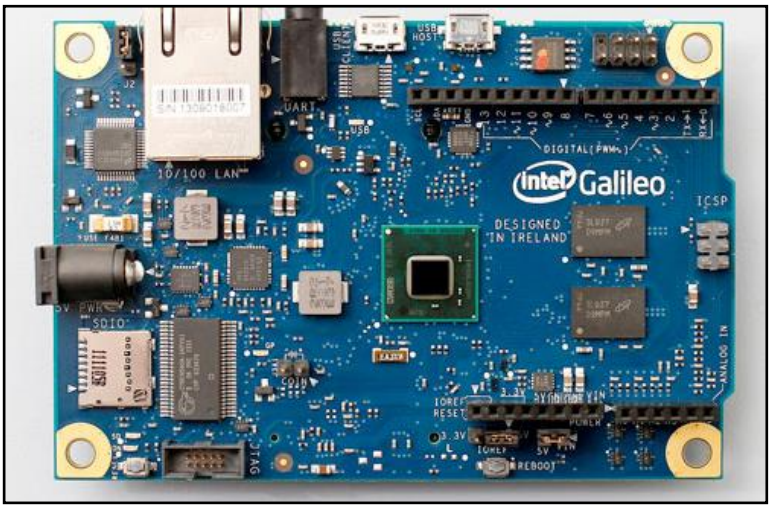


Figura 12-1: Tarjeta de desarrollo Galileo

Fuente: *http://www.neoteo.com/galileo-la-placa-de-desarrollod-de-intel-y-ardui*

- Alto costo
- Multiplataforma
- Entorno de programación interactivo
- Código abierto

1.5.3 Raspberry Pi

Es una placa computadora de costo bajo, es un ordenador reducido desarrollado por la fundación Raspberry Pi en el Reino Unido por la Universidad Cambridge con fines didácticos, soporta varios componentes para comportarse como un ordenador común (teclado, mouse, pantalla).

Utiliza lenguajes de alto nivel como Python, C++, y Java. Debido a la capacidad que tiene de soportar sistemas operativos basados en Linux, permite implementar servidores web dedicados (François, 2016, p. 22).

Figura 13-1: Tarjeta de desarrollo Raspberry Pi

Fuente: Omar Delgado, 2018

- Bajo costo
- Interoperable
- Entorno de programación interactivo fácil de usar
- *Hardware* y *software* Extensible

1.6 Módulos de conexión inalámbrica

1.6.1 Pinoccio

Un éxito de la campaña Crowfunding de la compañía Indiegogo una tarjeta que es compatible con Arduino basada en el estándar IEEE 802.15.4 con una red en malla integrada y una batería Li-Po, tiene la capacidad que le permite conectarse a través de Wi-Fi por medio de un shield, ideal para cubrir un área geográfica con una red inalámbrica. (Http://teslabem.com/productos/tarjetas-de-desarrollo.html)

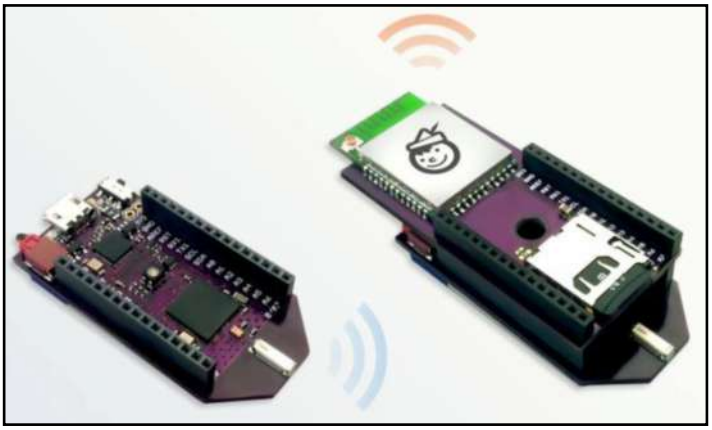


Figura 14-1: Módulo comunicación inalámbrica Pinoccio

Fuente: http://hacedores.com/que-tarjeta-de-desarrollo-elegir-parte-2/

1.6.2 NodeMCU

Es una plataforma de desarrollo de bajo coste de manera similar a Arduino, esta plataforma está orientada al IoT (Internet of Things - Internet de las Cosas), desarrollada para aplicaciones que necesiten conectarse a internet a través de Wi-Fi.

NodeMCU tiene un potente procesador de 32 bits que provee mayor flexibilidad, además de trabajar con el Lenguaje de Programación Extensible (LUA - Extensible Programming Language) usado por Arduino y lenguaje interpretado por LUA en general una mejor experiencia para el usuario (Kurniawan, 2015, p. 7).

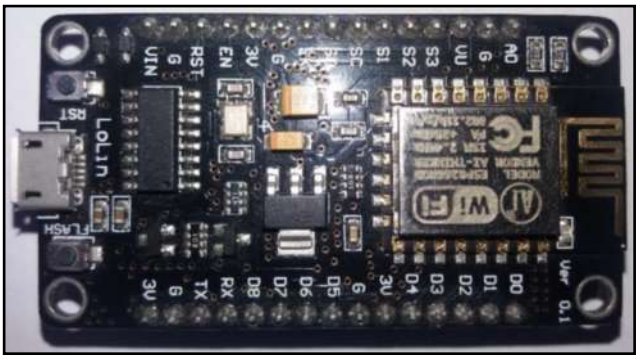


Figura 15-1: Módulo comunicación inalámbrica NodeMCU

Fuente: Omar Delgado, 2018

1.6.3 PcDuino

PcDuino es una tarjeta embebida que ejecuta una distribución de Linux, cuenta con una interfaz que es compatible con Arduino, es generalmente utilizado en aplicaciones que generalmente usan Phyton, C; pues el código se escribe directamente en la tarjeta, se ejecuta de manera nativa en la tarjeta (Kurniawan, 2015, p. 8).

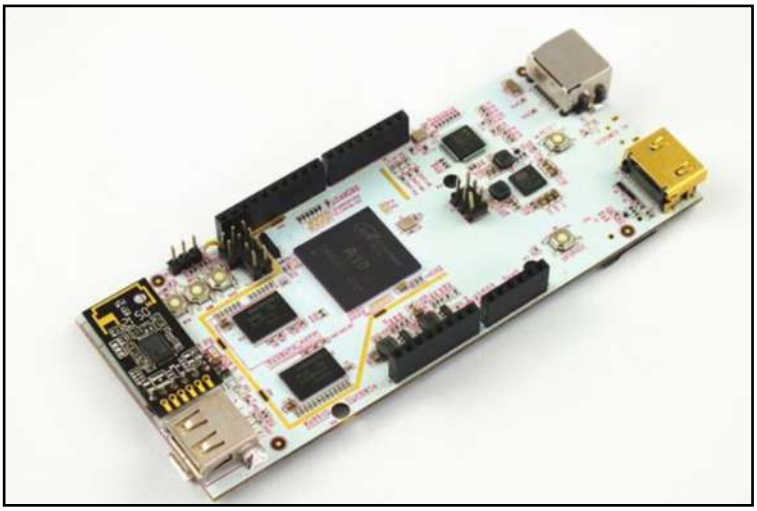


Figura 16-1: Módulo comunicación inalámbrica PcDuino

Fuente: http://hacedores.com/que-tarjeta-de-desarrollo-elegir-parte-2/

1.6.4 Beaglebone

La empresa de Texas Instruments ha diseñado la tarjeta BeagleBone desde cero para comunicarse con partes *hardware* (sensores, actuadores), esta tarjeta fue diseñada para los makers, que trae consigo nuevas características una de ellas trasladar el sistema operativo hacia la EEPROM (Electricaly Eresable Programmable Read Only Memory – Memoria Solo de Lectura Programable y Borrable Eléctricamente) memoria flash incorporada (McLaughlin, 2016, p. 41).

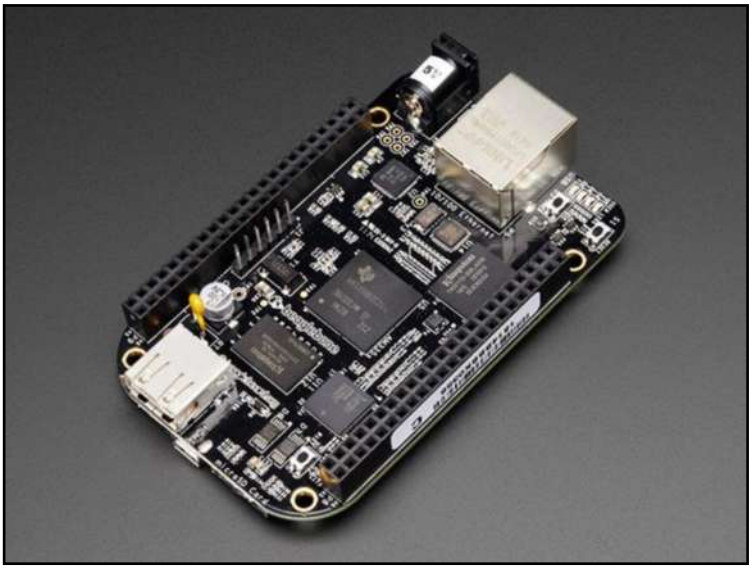


Figura 17-1: Módulo comunicación inalámbrica BeagleBone

Realizado por: http://hacedores.com/que-tarjeta-de-desarrollo-elegir-parte-2/

1.7 Topología

Es la manera en la que está configurada la red, como están interconectados los nodos siendo su configuración *hardware* compuesta por el transmisor (Tx), el receptor (Rx), medio de comunicación y procesamiento. Las topologías más conocidas tenemos: topología estrella, malla y mixta como se muestra en la figura 18-1.

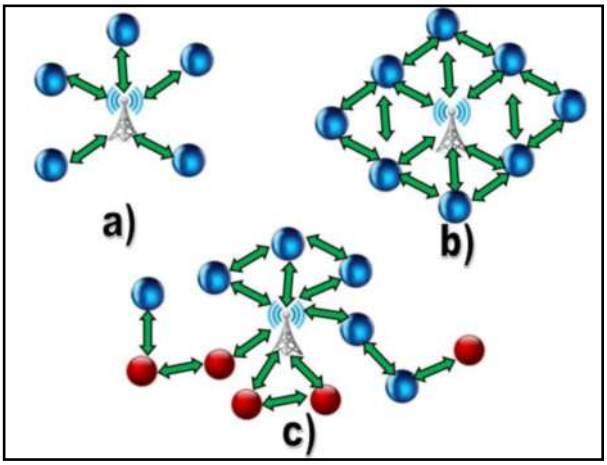


Figura 18-1: Topología a) estrella b) malla c) mixta

Realizado por: Omar Delgado, 2018

Estrella.- Es aquella red en la cual los nodos están conectados directamente con un nodo central y todas las comunicaciones realizadas lo harán a través de este, los nodos no están conectados entre sí, es decir comunicaciones punto a punto, cada nodo puede tomar el rol de esclavo o el rol de maestro (maestro- esclavo). Presenta un menor consumo de energía, la cual está limitada por la distancia entre los nodos, varía entre 30 a 100 metros.

Una gran desventaja es cuando falla la transmisión con uno de sus nodos se pierde la transmisión de la información, debido a que no existe otro camino alternativo. (Ruiz y Sánchez, 2013, pp. 327-328)

Malla.- Es aquella red en la cual todos los nodos están conectados entre sí a todos los nodos vecinos, cada nodo puede enviar y recibir información de otro nodo y del nodo central, una gran ventaja que posee es ser altamente tolerante a fallos debido a que cuenta con múltiples caminos (redundancia), el tiempo de transmisión varía dependiendo de la distancia entre los nodos y el número de nodos de la red (Ruiz y Sánchez, 2013, p. 329).

Mixta.- Es una red hibrida entre estrella y malla combina sus características como el bajo consumo energético y la posibilidad de cubrir una mayor extensión geográfica también tolera fallos gracias a los múltiples caminos. Esta red se amplía creándose nodos estrella alrededor de los nodos malla, conectándose a los más cercanos para así tener un ahorro energético.

1.7.1 Modos de transmisión

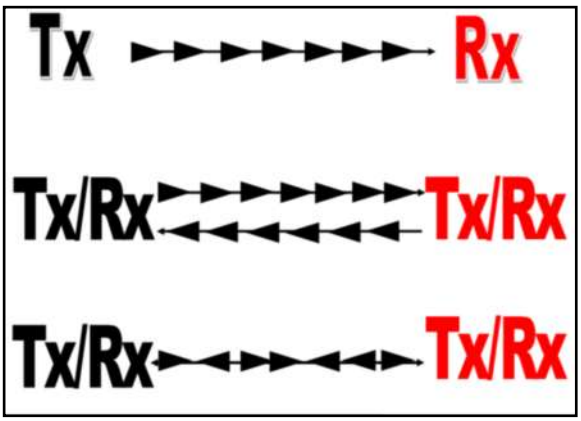


Figura 19-1: Modos de transmisión

Realizado por: Omar Delgado, 2018

Simplex.- El envío y recepción de la información se realiza en un solo sentido.

Half - Dúplex.- Él envió de información se lo realiza de ambos sentidos de transmisor a receptor y de receptor a emisor pero solo uno a la vez no ambos al mismo tiempo, es decir mientras se está enviando información no se puede recibir información, este caso se conoce como enlace asimétrico.

Full – Dúplex.- La transmisión de la información se puede realizar en ambos sentidos y al mismo tiempo, es decir mientras se está transmitiendo la información también se puede recibir información, este caso se conoce como enlace simétrico.

1.8 Base de Datos

En los años sesenta las aplicaciones se daban por lotes (batch), además solo realizaban una tarea en específico, con el paso del tiempo se tuvo la necesidad de integrar las aplicaciones de la misma manera interrelacionar los ficheros y eliminar redundancia (nombre, dirección, precio, etc.).

Estos conjuntos de ficheros interrelacionados recibieron el nombre Data Banks (Banco de datos) por sus estructuras complejas y procesos compartidos, luego con el paso de los años recibieron el nombre Data Bases (Base de Datos). (Date, 2007, p. 5)

Base de datos es un conjunto estructurado de datos los cuales se representan en entidades y relaciones, es la representación de un conjunto estructurado de datos de las diferentes entidades y sus interrelaciones que debe poder ser usadas de forma simultánea por múltiples usuarios de tipo distinto (Date, 2007, p. 9).

1.8.1 Gestor de Base de Datos

Los SGBD (Data Base Management Systems - Sistema Gestor de Bases de Datos) en los años sesenta y setenta eran centralizados en su totalidad comprendía de un gran ordenador y una red de terminales sin contar con memoria ni inteligencia.

Con el paso del tiempo se lograba una independencia de los programas en los aspectos físicos de las bases de datos, hoy en día los aspectos fundamentales de prioridad son tres multimedia, orientado a objetos e internet para su gestión existen varios gestores entre los más conocidos tenemos phpMyAdmin, MySQL, Oracle, Microsoft SQL server, PostgreSQL, DB2 entre otros (Ibáñez y Raya, 2011, p. 16).

PhpMyAdmin un gestor de bases de datos muy usado ya que su simplicidad y rendimiento son muy notables a la hora de administrar una base de datos, debido a su facilidad de uso y un corto tiempo de puesta en marcha carece de características avanzadas que cuentan otros gestores en el mercado.

Gracias a que trabaja bajo la licencia GPL (General Public License – Licencia Pública General) y su distribución libre le aportan beneficios extras como un rápido desarrollo y el alto grado de estabilidad (Ibáñez y Raya, 2011, p. 17), entre otras características:

- Desarrollado bajo C++
- Variedad en la disponibilidad del API (C, C++, Java, PHP, Python entre otros)
- Velocidad de respuesta destacable
- Soporta múltiples métodos de almacenamiento

1.9 Servidor Web

En 1989 del proyecto CERN (Concejo Europeo para la Investigación Nuclear) nace la web tiempo después Tim Berners le da lugar a lo que se conoce como WWW (World Wide Web - Red Informática Mundial) donde la idea original fue hacer más sencillo compartir textos con información científica para la comodidad del lector un sistema de hipertexto sería el encargado de realizar la función de enlazar los documentos mientras se realiza la lectura. (Andreu, 2011, p. 166).

El servicio web funciona siguiendo el modelo cliente – servidor muy común en aplicaciones que trabajan en una red, es decir el servidor recibe las peticiones del cliente y responde con ficheros solicitados (texto, imágenes).

Los servidores web se pueden localizar dentro de la misma red local y fuera en otra red (servidores remotos) ya sea en la misma ciudad o país, entre los servidores web más conocidos tenemos Apache, Microsoft IIS, Sun Java System Web Server, Ngnix, Lighttp, entre otros (Lara, 2011, p. 7).

Apache se deriva debido a que consistía inicialmente en un conjunto de parches que aplicaba NCSA (Next College Student Athlete) es decir un servidor parcheado (Patchy Server), desarrollador dentro del proyecto HTTP (Protocolo de transferencia de hipertexto) por la fundación Apache *Software*.

Apache presenta características mensajes de error, autenticación en base de datos, contenido negociado entre las más importantes, cabe recalcar que es de código abierto, multiplataforma, extensible, y gratuito (Mifsuf, 2012, p. 3).

CAPITULO 2

2. MARCO METODOLÓGICO

En el presente capitulo se detalla el diseño metodológico que se utiliza para el desarrollo de la propuesta tecnológica, situación actual, la concepción general del sistema de control de acceso vehicular así como también se brinda una descripción elementos *hardware* y *software* necesarios para su implementación.

2.1 Situación actual de la ESPOCH

En la Escuela Superior Politécnica de Chimborazo las infraestructuras viales fueron concebidas para un bajo volumen vehicular, inicialmente para tener un control de acceso de vehículos era controlado por un personal encargado de autorizar y llevar un registro de los vehículos que ingresan a la Institución, como era de esperarse con el avance de la tecnología se modificó la manera de controlar el ingreso.

Colocando unas barreras automáticas al a par con un dispensador de tickets para tener un registro del vehículo que ingresa, con el paso del tiempo se modificó el sistema, debido a que el antiguo sistema solamente registraba el número de vehículos que ingresaban más no que vehículo lo hacía, el nuevo sistema implementado contaba con una antena capaz de detectar el vehículo y permitir del acceso activando las barreras.

Actualmente la ESPOCH cuenta con tres ingresos en la institución ingreso principal, ingreso posterior y un ingreso lateral como se puede apreciar en la figura 1-2, dos de los cuales cuentan con dos barreras laterales automáticas deterioradas debido al uso nulo que ha tenido con el paso del tiempo, también cuentan con dos rompe velocidades tanto de entrada como de salida.

De los ingresos vehiculares ninguno de ellos cuenta con un control de acceso vehicular, de manera que cualquier vehículo puede ingresar a la ESPOCH, es por ello que para solucionar esta problemática se realiza la propuesta tecnológica que tiene como objetivo brindar un control en el acceso vehicular en la institución y así ayudar con la seguridad e integridad de las personas que conforman la ESPOCH.

Figura 1-2: Ingresos vehiculares de la ESPOCH

Fuente: ESPOCH, 2018

2.2 Requerimientos del sistema de control de acceso vehicular

El sistema de control de acceso vehicular para su diseño *hardware* y *software* debe poseer características que aseguren: escalabilidad, confiabilidad, flexibilidad y seguridad así como restringir el ingreso a personas ajenas a la institución para proteger la integridad y bienestar de las personas que la conforman.

Además de brindar confort y asistir con los registros a las cámaras de seguridad que cuenta la institución para poder evitar robos de vehículos por medio de los, partiendo de puntos de vital importancia como:

- Restringir el acceso vehicular a personas ajenas a la institución.
- Otorgar acceso vehicular a los usuarios autorizados.
- Emplear los recursos de comunicación y físicos que posee la institución.
- Identificar al usuario de manera única.
- Utilizar dispositivos para la comunicación inalámbrica.
- Utilizar *software* de licencia GPL.

- Poseer un servidor para el envío y recepción de información basado en una base de datos para el almacenaje y gestión de registros.
- Considerar una opción para que los registros sean respaldados.
- Usar un actuador para permitir o restringir el acceso vehicular.
- Mostrar mensajes para el usuario de ingreso y salida.

2.3 Concepción general del sistema

Se tomó como punto de partida el supuesto donde el propietario del vehículo es la misma persona que está manejando su propio vehículo y que está ingresando o saliendo de la institución por alguno de los acceso, de esta manera se encuentra detallado el esquema general del sistema, que se puede apreciar en la figura 2-2.

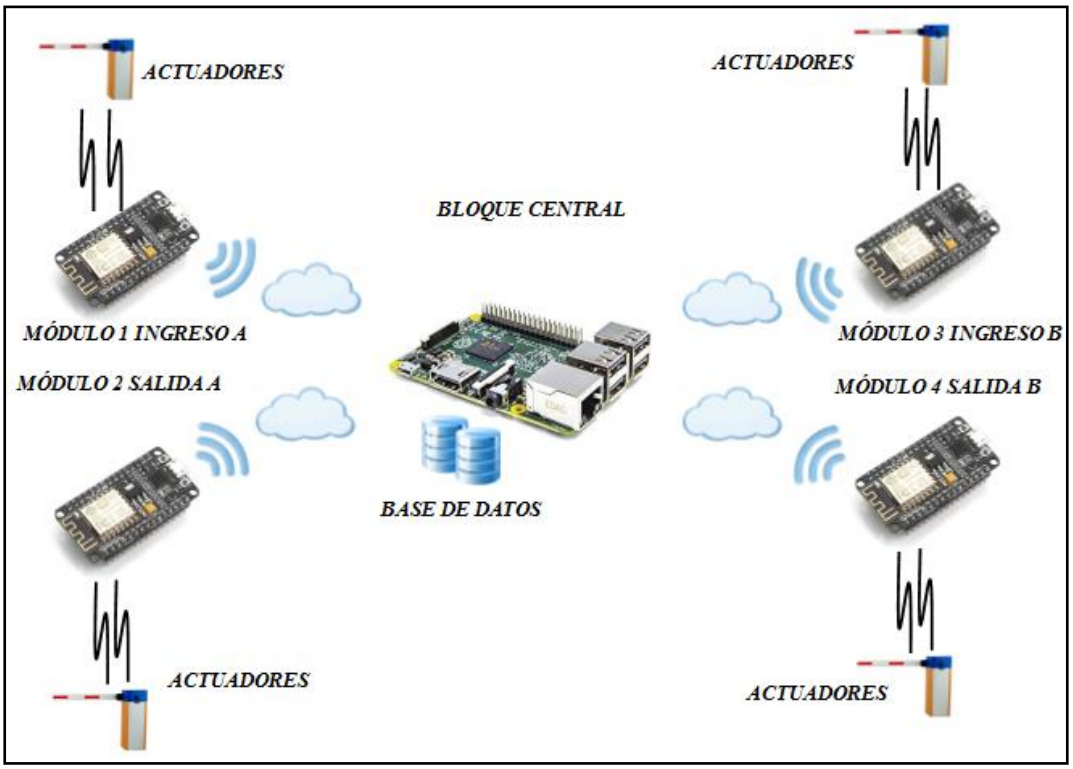


Figura 2-2: Esquema de la concepción general del sistema

Realizado por: *Omar Delgado, 2018*

El sistema está constituido por cuatro módulos y un bloque central: los módulos 1 y 3 de ingreso vehicular se encargan de la lectura, identificación, de los usuarios también del control

de los actuadores y envió de la información a través de internet para conectarse con el bloque central.

Los módulos 3 y 4 de salida vehicular se encargan de igual manera de la lectura y envió de información, para así tener un control tanto de ingreso como de salida de los vehículos en una base de datos almacenada en un servidor.

Los módulos de ingreso y salida cuentan con bloques de lectura los cuales son los encargados de recolectar información de usuarios, después pasa por el bloque de identificación donde se reconoce si el usuario es autorizado o no es autorizado dando paso al bloque de envió de información y la acción de lo actuadores o dispositivos finales.

La información enviada por los módulos es recolectada en el bloque central donde se procesa y almacenada los datos enviados por cada módulo, estos datos son almacenados para su posterior visualización en una base de datos alojada en un servidor.

2.4 Análisis comparativo de tecnologías de implementación

2.4.1 Tecnologías inalámbricas

Una vez se ha realizado el análisis de cada tecnología de comunicación inalámbrica de manera individual se procede a comparar las características más relevantes en la tabla 2-1.

Tabla 2-1: Comparación de tecnologías de comunicación inalámbrica

	Tasa de Transferencia	**Frecuencia de trabajo**	**Distancia**	**Ventajas**	**Desventajas**
Bluetooth clase 2	0.125Mbps	2.4Ghz	1m – 10m	Costo	Velocidad
ZigBee 1.0	0.25Mbps	2.4Ghz	10 - 100m	Bajo consumo	Velocidad
Wi-Fi 802.11 g	54Mbps	2.4Ghz o 5Ghz	100m	Velocidad	Costo
WiMax 802.16 e	80Mbps	2Ghz – 11Ghz	50Km	Velocidad	Costo

Realizado por: Omar Delgado B., 2018

Para evaluar los sistemas de identificación se utiliza la escala de Likert, donde es usada una ponderación de 1 a 5 estableciendo un nivel de eficiencia de las características de cada sistema, en la tabla 2-2 se puede apreciar la valoración usada. (Malhotra, 2004, p. 258)

Tabla 2-2: Escala de ponderación de Likert 1

1	2	3	4	5
Ineficiente	Nada eficiente	Poco eficiente	Eficiente	Muy eficiente
0%	1 – 25%	26 – 50%	51 – 75%	76 – 100%

Realizado por: Omar Delgado B., 2018

Para realizar el cálculo de la ponderación se utiliza la siguiente formula donde se calcula la ponderación de cada sistema evaluado para así conocer la eficiencia final de cada tecnología.

$$P = \frac{\sum Ni}{\text{Ti}} * 100\%$$

Donde:

P = La ponderación de cada sistema.

Ni = Nivel de incidencia de las características evaluadas.

Ti = El total de las incidencias.

Tabla 3-2: Ponderación de las tecnologías inalámbricas

	Nivel de Incidencia			
Característica	Bluetooth	ZigBee	Wi-Fi	WiMax
Velocidad transferencia	1	2	4	3
Frecuencia de operación	3	4	4	4
Alcance	1	2	3	4
Consumo	2	5	5	4
Costo	5	5	4	3
Total de Incidencias	12	18	20	18
Ponderación de Eficiencia	48%	72%	80%	72%

Realizado por: Omar Delgado B., 2018

Basándose en lo datos de la tabla 3-2, se decidió utilizar la tecnología Wi-Fi para el prototipo,

debido a que su ponderación de eficiencia es la más alta de todas con un 80%, ya que la velocidad de transferencia y alcance son los que más se adecuan para el prototipo además que una de sus características interoperabilidad es de ayuda con la compatibilidad de diferentes dispositivos.

Al ser seleccionada la tecnología WiFi por sus características que se adecuan al sistema, además de tener la posibilidad de utilizar los recursos wireless que cuenta la institución como las redes wi-fi eduroam y ESPOCH-PORTAL, se cuenta con flexibilidad, confiabilidad y seguridad al utilizar este recurso.

2.4.1.1 Tecnología inalámbrica Wi-Fi EDUROAM y ESPOCH-PORTAL

La ESPOCH cuenta con redes inalámbricas (Wi-Fi) que cubren en su totalidad la institución según el DTIC (Departamento de Tecnologías de la Información y Comunicación), para hacer uso de las mismas es necesario ser parte de la institución pues las credenciales personales son usadas para ingresar, las redes que se encuentran disponibles en todo el campus de la ESPOCH son: EDUROAM y ESPOCH-PORTAL. (DTIC, 2017b)

Brindan un servicio que permite movilidad tanto local como mundial de conectividad inalámbrica, desarrollado para la comunidad de investigación y académica, gracias a este servicio los integrantes de la institución (estudiantes, investigadores y personal administrativo) pueden tener conectividad e internet dentro del campus y cuando visiten otras instituciones.

Entre las instituciones del Ecuador que utilizan el servicio EDUROAM están: Universidad de Cuenca, Universidad Particular de Loja, Universidad de las Fuerzas Armadas, Escuela Politécnica Nacional, Universidad Central del Ecuador, Universidad Técnica de Ambato, Escuela Superior Politécnica del Litoral, Universidad Politécnica Salesiana entre otras (DTIC, 2017a).

Para la conectividad wireless entre los módulos del prototipo de control de acceso vehicular tanto de ingreso como de salida se lo realiza a través de las redes utilizables de la institución debido a su disponibilidad (24/7) y cobertura.

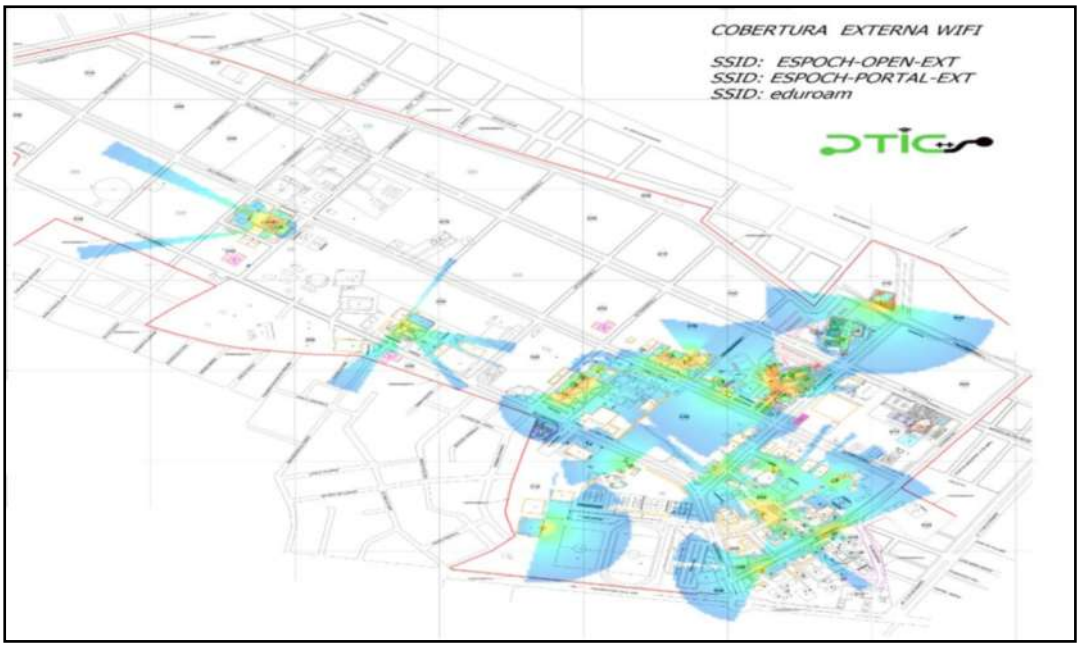


Figura 3-2: Mapa de cobertura de las redes de la ESPOCH

Fuente*: *http://redes.espoch.edu.ec/index.php/cobertura

2.4.1.2 Intensidad de la redes wireless en el acceso principal

Como se puede apreciar en la tabla 4-2, la red con mayor nivel de intensidad de la señal en la garita del acceso principal es la red eduroam, dicha red es la más adecuada para utilizar en el acceso principal debido a que cuenta con cobertura y su intensidad es de -50dbm que es un nivel excelente e idóneo con tasas de transferencias estables, en la figura 4-2 se puede apreciar con más detalle sus características.

Tabla 4-2: Intensidad de señal de las redes en la garita del acceso principal

Red WiFi	Intensidad	Canal	Equipo	Estándar	Banda	Velocidad
Eduroam	-51dbm	6	Cisco Inc.	802.11.n	2.4Ghz	144.4Mbps
ESPOCH-Portal	-50dbm	6	Cisco Inc.	802.11.n	2.4Ghz	144.4Mbps

Realizado por: Omar Delgado B., 2018

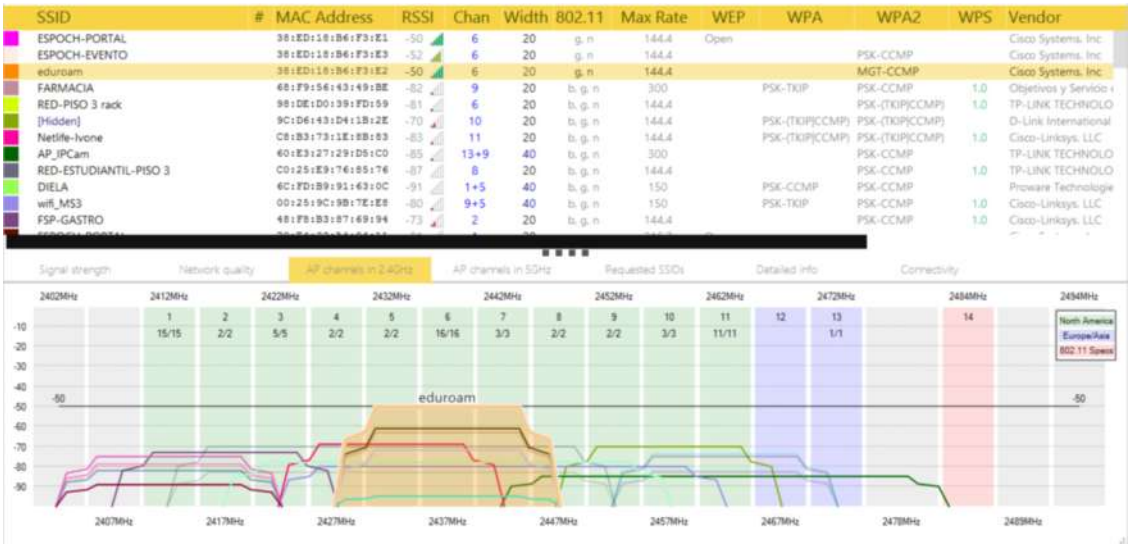


Figura 4-2: Intensidad de señal de las redes en la garita del acceso principal

***Fuente*:** Omar Delgado B., 2018

2.4.1.3 Intensidad de la redes wireless para acceso posterior

Como se puede apreciar en la tabla 5-2, la red con mayor nivel de intensidad de la señal en la garita del acceso posterior es la red ESPOCH-PORTAL, dicha red es la más adecuada para utilizar en el acceso principal debido a que cuenta con cobertura y su intensidad es de -48dbm que es un nivel excelente e idóneo con tasas de transferencias estables, en la figura 5-2 se puede apreciar con más detalle sus características.

Tabla 5-2: Intensidad de señal las redes en la garita del acceso posterior

Red WiFi	Intensidad	Canal	Equipo	Estándar	Banda	Velocidad
Eduroam	-68dbm	11	Cisco Inc.	802.11.n	2.4Ghz	216.7Mbps
ESPOCH-Portal	-48dbm	6	Cisco Inc.	802.11.n	2.4Ghz	216.7Mbps

Realizado por: Omar Delgado B., 2018

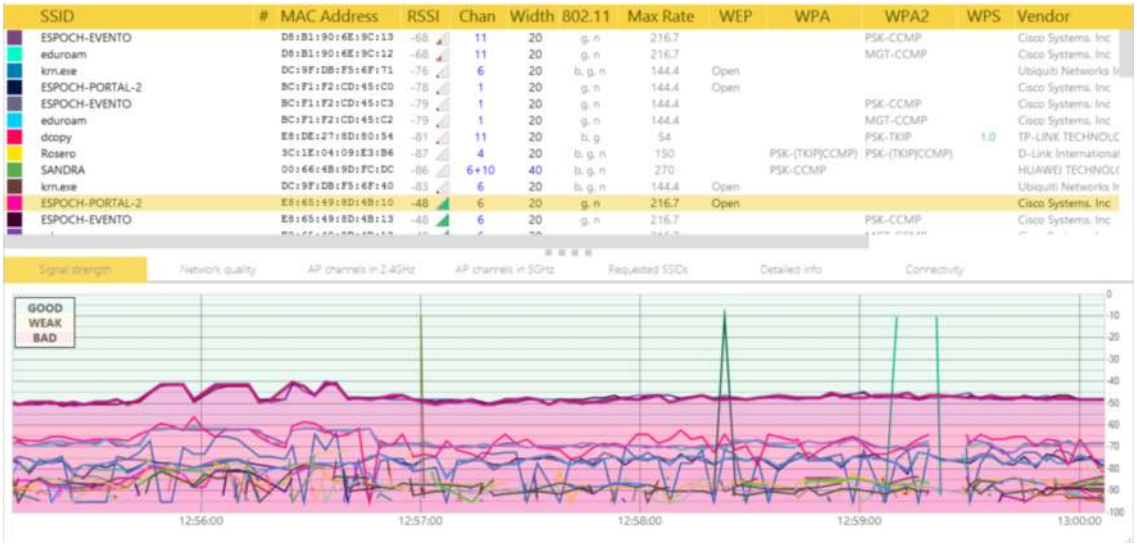


Figura 5-2: Intensidad de señal las redes en la garita del acceso posterior

***Fuente*:** Omar Delgado B., 2018

2.4.2 Sistemas de identificación

Una vez se ha realizado el análisis de cada sistema de identificación de manera individual se procede a comparar las características más relevantes en la tabla 6-2.

Tabla 6-2: Comparación de los sistemas de identificación

	Código de Barras	**Tarjetas Magnéticas**	**Sistemas Biométricos**	**RFID Pasivo**	**RFID Activo**
Precio	Bajo	Medio	Alto	Bajo	Alto
Durabilidad	Corto	Largo	Indefinido	Indefinido	Depende de la batería 3-5 años
Alimentación externa	Si	No	Si	No	Si
Almacenamiento	Lineal (8-30 caracteres)	Hasta 8 MB	No aplica	Hasta 64 KB	Hasta 8MB
Nivel de Seguridad	Ninguno	Medio	Alto	Baja - alta	Alta

Información Modificable	No	Si	No	Si	Si
Línea de vista	Si	Si	Si	No	No
Contacto	No	Si	No	No	No
Distancia de Lectura	Hasta 1.5m	0cm	No aplica	Hasta 1m	Hasta 10m

Realizado por: Omar Delgado B., 2018

De la misma manera utilizando la escala de Likert se calcula la eficiencia de sistema de identificación seleccionada para la comparación y selección a usar.

Tabla 7-2: Ponderación de los sistemas de identificación

Característica	Nivel de Incidencia				
	Código de Barras	Tarjetas Magnéticas	Sistemas Biométricos	RFID Pasivo	RFID Activo
Precio	4	4	1	5	4
Duración	3	3	4	4	3
Almacenamiento	1	1	5	4	4
Nivel de Seguridad	1	3	5	4	4
Distancia de Lectura	2	1	4	4	5
Total de Incidencias	11	12	14	21	20
Ponderación de Eficiencia	44%	48%	56%	84%	80%

Realizado por: Omar Delgado B., 2018

Basado en los datos arrojados por la tabla 7-2 de incidencia se decidió utilizar la tecnología de identificación RFID pasiva en el prototipo, debido a que la ponderación es del 84% ya que nos presenta ahorro de espacio, menor costo, larga duración por la forma de trabajo de las etiquetas.

Al seleccionar la tecnología innovadora RFID por sus características antes mencionadas cabe recalcar su principal ventaja la cual es la escalabilidad debido a que el número de etiquetas y lecturas puede adecuarse a los requerimientos que necesiten ser cubiertos.

2.4.2.1 Sistema de identificación RFID

El sistema de identificación RFID a utilizarse cuenta dos partes fundamentales el lector RC522 que incorpora una antena para la comunicación y las etiquetas que son tarjetas y llaveros que cuentan de la misma manera una antena y un código único de identificación.

Lector RFID (RC522).- Los lectores RFID actualmente es uno de los sistemas más importantes de identificación, debido a su interoperabilidad es reconocida como un dispositivo de recolección de información en el IDE de Arduino, se controla a través del protocolo SPI, gracias a esta funcionalidad es compatible con casi todos los microcontroladores (Hunt y Puglia, 2007, p. 5). Sus características más importantes:

- Frecuencia de trabajo 13,56Mhz
- Alimentación 3,3 V – 30mA
- Velocidad de transmisión 10Mbps
- Dimensiones 40 x 60 mm
- Distancia de Lectura 0 a 60mm

Anexo C

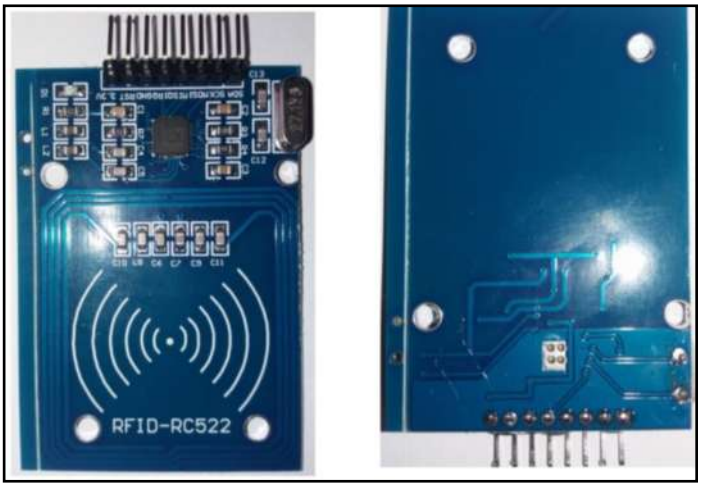


Figura 6-2: Lector RFID RC522C

Fuente*: *Omar Delgado B., 2018

Etiqueta RFID

Las etiquetas seleccionadas que usaran son tarjetas y llaveros pasivos que trabajan en alta frecuencia (HF) de 13,56 MHz debido a que no necesitan alimentación interna debido a que la

lectura y envió de datos se los hace aprovechando el campo magnético provocado al bobinado, cuyas características se acoplan a las del lector RFID antes mencionado como:

- Frecuencia de trabajo 13,56Mhz
- No necesitan alimentación
- Velocidad de transmisión 10Mbps
- Dimensiones 85.5 x 54 x0.84mm
- Distancia de Lectura 0 a 60mm

Figura 7-2: Tag llavero y tarjeta RFID

***Fuente*:** *Omar Delgado B., 2018*

2.4.3 Tarjetas de desarrollo

Una vez se ha realizado el análisis de cada tarjeta de desarrollo de manera individual se procede a comparar las características más relevantes en la tabla 8-2.

Tabla 8-2: Comparación de las tarjetas de desarrollo

	Arduino	**Galileo**	**Raspberry Pi**
Fabricante	Arduino	Intel	Fundación Raspberry Pi
Modelo	Arduino uno R3	Board Intel Galileo	Raspberry Pi 2 modelo B
Procesador	ATMega 328	SoC Quark X100	Broadcom BCM2836 ARM Cortex-A7
RAM	32KB	250MB	1GB
Flash	2KB	8Mb	-
Ethernet	Modulo	10/100	10/100
E/S Analógicas	6	6	-

E/S Digitales	14	14	8
Voltaje operación	5V	3.3V / 5V	3.3V/5V
Voltaje de entrada	5V	5V	7V
USB	-	2	4
Entorno de desarrollo	Arduino IDE	Arduino IDE	Linux, IDLE, QEMU, ECLIPSE, WINDOWS
Procesamiento	16Mhz	400Mhz	900Mhz
S.O.	-	Linux, Windows	Linux, Windows (10)
Precio	$30	$90	$60

Realizado por: Omar Delgado B., 2018

De la misma manera utilizando la escala de Likert se calcula la eficiencia de cada tarjeta de desarrollo seleccionada para la comparación y selección a usar.

Tabla 9-2: Ponderación de las tarjetas de desarrollo

Característica	Nivel de Incidencia		
	Arduino	Galileo	Raspberry Pi
Procesador	3	4	5
RAM	1	3	5
Flash	2	3	1
Ethernet	2	4	4
Costo	5	4	4
Total de Incidencias	13	18	19
Ponderación de Eficiencia	52%	72%	76%

Realizado por: Omar Delgado B., 2018

Con los datos de la tabla 9-2 se obtiene que la tarjeta de desarrollo utilizada para el prototipo realizado es Raspberry pi por su ponderación de eficiencia de 76% debido a su bajo costo, prestaciones, el entorno de desarrollo más amigable, y debido a su popularidad existe una amplia gama de documentación tanto bibliográfica como de ejemplos ideal para realizar aplicaciones de bajo consumo y larga duración.

Al seleccionar la tarjeta de desarrollo raspberry pi por sus características antes mencionadas cabe recalcar su principal ventaja la cual es poseer la facilidad de creador servidores en un lenguaje nativo de programación propio debido a que sus distribuciones son de código abierto.

2.4.3.1 Tarjeta de desarrollo Raspberry Pi 2 B

Es una placa de desarrollo considerada una de las mejores en relación calidad precio, la placa se lo utilizo como un pequeño ordenador el cual dispone de sistemas operativos basados en distribuciones Linux de código abierto, de los cuales se escoge Raspbian debido a que es la distribución que cuenta con actualizaciones constantes.

En este modelo el núcleo del sistema operativo se ha mantenido la compatibilidad con versiones anteriores y actualizado para aprovechar el máximo la última tecnología ARM (Advanced RISC Machine – Maquina Avanzada RISC) RISC (Reduced Instruction Set Computer – Ordenador con Conjunto Reducido de Instrucciones) (François, 2016, p. 30). Entre las características más relevantes tenemos:

- Memoria RAM 1GB
- Procesador ARM Cortex-A7 (4 núcleos) de 900Mhz
- Conector hembra Ethernet RJ45
- 4 Conectores hembra USB 2.0
- Slot para tarjeta micro SD (Secure Digital – Seguro Digital)
- Alimentación 5V - 600mA
- Sistema Operativo Raspbian

Ver Anexo A

Figura 8-2: Raspberry pi 2 modelo B

Fuente: *Omar Delgado B., 2018*

2.4.4 Módulos de comunicación inalámbrica

Una vez se ha realizado el análisis de cada módulo de comunicación inalámbrica de manera individual se procede a comparar las características más relevantes en la tabla 10-2.

Tabla 10-2: Comparación de los módulos de comunicación inalámbrica

	Pinoccio	**NodeMCU**	**PcDuino**	**BeagleBone**
Fabricante	Indiegogo	Amica	LinkSprite	BeagleBoard
Modelo	Pinoccio	ESP8266	PcDuino 1	BeagleBone Black
Memoria	Tarjeta SD	4MB	1GB	512MB
Terminales	32	30	52	92
Alimentación	5V	3.3V / 5V	3.3V / 5V	3.3V /5V
Wi-Fi Incorporado	No	Si	No	Si
Entorno de Desarrollo	Arduino IDE	Arduino IDE	Arduino IDE	Arduino IDE
Precio	$49	$15	60$	$45

Realizado por: Omar Delgado B., 2018

De la misma manera utilizando la escala de Likert se calcula la eficiencia de cada tarjeta de desarrollo seleccionada para la comparación y selección a usar.

Tabla 11-2: Ponderación de los módulos de comunicación inalámbrica

Característica	Nivel de Incidencia			
	Pinoccio	NodeMCU	PcDuino	BeagleBone
Memoria	1	3	4	4
Numero de terminales	3	3	4	3
Alimentación	2	4	4	4
Wi-fi inc.	1	5	1	5
Costo	2	5	1	2
Total de Incidencias	9	20	14	18
Ponderación de Eficiencia	36%	80%	56%	72%

Realizado por: Omar Delgado B., 2018

De la tabla 11-2 se obtuvo que el módulo de comunicación inalámbrica ideal para el uso en la implementación del prototipo sea NodeMCU por su ponderación de eficiencia de 80%, debido a su bajo consumo de energía, su número de terminales abastece en su totalidad, no existe un desperdicios en los recursos al elegir esta plataforma además el precio es conveniente.

Al seleccionar módulo de comunicación inalámbrico se cuenta con la posibilidad de ser programado en el IDE Arduino debido a que es compatible con el mismo lenguaje de programación además de contar con un chip wi-fi integrado a la misma placa.

2.4.4.1 Módulo de comunicación inalámbrica NodeMCU

La tarjeta NodeMCU debe su popularidad a su característica propia de poseer un chip Wi-Fi integrado en su placa, lo que provee de versatilidad a un mundo de variedad de aplicaciones, en el prototipo es utilizada para él envió de información a través de internet (Kurniawan, 2015, p. 67). Sus principales características:

- Memoria 4MB
- Chip Wi-Fi integrado (802.11b/g/n)
- 13 Terminales digitales (D0 – D12)
- 1 pin analógico (A0)
- Alimentación 5V – 50 mA
- Entorno de programación IDE Arduino

Ver Anexo B

Figura 9-2: Placa NodeMCU v2.

***Fuente*:** *Omar Delgado B., 2018*

Para el prototipo realizado se seleccionaron los dispositivos y tecnologías más adecuados para el sistema propuesto, se pueden apreciar en la tabla 12-2 donde basándose en las características como: escalabilidad, confiabilidad, seguridad y confiabilidad se asegura que cumpla los requerimientos que debe cumplir el sistema de acceso vehicular SAVEO.

Tabla 12-2: Resumen tecnología, tarjeta, módulo seleccionados

Tecnología	Sistema de Identificación	Tarjeta de desarrollo	Módulo de comunicación inalámbrica
Wi-Fi	RFID (pasiva)	Raspberry Pi	NodeMCU

Realizado por: Omar Delgado B., 2018

2.4.5 Elementos electrónicos y mecánicos para la implementación del prototipo

Elementos auxiliares del prototipo.- Son los elementos conocidos como dispositivos finales que son los encargados de realizar una determinada acción entre los dispositivos utilizados en el prototipo tenemos: LCD (Pantalla de cristal líquido), Servomotores, Leds y los dispositivos pasivos resistencias así como también jumpers tanto hembras como machos.

LCD.- Este dispositivo se utilizara para mostrar los mensajes de bienvenida al usuario, dispositivo que se alimenta con 5v, cuenta con una pantalla de 16x2 segmentos y es compatible con la tecnología utilizada. En la figura 10-2 podemos apreciar el lcd.

Servomotor.- Utilizado como dispositivo final también conocido como actuador en el prototipo realizara la acción de barrera vehicular, el modelo utilizado de servomotor (SG90) cuenta con una alimentación de 5V. En la figura 10-2 se puede apreciar el servomotor SG90.

I2C.- Es un módulo (bus controlador) para lcd que está formado por un microcontrolador, un pic y un bus de datos que trabajan como un multiplexado para reducir y optimizar espacio y terminales que son utilizados por las tarjetas programables que usan lcd para mostrar mensajes.

Elementos varios.- Para la elaboración del prototipo se utilizaron varios dispositivos finales como lo son protoboard donde están montados los elementos y dispositivos, resistencias para ofrecer protección a los distintos elementos y dispositivos utilizados y finalmente diodos led que son utilizados como indicadores en el prototipo.

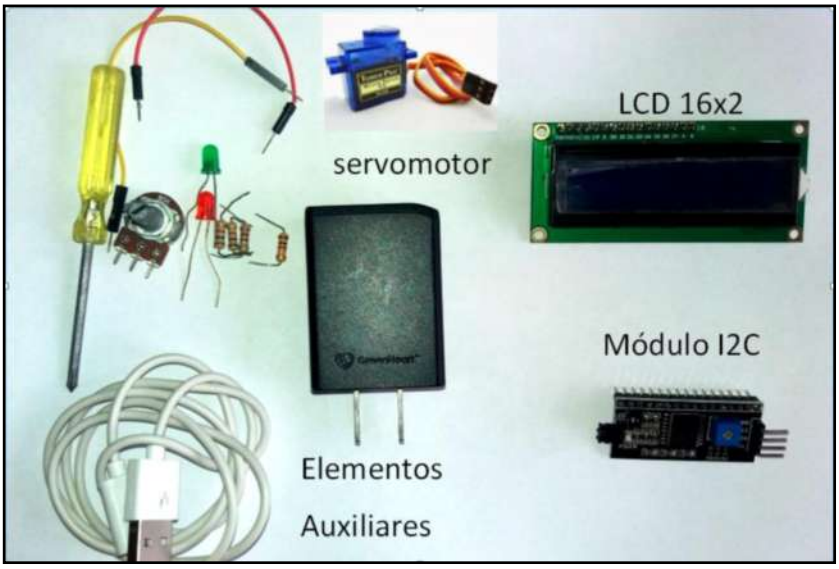


Figura 10-2: Elementos Auxiliares

Fuente*: *Omar Delgado B., 2018

2.5 Diseño general del sistema del control vehicular

Figura 11-2: Bloques general del sistema

Realizado por: Omar Delgado B., 2018

El esquema general del sistema consta de tres bloques, bloque de Entrada, Control y Salida en donde el bloque de Entrada se realiza las funciones recolectar información, procesamiento de la información, identificación de usuario, y transmisión de datos.

Posteriormente el bloque de Control tiene las funciones de recepción de la información, procesamiento de la información y almacenaje de datos para finalmente pasar al bloque de Salida que se encarga de realizar funciones de la misma manera que el bloque de entrada de manera inversa, donde las características del *software* más relevantes utilizadas son las siguientes:

- Sistema Operativo: Raspbian
- Entorno de programación: IDE Arduino
- Servidor Web: Apache
- Gestión de base de datos: phpMyAdmin
- Lenguaje de Programación: PHP (Hypertext Processor – Procesador de Hipertexto)

Después de haber estudiado la tecnología seleccionada para la implementación del prototipo se procede al diseño de los subsistemas.

2.5.1 Mecanismo de Entrada

El mecanismo consta de la recolección de información del usuario que ingresa sale de la institución el mismo que es registrado en la base datos y se procesa la información a través del identificador asignado comparándola y permite el acceso.

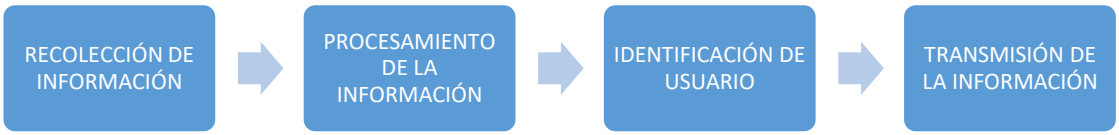


Figura 12-2: Bloques del mecanismo de entrada

Realizado por: Omar Delgado B., 2018

Este proceso se realiza a través de la utilización del lector RFID que es la parte encargada de recolectar los datos que tenga almacenada la etiqueta, el siguiente bloque de procesamiento e identificación está formado por el NodeMCU que realiza la identificación y el procesamiento de la información para su posterior envío a través de internet vía wireless, los elementos utilizados en el bloque de entrada se puede apreciar de la misma manera en la figura 13-2.

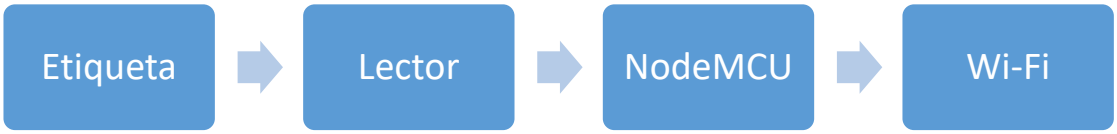


Figura 13-2: Bloques de dispositivos del mecanismo de entrada

***Realizado por*:** *Omar Delgado B., 2018*

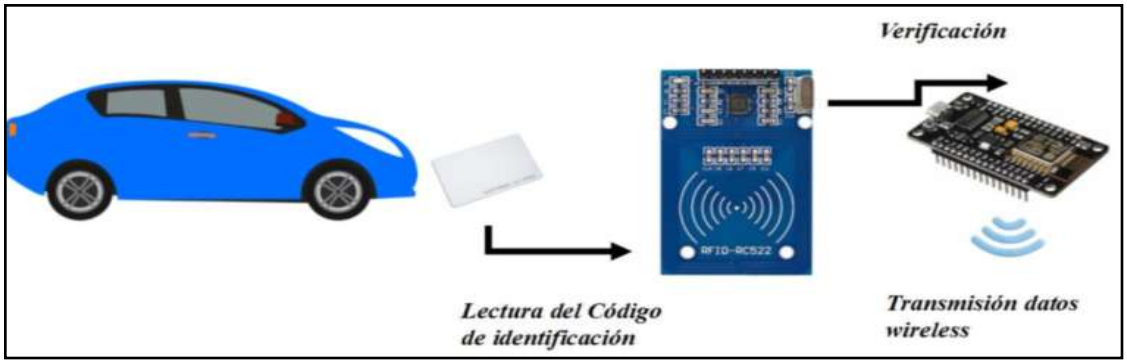


***Figura 14-2*:** Esquema del diseño del mecanismo de entrada

Realizado por: *Omar Delgado B., 2018*

En la etiqueta se almacenan los datos, como el código único de identificador y otros datos necesarios para poder leer el código identificador, posterior se realiza la lectura de los datos, el lector está conectado directamente al módulo de comunicación inalámbrica con el cual se transmitirán los datos por wi-fi.

El algoritmo del mecanismo de entrada está representado por el diagrama de flujo que se puede apreciar en la figura 15-2 donde pasa ciertos pasos secuenciales como:

- Localizar la red wi-fi a través del NodeMCU
- Conectarse a la red wi-fi a través del módulo NodeMCU

- Detectar la disponibilidad del lector RFID
- Mensaje de espera a una tarjeta
- Detectar correctamente la tarjeta
- Conectar con el servidor
- Enviar los datos a través de wireless

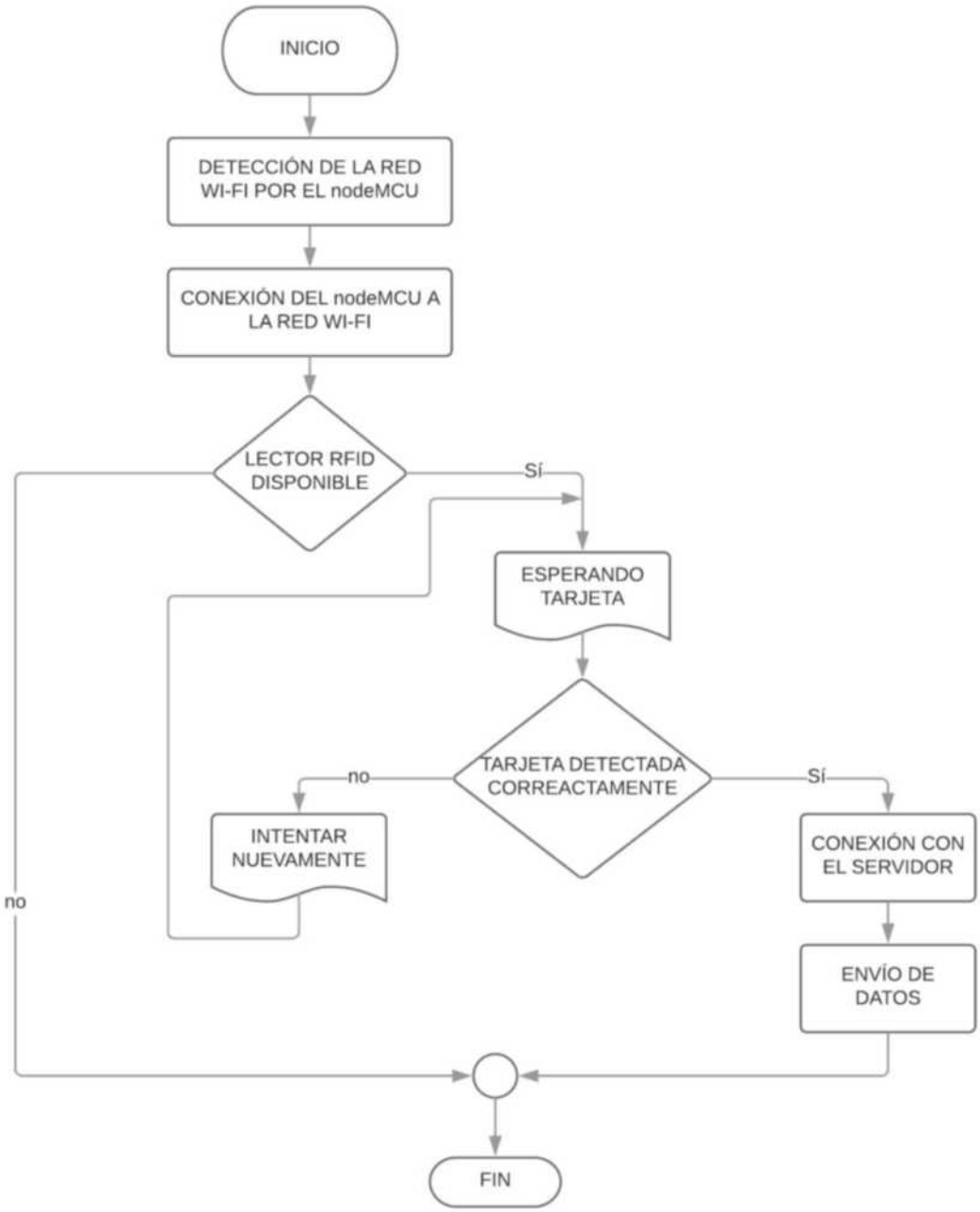


Figura 15-2: Diagrama de flujo del mecanismo de entrada

***Realizado por*:** *Omar Delgado B., 2018*

2.5.2 Mecanismo de Control

La función principal del mecanismo de control es la recepción de la información, la verificación de los campos que se encuentren correctos para su posterior procesamiento y almacenaje.

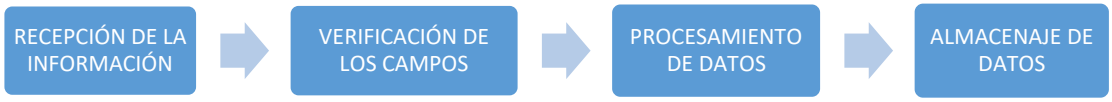


Figura 16-2: Bloques de dispositivos del mecanismo de control

Realizado por: Omar Delgado B., 2018

La recepción de la información se lo hace a través de internet por medio de un servidor apache creado a través de la tarjeta de desarrollo Raspberry pi, donde se realiza el procesamiento de los datos receptados y finalmente la información sea almacenada en la base de datos, donde se puede realizar búsquedas en base a su identificador, fecha, u hora.

Los elementos utilizados en los bloques del mecanismo de control se pueden apreciar en la figura 17-2 donde cada etapa es representada por los elementos que se utiliza.

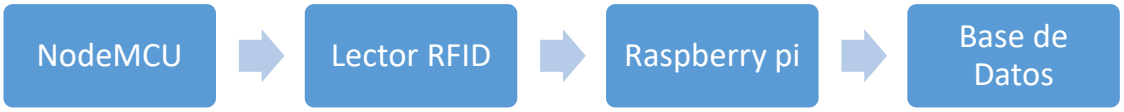


Figura 17-2: Bloques de dispositivos del mecanismo de salida

Realizado por: Omar Delgado B., 2018

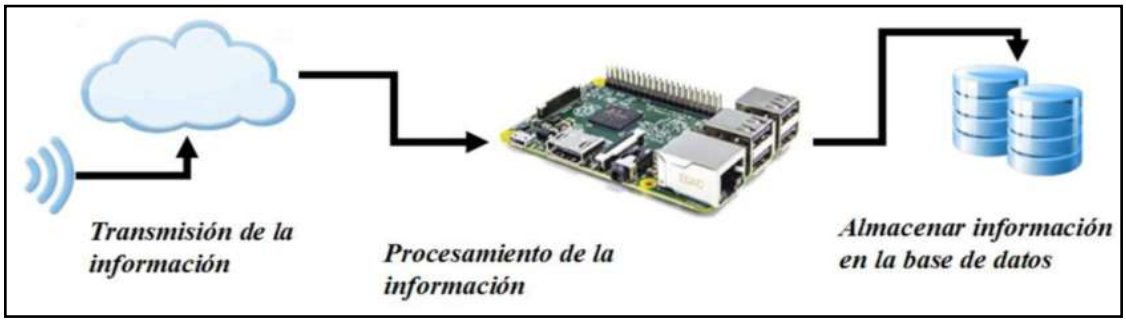


***Figura 18-2*:** Esquema del diseño del mecanismo de control

Realizado por: *Omar Delgado B., 2018*

EL proceso para almacenar los registros se lo hace estableciendo conexión con el servidor luego se realiza la búsqueda de la base de datos y finalmente se encuentra la tabla de usuarios para almacenar los registros y se guarda la información.

El algoritmo del mecanismo de control es representado por el diagrama de flujo se puede apreciar en la figura 19-2 pasa ciertos pasos secuenciales:

- Conectar a internet
- Iniciar el servidor
- Detección de página establecida
- Comparación de campos correctos (user, pass, base de datos)
- Búsqueda de la base de datos ‘usuarios’
- Almacenaje de los registros en la base de datos.

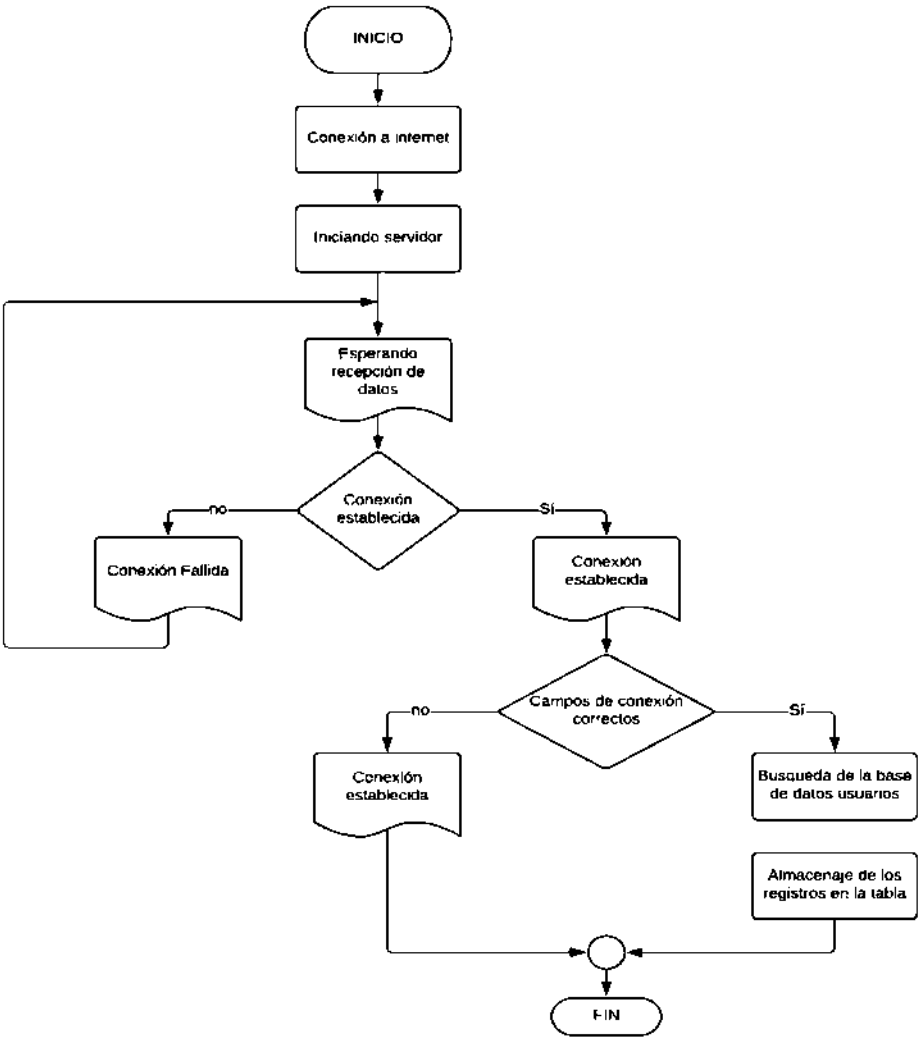


Figura 19-2: Diagrama de flujo del mecanismo de control

***Realizado por*:** *Omar Delgado B., 2018*

2.5.3 Mecanismo de Salida

El bloque de salida primero realiza la transmisión de la información y la identificación con la ayuda del módulo de comunicación inalámbrica NodeMCU, el procesamiento de la información por medio de la raspberry pi que tiene alojado una base de datos en su servidor, para finalmente activar los actuadores que darán acceso (barra de acceso vehicular).

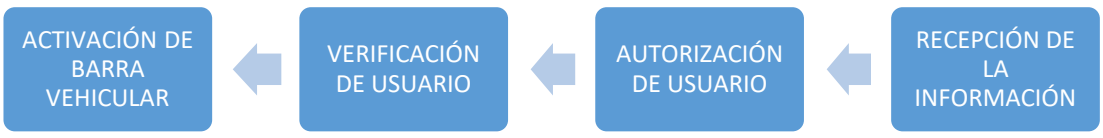


Figura 20-2: Bloques del mecanismo de salida

Realizado por: *Omar Delgado B., 2018*

El bloque del mecanismo de control es representado en la figura 20-2 donde se puede apreciar los bloques formados por los dispositivos constitutivos para realizar las tareas del bloque de salida para finalmente activar la barrera vehicular así dando paso al vehículo que ingrese o salga por el acceso usado.

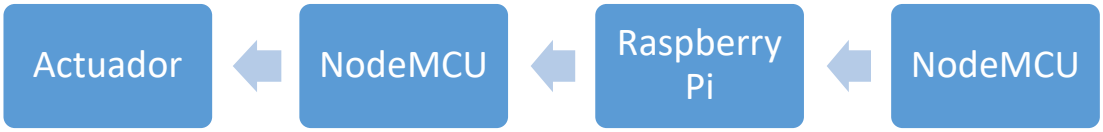


Figura 21-2: Bloques de dispositivos del mecanismo de salida

Realizado por: *Omar Delgado B., 2018*

Como se puede apreciar el diagrama de bloques cuenta con el dispositivo NodeMCU dos veces utilizado en el mismo bloque de salida debido a que inicialmente recibe la información para luego realizar una comparación con los campos alojados en su código para una posterior aceptación de usuario y activación del actuador.

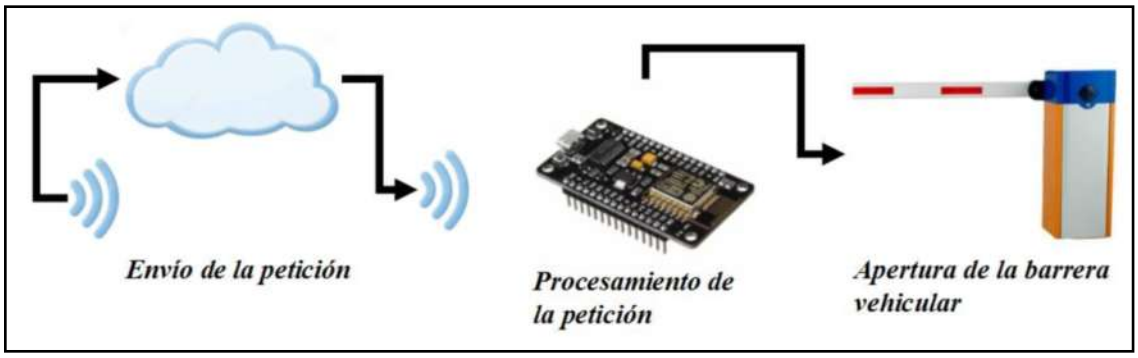


***Figura 22-2*:** Esquema del diseño del mecanismo de salida

Realizado por: *Omar Delgado B., 2018*

El algoritmo del bloque de salida es representado por el diagrama de flujo que se puede apreciar en la figura 23-2 donde pasa ciertos pasos secuenciales como:

- Leer la etiqueta
- Comparar autorización de usuario

- Mensaje de autorización
- Verificar tipo de usuario
- Mensaje de bienvenida o salida
- Activación de barrera vehicular
- Detección de vehículo
- Desactivación de la barrera

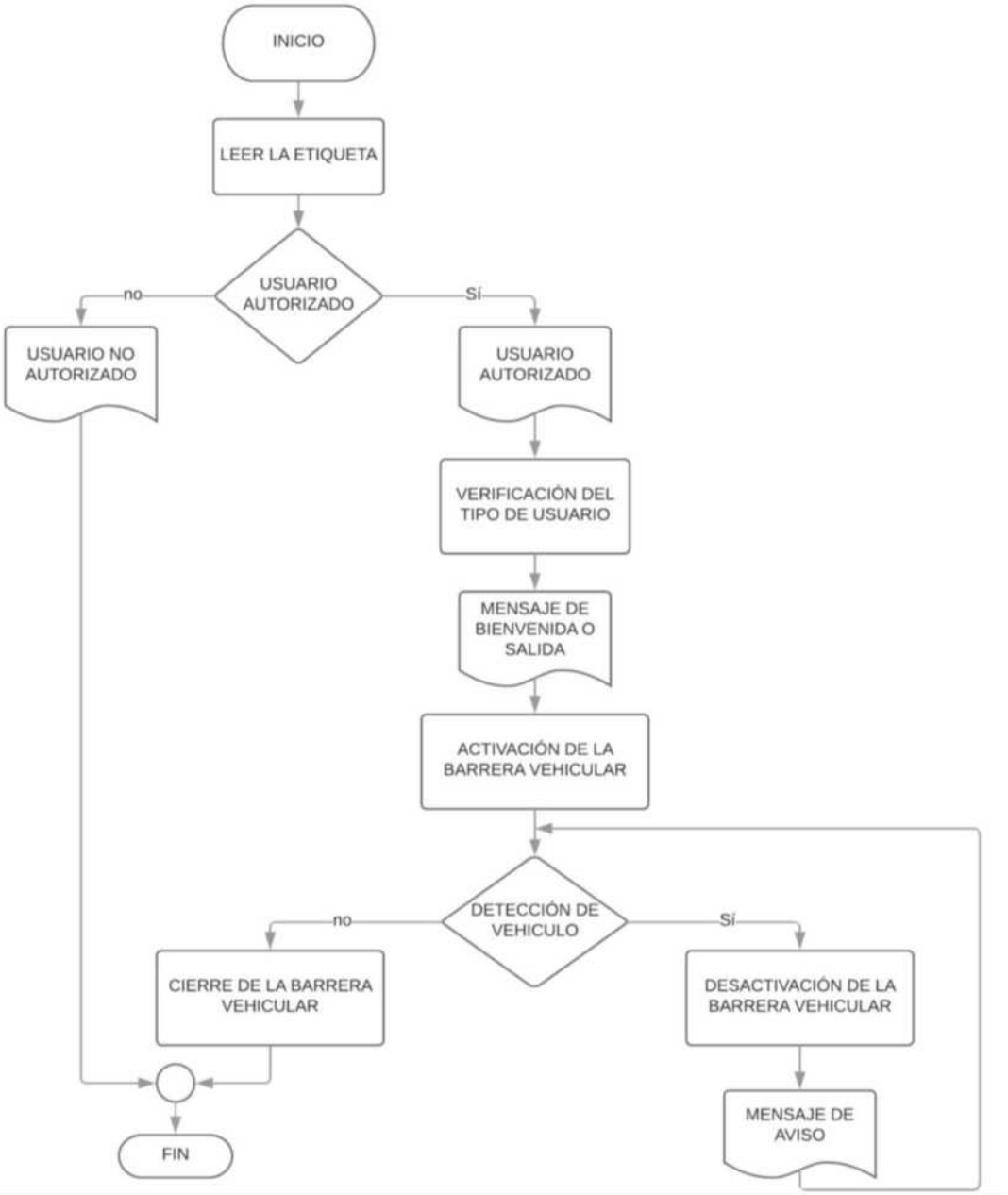


Figura 23-2: Diagrama de flujo del mecanismo salida

***Realizado por*:** *Omar Delgado B., 2018*

2.4 Diagramas de conexión física

De las topologías expuestas que se ajusta de mejor manera al sistema es la estrella debido a que los módulos están conectados directamente con un nodo central en este caso la raspberry pi y todas las comunicaciones realizadas lo harán a través de este, los módulos no están conectados entre sí, es decir comunicaciones punto a punto, cada módulo toma el rol de esclavo.

El servidor tiene comunicación half dúplex con los módulos tanto como para establecer comunicación así como también para almacenar la información en la base de datos, a continuación se pueden apreciar las conexiones físicas entre los dispositivos.

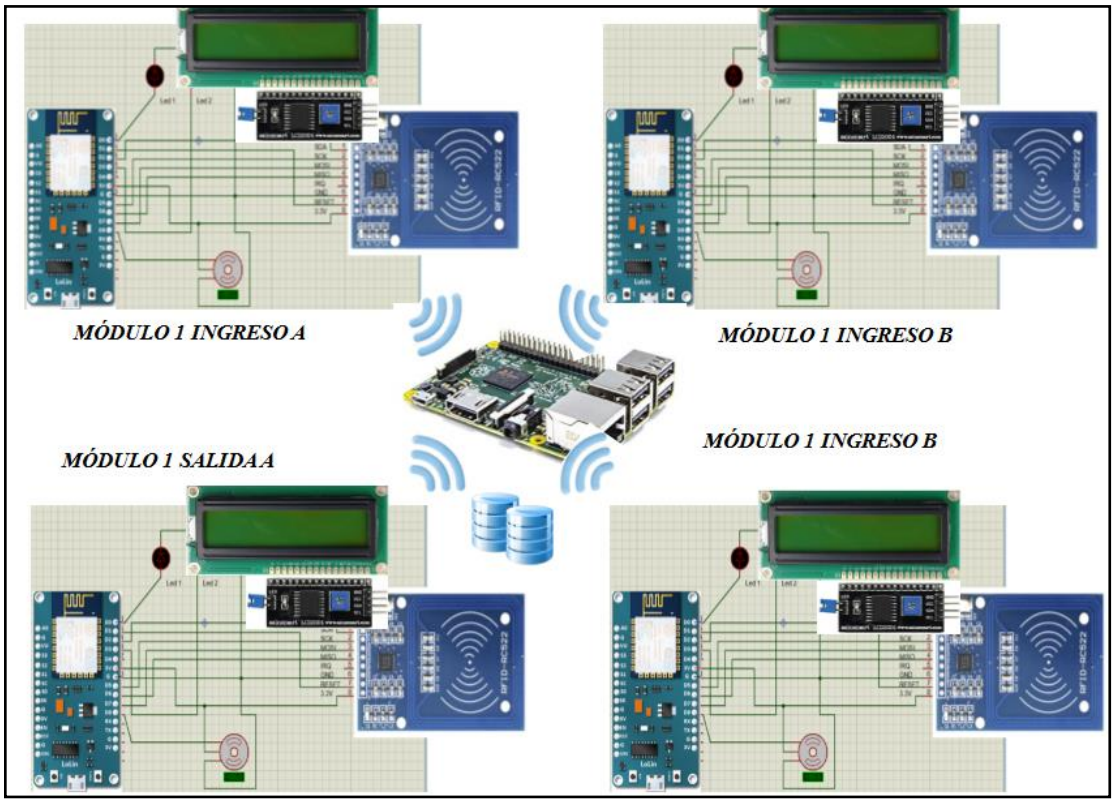


Figura 24-2: Conexión de los módulos de ingreso y salida

Realizado por: *Omar Delgado B., 2018*

Las conexiones física que se debe realizar entre el modulo lector el NodeMCU y los dispositivos finales se puede observar en las siguientes tablas, donde están conectados de la siguiente manera:

- El sensor de radiofrecuencia RFID se encuentra conectado con el NodeMCU como se observa en la tabla 13-2, donde es alimentado a través del USB 5V, el cual es utilizado para los cuatro módulos.

Tabla 13-2: Conexión del lector RFID con el módulo NodeMCU

Terminal NodeMCU	Terminal Módulo RFID
D2	SDA
D5	SCK
D7	MOSI
D6	MISO
-	IRQ
GND	GND
D1	RST
3.3V	3.3V

Realizado por: Omar Delgado B., 2018

- La conexión de los terminales entre el módulo I2C y el LCD (16x2) para visualizar los mensajes hacia el usuario se puede apreciar en la tabla 14-2.

Tabla 14-2: Conexión del módulo I2C con el LCD 16x2

Módulo I2C	**LCD**
VSS	VSS
Reset	VDD
CS	V0
RD	RS
WR	RW
Clock	E
DB0	D0
DB1	D1
DB2	D2
DB3	D3
DB4	D4
DB5	D5

DB6	D6
DB7	D7
Vin	A
Ground	K

Realizado por: Omar Delgado B., 2018

- Los indicadores led, lcd se conectan hacia el NodeMCU en los terminales D0, D3 y D4 respectivamente la señal para el servomotor será utilizada en el terminal D8 y alimentados respectivamente con 5V.

Tabla 15-2: Conexión del bus controlador I2C con el módulo NodeMCU

Terminal NodeMCU	Terminal Módulo RFID
SDA	D4
SCL	D3
VCC	Vin
GND	GND

Realizado por: Omar Delgado B., 2018

2.5 Base de datos: Diagrama Entidad-Relación

En la figura 25-2 se puede apreciar la organización del diagrama de base de datos usada para registrar los datos de los usuarios y de los vehículos que ingresan a la institución, las relaciones existentes en las tablas son de gran ayuda para tener un mejor control con los datos en el servidor como son el caso del usuario Docente cuyos campos (ID, Cédula, Celular, Facultad, Placa, Modelo, Tipo, hora) pueden ser ocupados para realizar búsquedas de los registros en la tabla de usuarios.

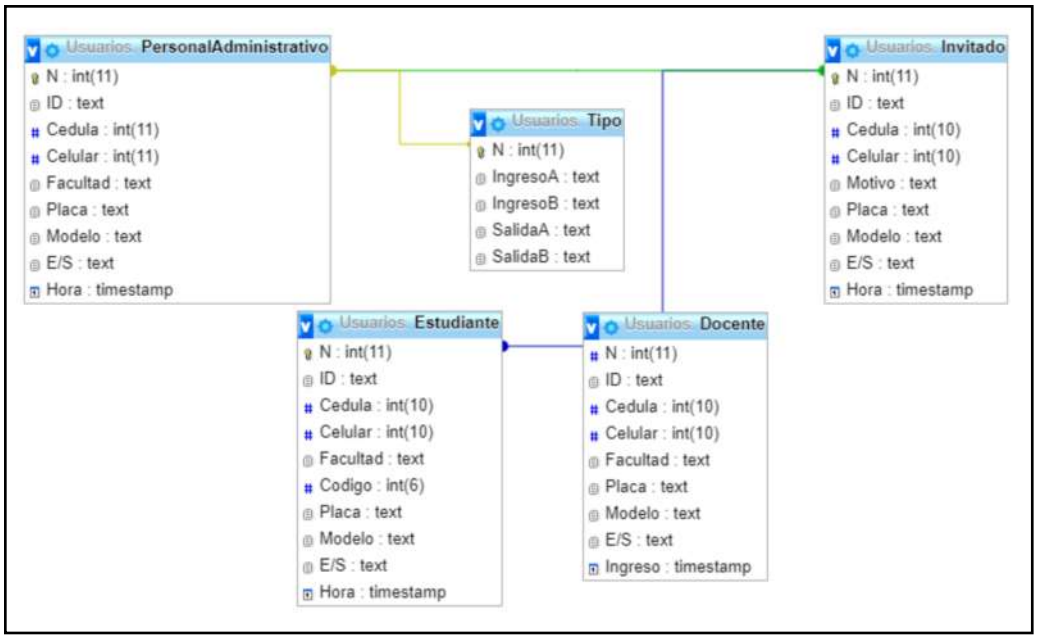


Figura 25-2: Diagrama Entidad-Relación de usuarios

***Fuente*:** Omar Delgado B., 2018

2.6 Herramientas Software

2.6.1 Sistema Operativo Raspbian

Raspbian es una distribución libre de Linux basada a partir del sistema Debian, Raspbian es uno de los sistemas operativos oficiales soportados por raspberry pi ofrece una cantidad superior a los 35000 programas compilados tanto de desarrollo como ejecución de aplicaciones dentro de raspberry. (François, 2016, p. 90)

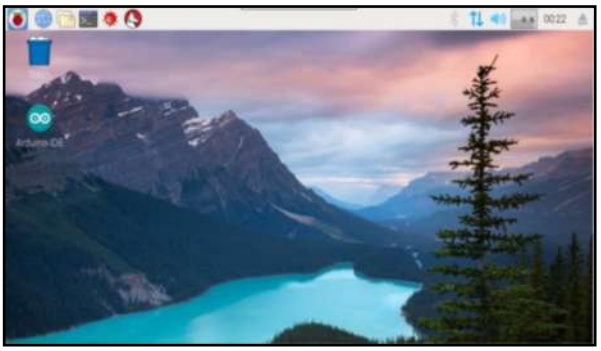


Figura 26-2: Sistema operativo montado en raspberry (Raspbian)

***Fuente*:** Omar Delgado B., 2018

El sistema operativo Raspbian se utilizó para la configuración en la parte del mecanismo de control así como instalación de los *software* lenguaje de programación php para la elaboración de las paginas para establecer comunicación y envió de la información, servidor apache usado para la recepción de las paginas creadas, la base de datos para el almacenaje de los registros y finalmente un gestor para la base de datos a continuación los pasos secuenciales seguidos:

1. Realizar la configuración inicial como zona horaria, teclado, teclado entre otras.
2. Activar el adaptador Ethernet para acceder a internet.
3. Actualizar los programas y sistema desde la línea de comandos.
4. Modificar el fichero de definición de red para establecer una ip estática.
5. Instalar el servidor VNC y el cliente VNC en el equipo para acceso remoto. (opcional)
6. Montar un servidor web usando apache.
7. Instalamos el lenguaje de programación php para crear contenido dinámico.
8. Crear la base de datos de los usuarios.
9. Crear las tablas en la base de datos para guardar los registros.

Ver anexo G

2.6.2 Servidor Apache

Es un programa que transporta los datos de hipertexto, páginas web con todos sus complementos, estos servidores utilizan el protocolo http, están alojados en un ordenador que tiene conexión a internet esperando que algún navegador realiza alguna petición para así responder la petición y enviar un código HTML (Hypertext Markup Language – Lenguaje de Marcas de Hipertexto).

Apatchy Server es completamente libre ya que es un *software* bajo la licencia GPL y de código abierto, puede trabajar con diferentes sistemas operativos sin reducir el rendimiento, también soporta diferentes lenguajes como Perl, PHP, Phyton entre otros (Fulfuts, 2010, p. 16). En las figuras 27-2 y 28-2 se puede observar las pantallas del servidor web apache.

Figura 27-2: Pagina de información de servidor apache

***Fuente*:** Omar Delgado B., 2018

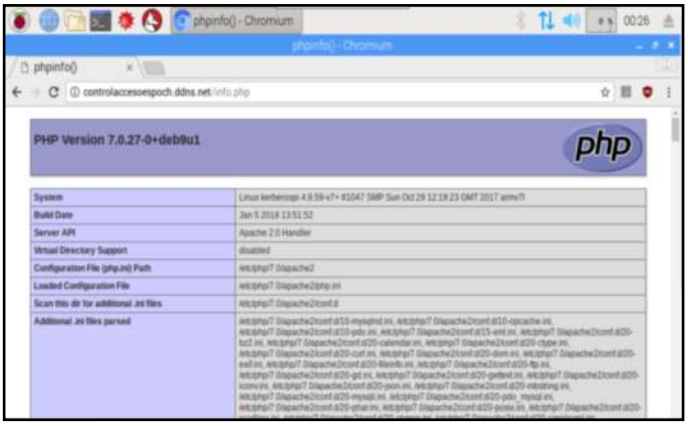


Figura 28-2: Pagina de información características del servidor apache

***Fuente*:** Omar Delgado B., 2018

El servidor web apache se utilizó para la configuración en la parte del mecanismo de control así como la creación de las páginas web para establecer comunicación como para realizar él envió de los datos, a continuación los pasos secuenciales seguidos:

1. Crear una página web para mostrar la página inicial de apache.
2. Crear una página web (info.php) para mostrar las características de la versión de apache.
3. Crear una página web (config.php) para establecer conexión con la base de datos.
4. Crear la página web (users.php) para enviar la información con los datos de los campos para llenar la tabla de registros.

Ver Anexo E

2.6.3 PhpMyAdmin

PhpMyAdmin es la base de datos más popular alrededor del mundo, su fácil uso, confiabilidad, y rendimiento convierten esta base de datos en la principal opción para aplicaciones web cuya administración lo realiza phpMyAdmin que es un *software* de código abierto diseñado para administrar y gestionar los datos.

Mediante la ayuda de una interfaz gráfica, que cuenta con características como navegar, crear modificar las bases de datos mediante tablas, campos e índices; una de las características que posee esta herramienta es la de importar y exportar ya sean base de datos completas o búsquedas realizadas sobre la misma. (Arias, 2015, p. 195)
En la figura 29-2 se puede apreciar el entorno phpMyAdmin para manejar la base de datos.

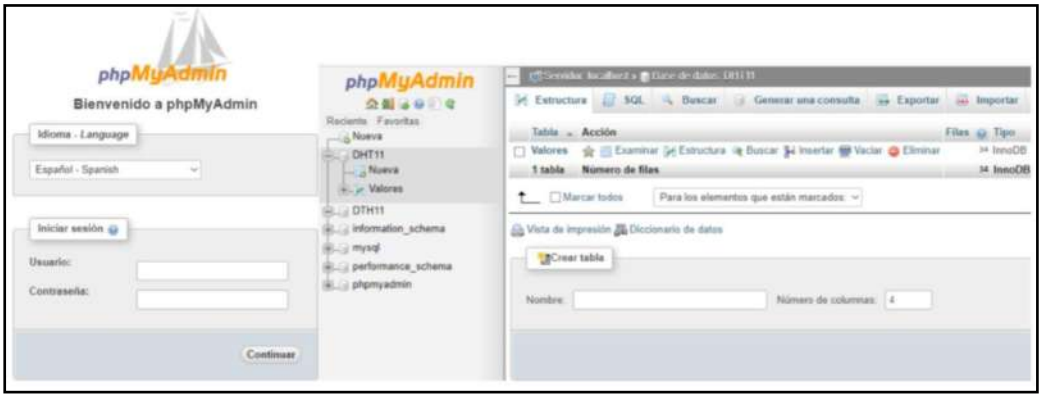


Figura 29-2: Gestor de base de datos phpMyAdmin

***Fuente*:** Omar Delgado B., 2018

PhpMyAdmin es parte del mecanismo de control aquí se crea la base de datos y las tablas para almacenar los datos en los campos de las tablas, de la misma manera se utiliza el gestor de base de datos phpMyAdmin para el ingreso solo por parte del personal administrativo a través de un usuario y contraseña para realizar la manipulación de la base de datos, a continuación los pasos secuenciales seguidos:

1. Colocar un usuario y contraseña para ingresar al gestor.
2. Crear una base de datos nueva.
3. Colocar un nombre a la base de datos (Users).
4. Elegir el tipo de base de datos que se va a utilizar (utl8_general_ci) para introducción de los campos.

5. Guardar la base de datos.
6. Crear las tablas necesarias dentro de la base de datos creada.
7. Colocar los campos que tendrá la tabla y su tipo (id, int, cédula, int, nombre, txt entre otros).
8. Guardar la tabla que se crea.

Ver Anexo F

2.6.4 Software IDE Arduino

Integrated Development Environment (Entorno de Desarrollo Integrado), es un entrono fácil y sencillo de usar de código abierto basado en el lenguaje de programación C++, es multiplataforma es decir soporta variedad de placas de desarrollo disponible en plataformas como: Windows, Mac y distribuciones de Linux.

Este *software* permite la creación, ejecución y desarrollo de una variedad de aplicaciones que una vez escrito el programa se lo cargara a la placa a través del USB, de esta manera permite controlar e interactuar tanto en la parte de *hardware* como en el *software* (Torrente, 2013, p. 127), versión utilizada es 1.8.5.

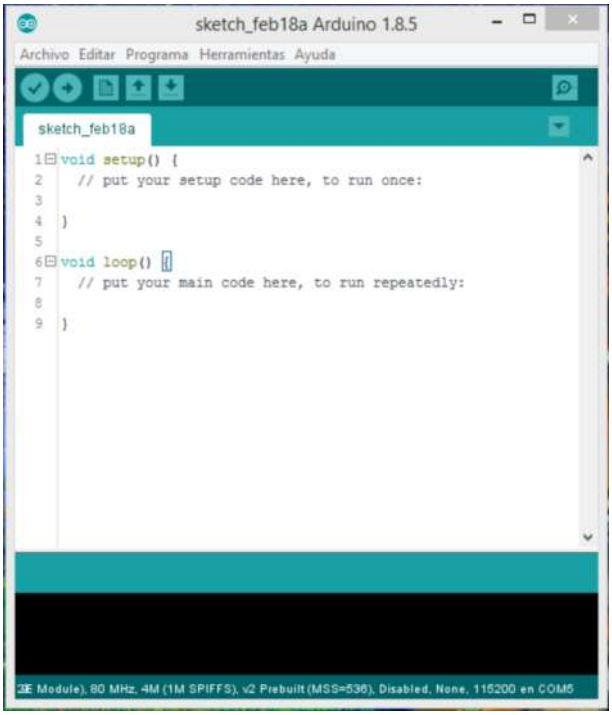


Figura 30-2: Entorno de programación IDE Arduino

***Fuente*:** Omar Delgado B., 2018

El entorno de programación es el IDE de Arduino en el cual podemos realizar la programación a los módulos de comunicación inalámbrica NodeMCU debido a que este *software* cuenta con una variada compatibilidad de placas, para empezar a programar se debe agregar la placa que se va a usar debido a que las placas por defecto del *software* se encuentra instalado.

Para ello se añadir la placa ESP8266 al repertorio de placas, se selecciona el modelo y la velocidad de grabado del programa acto seguido se instalan las librerías necesarias para su correcto funcionamiento y se empieza con la programación, a continuación los pasos secuenciales seguidos:

1. Agregar la placa ESP8266 al entorno IDE de Arduino.
2. Seleccionar el modelo de la placa NodeMCU v2.
3. Seleccionar la velocidad de transmisión por el bus serial (11520).
4. Agregar las librerías utilizadas en el programa (wifi8266, wire, lcd, entre otras)
5. Establecer las variables que serán necesarias su uso posterior (pass, user, url entre otros).
6. Asignar los pines que se conectaran con los demás dispositivos (lector, I2C, servo)
7. Establecer conexión con el servidor.
8. Crear las funciones que serán llamadas en el transcurso del programa (Saludo, Autorizado, No autorizado entre otras).
9. Realizar la programación de cada una de las funciones a utilizar para que ejecuten las acciones que se detallan en la línea de comandos.
10. Activar los terminales y dispositivos que tienen como función dar mensajes de alerta.
11. Realizar la programación sobre el lector RFID para que esté disponible para detectar las etiquetas.
12. Conectar con el servidor para su posterior envió de los campos para el almacenaje en la base de datos.
13. Programar todos las partes necesarias para la comparación, ejecución de los dispositivos conectados a la placa así como también para la ejecución de los dispositivos finales.
14. Llamar a las funciones que sean requeridas para que ejecuten su código programado (mensajes al usuario, activación de la barrera vehicular entre otras).

Ver Anexo D

2.7 Análisis económico del prototipo implementado

En la tabla 16-2 se puede apreciar el presupuesto económico del prototipo implementado, la cual presenta la parte económica de los costos tanto en la parte *hardware* como *software* del prototipo implementado.

Tabla 16-2: Análisis económico del prototipo implementado

	DISPOSITIVO	CANT.	COSTO U. ($ USD)	COSTO T. ($USD)
HARDWARE	Pc Administrador	1	400,00	400,00
	Raspberry Pi 2 B	1	70,00	70,00
	Lector RFID	4	6,00	24,00
	NodeMCU v2	4	11,00	44,00
	Tag (Llaveros)	4	1,00	4,00
	Tag (Tarjetas)	4	1,00	4,00
	IC2	4	5,00	20,00
	LCD	4	6,00	24,00
	Servomotor	4	6,00	24,00
	Cargador	5	10,00	50,00
	Protoboard	4	3,00	12,00
	Elementos Aux.		50,00	50,00
	Varios		80,00	80,00
SOFTWARE	Base de datos		0,00	0,00
	Sistema Operativo		0,00	0,00
	Lenguajes de P.		0,00	0,00
	Servidor web		0,00	0,00
			TOTAL	806,00

Realizado por: Omar Delgado B., 2018

De los valores obtenidos en la tabla 16-2, su puede observar que el costo total *hardware* del prototipo implementado tiene un valor de 806,00$ dólares americanos, que representa un 100% del total de costos y el valor del costo *software* tiene un valor de 0,00$ dólares americanos, que representa un 0% del total de costos, debido a que la los requerimientos de la propuesta fueron encaminados a utilizar *software* de licencia libre.

Lo que conlleva a que los costos netos correspondan a la parte *hardware* donde el mayor porcentaje tiene la PC de administrador con un 49,63%. Del análisis realizado se puede determinar que el costo del prototipo implementado es bajo y cumple con los requisitos de operatividad planteados.

2.8 Análisis económico de SAVEO

En la tabla 17-2 se puede apreciar el presupuesto económico del sistema para ser implementado, la cual presenta la parte económica los costos tanto en la parte *hardware* como *software* para su puesta en marcha.

Tabla 17-2: Análisis económico de SAVEO

	DISPOSITIVO	**CANT.**	**COSTO U. ($ USD)**	**COSTO T. ($USD)**
HARDWARE	Pc Administrador	2	375	750,00
	Raspberry Pi 2 B	1	70,00	70,00
	NodeMCU v2	8	11,00	88,00
	Lector RFID	8	6,00	48,00
	Tags	1671	0,80	1336,80
	Cargador	5	10,00	50,00
	Tablero led	4	60,00	240,00
	Barrera vehicular	8	110,00	880,00
	Elementos Aux.		100,00	100,00
	Varios		200,00	200,00
SOFTWARE	Base de datos		0,00	0,00
	Sistema Operativo		0,00	0,00
	Lenguajes de P.		0,00	0,00
	Servidor web		0,00	0,00
			TOTAL	3762,80

Realizado por: Omar Delgado B., 2018

De los valores obtenidos en la tabla 17-2, su puede observar que el costo total *hardware* de SAVEO tiene un valor de 3762,80$ dólares americanos, que representa el 100% del total de costos y el valor del costo *software* tiene un valor de 0,00$ dólares americanos, que representa el 0% del total de costos, nuevamente recalcando que el valor neto de los costos corresponde a

la parte *hardware* debido a que los requerimientos de SAVEO es utilizar *software* de licencia libre.

Lo que conlleva a que los costos netos correspondan a la parte *hardware* donde el mayor porcentaje tienen los tags con un 35,52% correspondiente a los identificadores de los docentes, personal administrativo y empleados para los estudiantes se puede utilizar los carnets que se les entrega a los estudiantes donde los costos correrán por cada estudiante.

Del análisis realizado se puede determinar que el costo del prototipo implementado es bajo, viable y cumple con los requisitos de control vehicular propuestos por SAVEO.

2.9 Evaluación de la propuesta del sistema de control de acceso vehicular

Para evaluar el sistema de control de acceso vehicular propuesto, se realiza una tabla tomando en cuenta las características más importantes que debe cumplir la propuesta, para ilustrar su evaluación se utiliza otra vez la escala de Likert, donde la ponderación usada se puede apreciar en la tabla 18-2.

Tabla 18-2: Escala de ponderación de Likert 2

1	2	3	4	5
Muy Malo	Malo	Regular	Buena	Muy Buena
0%	1 – 25%	26 – 50%	51 – 75%	76 – 100%

Realizado por: Omar Delgado B., 2018

En base al análisis realizado para optar por la tecnología más adecuada para el sistema propuesto, la experiencia con los dispositivos utilizados, y demás componentes; se procede a realizar la ponderación en la tabla de factibilidad que se puede apreciar en la tabla 19-2.

Tabla 19-2: Ponderación de la propuesta del sistema de control de acceso vehicular

Factores influyentes	**Ponderación (%)**
Disponibilidad	99
Escalabilidad	99
Factibilidad	99
Fiabilidad	99

Realizado por: Omar Delgado B., 2018

En la tabla 19-2 podemos apreciar la ponderación de las características tomadas en consideración, de las cuales se tiene un 99% correspondiente a la disponibilidad debido a que se dispone de la, infraestructura física y recursos necesarios para el funcionamiento de SAVEO.

Escalabilidad con un 99% debido a la posibilidad de extender su capacidad ya que está diseñado con una topología estrella lo que significa que se pueden adicionar módulos al sistema sin ninguna complejidad, un 99% correspondiente a la factibilidad puesto que el diseño del sistema que se planteo es viable asimismo los dispositivos y elementos necesarios para su ejecución son de bajo costo y de fácil adquisición.

SAVEO tiene un 99% de fiabilidad ya que sus propiedades cumplen con la función que fue concebido que es realizar el control de acceso vehicular, puesto que los resultados de ponderación son virtuosos y los beneficios que va a traer a la institución apoyaran la integridad, seguridad de los individuos que la conforman la institución por consiguiente siendo posible su implementación.

CAPITULO 3

3. MARCO DE PRUEBAS Y RESULTADOS

En el presente capitulo se detallan los resultados obtenidos en las pruebas de funcionamiento realizadas al prototipo de control de acceso vehicular, tanto en *hardware* como en *software*. En las pruebas realizadas a las etapas del sistema están: funcionamiento, tiempos de respuesta, latencia, distancia de operación, registro de la base de datos, reportes, y finalmente pruebas de tráfico.

Para la ejecución de las pruebas realizadas tanto en *hardware* y *software* se toma una muestra de 8 usuarios debido a las limitaciones físicas y cuestiones económicas, los usuarios son representados por los docentes de la FIE de forma aleatoria, se tomaron en cuenta dos de los tres accesos debido a que son los que cuentan con estructura física adecuada.

3.1 Etapa de entrada y salida

Se evalúan de igual manera el mecanismo de entrada como el mecanismo de salida debido a que utilizan funciones similares y sus dispositivos usados son los mismos.

El prototipo ha estado en funcionamiento 1600 horas que implica 2 meses 1 semana de continua alimentación eléctrica (5v) y no se visualiza daños físicos por calentamiento, cortocircuitos entre otros, por añadidura de la misma manera no presento fallos el motor que controla la apertura de la barrera. Se considera que las horas en funcionamiento son suficientes para aprobar su corrector diseño, y construcción *hardware* para una disponibilidad del sistema 24/7.

3.1.1 Distancia de operación para la lectura de una etiqueta

Tabla 1-3: Distancia de operación del lector

Distancia (cm)	Tarjeta	Llavero
0.5	Detecta	Detecta
1	Detecta	Detecta

1.5	Detecta	Detecta
2	Detecta	Detecta
2.5	Detecta	Detecta
3	Detecta	No Detecta
3.5	Detecta	No Detecta
4	No Detecta	No Detecta

Realizado por: Omar Delgado B., 2018

Como se puede apreciar en la tabla 1-3 la distancia máxima a la que se puede realizar una lectura adecuada en una tarjeta es de 3.5 cm y en un llavero es de 2.5 cm la diferencia se debe al alcance de la antena emisora debido a los materiales de construcción de las etiquetas (llavero y tarjeta).

3.1.2 Tiempo de encendido bloque central

Tabla 2-3: Tiempo de encendido del bloque central

Encendido (segundos)	43.17	53.51	43.82	52.21	42.1	52.64	42.97	52.83	43.87	50.85
Reinicio (segundos)	38.12	38.84	48.33	38.48	38.57	47.68	37.68	38.22	46.43	37.94

Realizado por: Omar Delgado B., 2018

El bloque central se demora 47.78 segundos la primera vez que es encendido para estar operativo, de manera similar pero con tiempo inferior al de encendido, el tiempo de reinicio es de 41.03 segundos para estar nuevamente operativo.

3.1.3 Tiempo de encendido módulos

Tabla 3-3: Tiempo de encendido de los módulos

Encendido (segundos)	8	8.13	3.81	3.75	7.14	7.85	7.93	7.94	7.79	7.8
Reinicio (segundos)	4.02	1.09	3.95	3.93	3.87	3.88	4.07	3.8	3.87	3.81

Realizado por: Omar Delgado B., 2018

De manera similar los módulos de comunicación inalámbrica toman un tiempo de 7.01 segundos para estar operativo al encenderse, igualmente el tiempo de reinicio es inferior que el de encendido con un tiempo de 3.63 segundos para estar operativo.

3.1.4 Tiempo de paso de un vehículo

Tabla 4-3: Tiempo de paso de un vehículo por el área de control

Encendido (segundos)	8	8.13	6.81	7.75	7.14	7.85	7.93	8.94	9.79	9.8

Realizado por: Omar Delgado B., 2018

Como se muestra en la tabla 4-3 de los datos recolectados de los tiempos necesarios para pasar por el área de control, donde el tiempo promedio de paso vehicular es de 8.21 segundos, tiempo suficiente para que el vehículo pase por la barrera vehicular e ingrese a la institución y el lector este nuevamente operativo para realizar una nueva lectura.

3.2 Etapa de control

De la misma manera la parte *software* del prototipo ha estado en funcionamiento por 1600 horas que implica 2 meses 1 semana y no se presentan daños *software* por falla del sistema operativo, alteración en los tiempos de respuesta, fallos en el envío y recepción de la información entre otros. Estas horas en funcionamiento han sido suficientes para aprobar su corrector diseño, y construcción *software* para una disponibilidad del sistema 24/7.

3.2.1 Registro de lectura

Copy Delete	304	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-02-23	12:13:12
Copy Delete	305	0605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA	2018-02-23	12:14:14
Copy Delete	306	0606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-02-23	12:14:15
Copy Delete	308	0609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoB	2018-02-23	12:32:53
Copy Delete	309	0604675669	Ing.FaustoCabrera	FIE	MAZDA	HGF-221	IngresoA	2018-02-23	12:41:32
Copy Delete	310	0607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-02-23	12:48:41

Figura 1-3: Registros en la base de datos

***Fuente*:** Omar Delgado B., 2018

Se puede apreciar en la figura 1-3 los registros generados por el sistema de control vehicular cada registro cuenta con los campos Id, Nombre, Número de cédula, Facultad, Modelo, Placa, Tipo, finalmente la hora en la que realizo el ingreso o salida de la institución.

3.2.2 Búsqueda en la base de datos

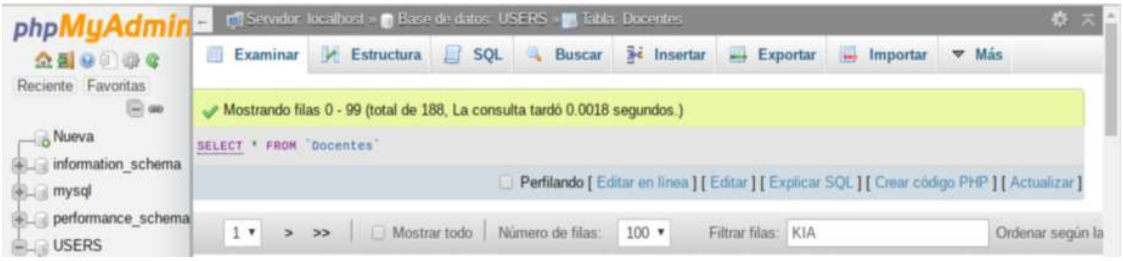


Figura 2-3: Búsqueda por un campo en los registros de la base de datos

***Fuente*:** Omar Delgado B., 2018

Podemos apreciar en la figura 2-3 las opciones de manipulación de la base de datos, donde se puede distinguir la búsqueda que se realiza en la base dato el campo "modelo" (KIA) dando como resultado los registros de los usuarios que tengan el modelo igual a la búsqueda que se puede distinguir en la figura 3-3.

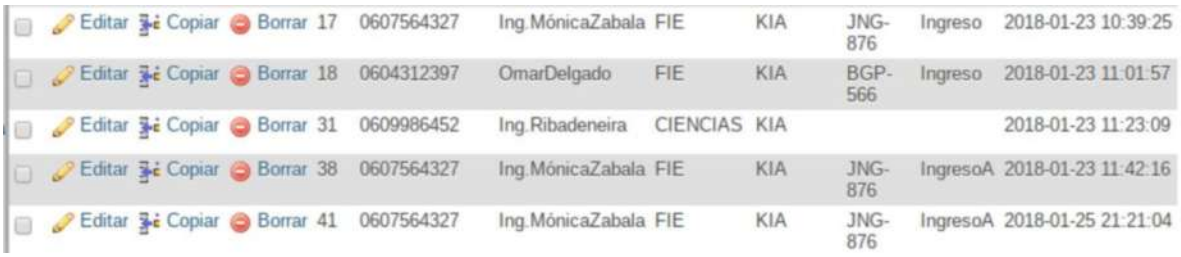


Figura 3-3: Resultado de la búsqueda filtrada por un campo en la base de datos

***Fuente*:** Omar Delgado B., 2018

3.2.3 Latencia generada hacia el servidor

Tabla 5-3: Latencia generada hacia servidor

Latencia (ms)	0.125	0.123	0.112	0.122	0.135	0.119	0.134	0.138	0.126	0.158

Realizado por: Omar Delgado B., 2018

Se midió la latencia que tiene la conexión entre el nodo central hacia el servidor alojado en la misma tarjeta de desarrollo, donde los resultados de la inmediatez de la conexión se pueden apreciar tanto en la tabla 5-3 como en la figura 4-3, donde la latencia media es de 0.129 ms este valor significa una excelente latencia debido a que la red ofrece una velocidad de transferencia superior a los 100Mbps.

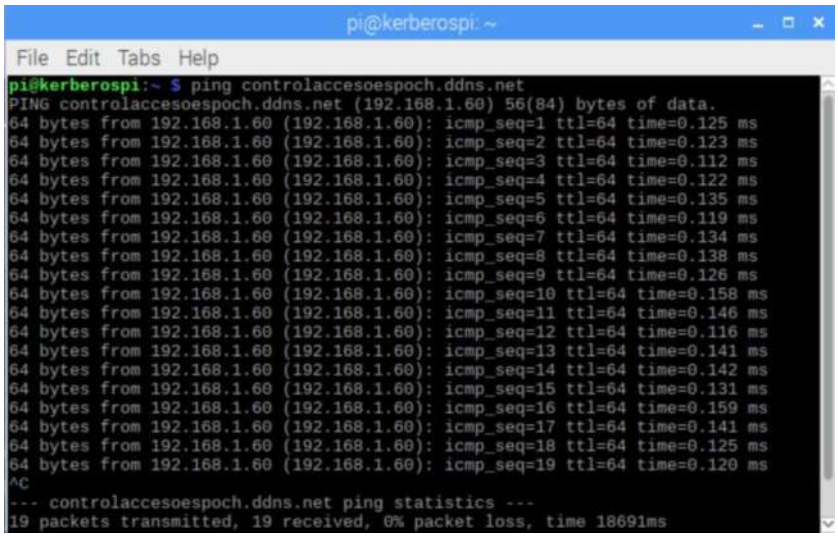


Figura 4-3: Conectividad realizado desde el servidor hacia el servidor

***Fuente*:** Omar Delgado B., 2018

3.2.4 Latencia entre el servidor y los módulos

Tabla 6-3: Latencia generada entre el servidor y el módulo de ingreso A

Latencia (ms)	17.1	7.43	24.2	16.9	8.35	27.0	19.2	11.9	29.7	21.1

Realizado por: Omar Delgado B., 2018

De manera igual se midió la latencia que tiene la conexión entre el módulo de ingreso A hacia el nodo central, donde los resultados de la inmediatez de la conexión se pueden apreciar tanto en la tabla 6-3 como en la figura 5-3, donde la latencia media es de 18.29 ms este valor significa una excelente latencia debido a que la red ofrece una velocidad de la red.

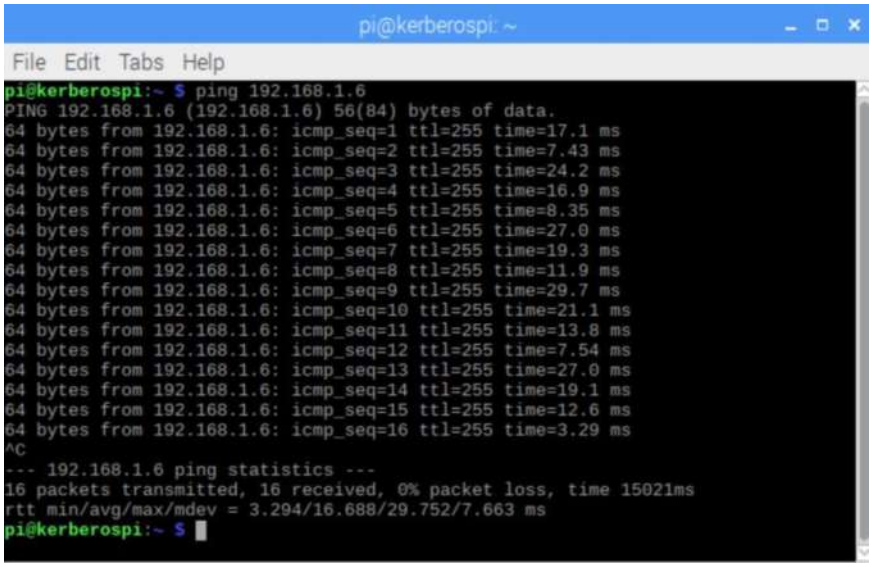


Figura 5-3: Ping realizado desde el servidor hacia el módulo de ingreso A

***Fuente*:** Omar Delgado B., 2018

Tabla 7-3: Latencia generada entre el servidor y el módulo de ingreso B

Latencia (ms)	4.49	22.5	13.2	5.47	23.7	13.1	30.1	21.6	12.5	30.3

Realizado por: Omar Delgado B., 2018

De manera igual se midió la latencia que tiene la conexión entre el módulo de ingreso B hacia el nodo central, donde los resultados de la inmediatez de la conexión se pueden apreciar tanto en la tabla 7-3 como en la figura 6-3, donde la latencia media es de 17.69 ms este valor significa una media latencia debido a que la red ofrece una velocidad de la red.

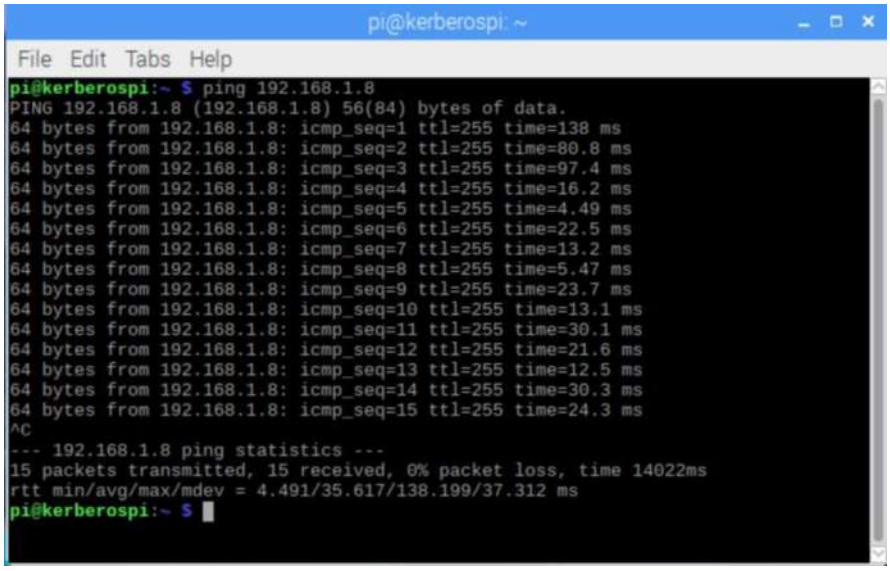


Figura 6-3: Ping realizado desde el servidor hacia el módulo de ingreso B

***Fuente*:** Omar Delgado B., 2018

Tabla 8-3: Latencia generada entre el servidor y el módulo de salida A

Latencia (ms)	19.9	13.2	5.80	25.2	16.5	11.3	27.3	25.3	10.6	5.13

Realizado por: Omar Delgado B., 2018

De manera igual se midió la latencia que tiene la conexión entre el módulo de salida A hacia el nodo central, donde los resultados de la inmediatez de la conexión se pueden apreciar tanto en la tabla 8-3 como en la figura 7-3, donde la latencia media es de 16.02 ms este valor significa una media latencia debido a que la red ofrece una velocidad de la red.

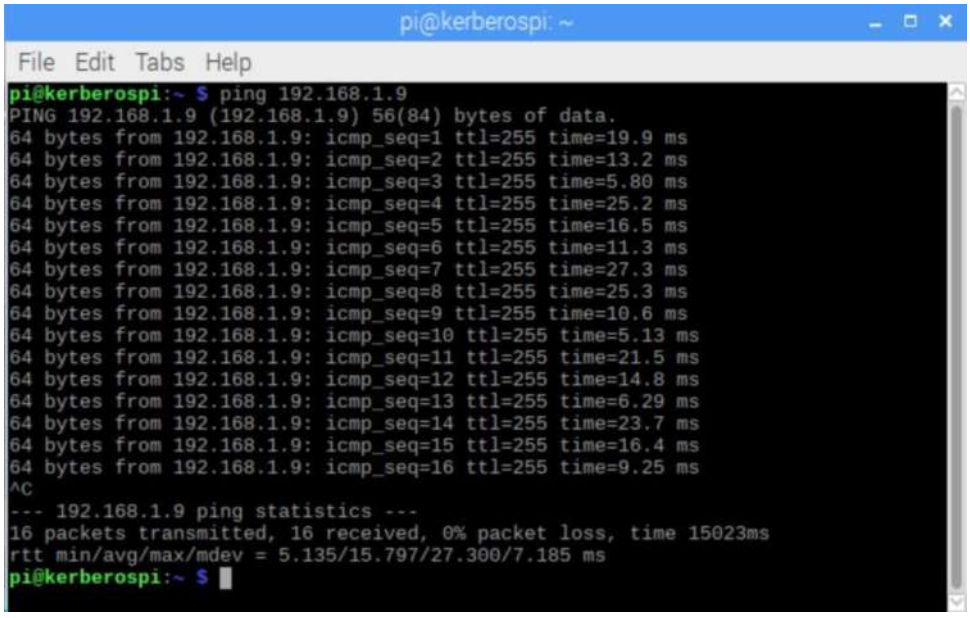


Figura 7-3: Conectividad realizado desde el servidor hacia el módulo de salida A

***Fuente*:** Omar Delgado B., 2018

Tabla 9-3: Latencia generada entre el servidor hacia el módulo de salida B

Latencia (ms)	15.6	6.13	25.3	16.2	13.8	28.1	23.6	11.4	4.03	22.8

Realizado por: Omar Delgado B., 2018

De manera igual se midió la latencia que tiene la conexión entre el módulo de ingreso B hacia el nodo central, donde los resultados de la inmediatez de la conexión se pueden apreciar tanto

en la tabla 9-3 como en la figura 8-3, donde la latencia media es de 16.69 ms este valor significa una media latencia debido a que la red ofrece una velocidad de la red.

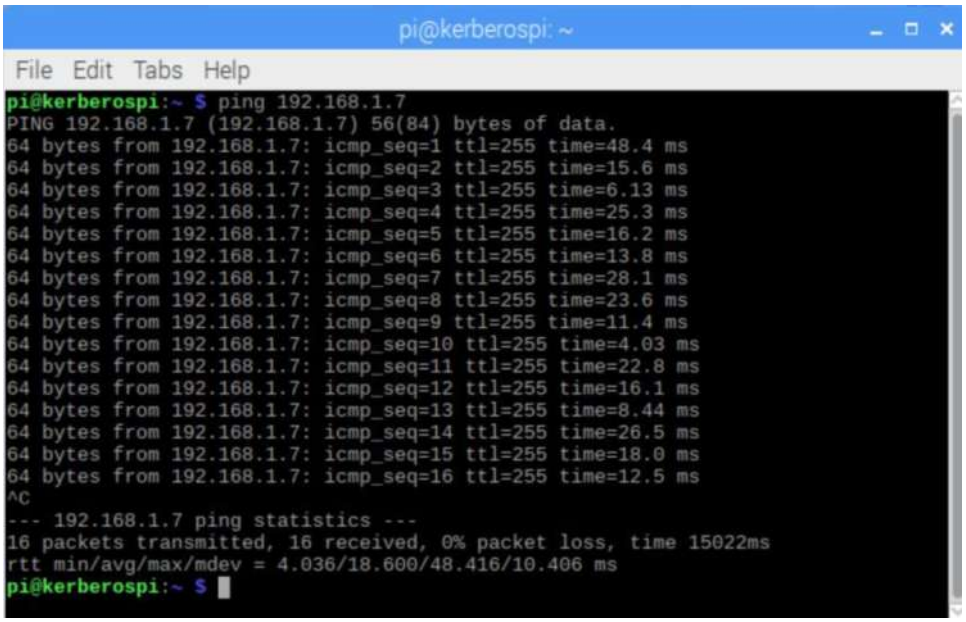


Figura 8-3: Conectividad realizado desde el servidor hacia el módulo de salida B

***Fuente*:** Omar Delgado B., 2018

3.2.5 Latencia entre el lector y servidor en el envío de información de llaveros

Tabla 10-3: Latencia generada en los llaveros hacia el servidor

Prueba	Llavero 1 (seg)	Llavero 2 (seg)	Llavero 3 (seg)	Llavero 4 (seg)
1	2	1	2	1
2	1	1	2	2
3	1	1	1	1
4	1	1	1	1
5	1	1	1	1
6	1	1	1	1
7	1	1	1	1
8	1	2	1	1
9	1	1	2	1
10	1	1	1	1

Realizado por: Omar Delgado B., 2018

Se realizó mediciones de la latencia generada por las etiquetas (llaveros) desde el paso de la etiqueta por el lector hasta el posterior almacenamiento de la información en la base de datos donde el tiempo que se demora en almacenar la información se puede apreciar en la tabla 10-3, donde el tiempo de latencia generado por los llaveros desde que realiza la respectiva lectura hasta su almacenamiento en los registros es de una media de 1.15 segundos, que no representa un tiempo considerable para reducir.

3.2.6 Latencia entre el lector y servidor en el envío de información de tarjetas

Tabla 11-3: Latencia generada en las tarjetas hacia el servidor

Prueba	Tarjeta 1 (seg)	Tarjeta 2 (seg)	Tarjeta 3 (seg)	Tarjeta 4 (seg)
1	1	1	1	1
2	2	1	1	1
3	1	1	1	1
4	1	1	2	2
5	1	1	1	1
6	1	1	1	2
7	2	1	1	1
8	1	1	1	1
9	1	1	1	1
10	1	1	1	1

Realizado por: Omar Delgado B., 2018

Se realizó mediciones de la latencia generada por las etiquetas (Tarjetas) desde el paso de la etiqueta por el lector hasta el posterior almacenamiento de la información en la base de datos donde el tiempo exacto que tarda en transmitir y almacenar la información se puede apreciar en la tabla 11-3, donde el tiempo de latencia generado por los tarjetas desde que realiza la respectiva lectura hasta su almacenamiento en los registros es de una media de 1.125 segundos, que al igual que los llaveros no representa un tiempo considerable para reducir.

3.3 Rendimiento de SAVEO

3.3.1 Encendido general

Tabla 12-3: Tiempos de encendido general del sistema

Encendido (segundos)	51.17	61.64	47.63	55.96	49.24	60.49	50.9	60.77	51.63	58.65
Reinicio (segundos)	42.14	39.93	52.28	42.41	42.44	51.56	41.75	42.02	50.3	41.75

Realizado por: Omar Delgado B., 2018

El sistema se demora 54.81 segundos la primera vez que es encendido para estar operativo, esto implica tanto el bloque central como sus módulos de ingreso y salida así como también los actuadores, de manera similar pero con tiempo inferior al de encendido, este tiempo se considera bajo debido a que una vez que se enciende el sistema permanecerá trabajando el tiempo que sea necesario, de manera similar el tiempo de reinicio es de 44.66 segundos si por algún motivo el sistema necesita reiniciarse su tiempo es reducido.

3.3.2 Tiempo de respuesta de la petición

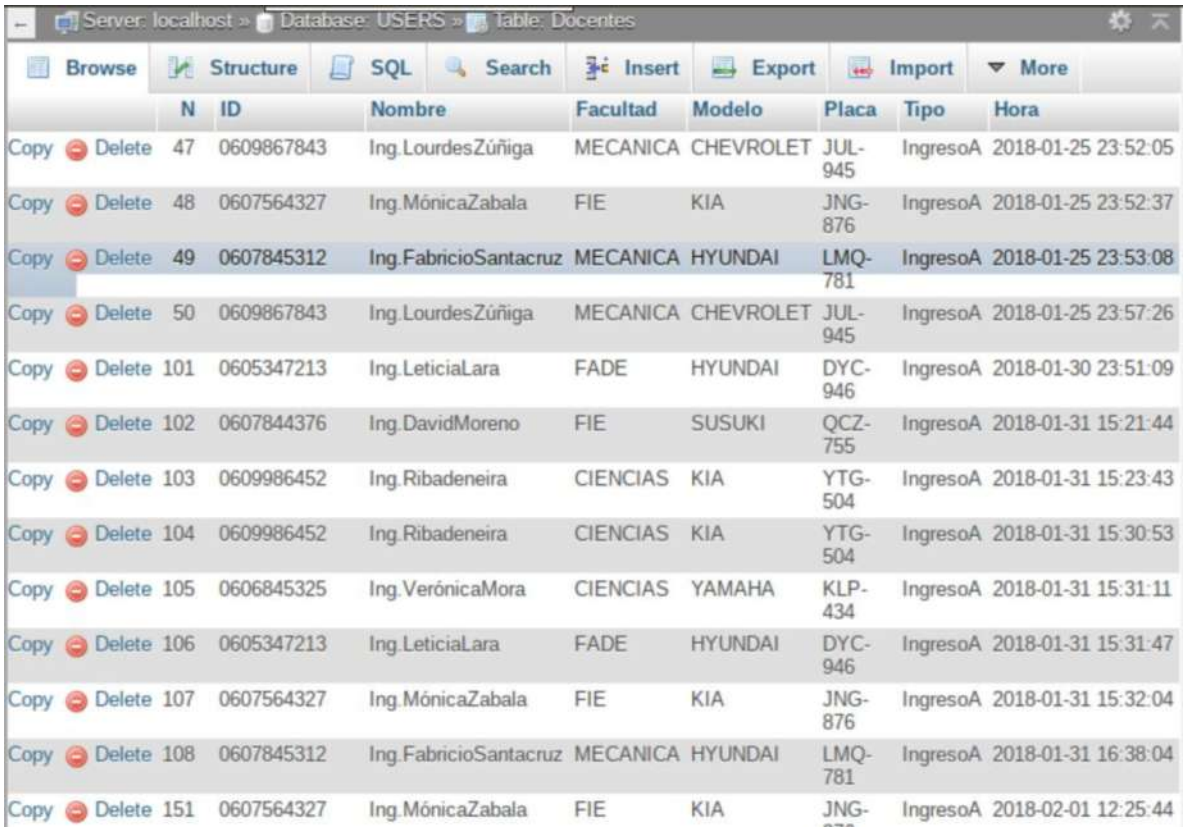
Tabla 14-3: Tiempos de respuesta de la petición

Tarjeta (segundos)	7.96	8.61	8.61	8.7	7.65	8.75	8.63	8.61	8.62	8.48
Llavero (segundos)	8.76	8.7	8.67	8.76	8.72	8.56	8.64	8.65	8.71	8.21

Realizado por: Omar Delgado B., 2018

El tiempo promedio de espera que toma al sistema receptar una petición hasta accionar la barrera vehicular es de 8.42 la tarjeta y 8.64 segundos el llavero, este tiempo se desglosa en leer la etiqueta, identificar si es un usuario autorizado, mostrar los mensajes al usuario y finalmente enviar los datos hacia el servidor para su posterior almacenaje, debido a estos tiempos aditivos el tiempo de repuesta de petición en el llavero es de 0.43 segundos y en la tarjeta es de 0.21 segundos siendo muy semejantes.

3.3.3 Fidelidad de los reportes de datos



	N	ID	Nombre	Facultad	Modelo	Placa	Tipo	Hora
Copy Delete	47	0609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-25 23:52:05
Copy Delete	48	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-01-25 23:52:37
Copy Delete	49	0607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-01-25 23:53:08
Copy Delete	50	0609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-25 23:57:26
Copy Delete	101	0605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA	2018-01-30 23:51:09
Copy Delete	102	0607844376	Ing.DavidMoreno	FIE	SUSUKI	QCZ-755	IngresoA	2018-01-31 15:21:44
Copy Delete	103	0609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-01-31 15:23:43
Copy Delete	104	0609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-01-31 15:30:53
Copy Delete	105	0606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-01-31 15:31:11
Copy Delete	106	0605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA	2018-01-31 15:31:47
Copy Delete	107	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-01-31 15:32:04
Copy Delete	108	0607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-01-31 16:38:04
Copy Delete	151	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-	IngresoA	2018-02-01 12:25:44

Figura 9-3: Reportes generados en la base de datos

***Fuente*:** Omar Delgado B., 2018

En la figura 9-3 se pueden apreciar los registros generados por el servidor que se encuentran almacenados en la base datos, de los campos creados el de mayor relevancia es la hora ya sea de ingreso o salida, cuyo registro fue evaluado con la hora actual que se realiza la lectura donde se tiene una diferencia de 1 segundo entre la hora que se pasa la etiqueta y el registro en la base de datos, donde se demuestra la fidelidad de los datos.

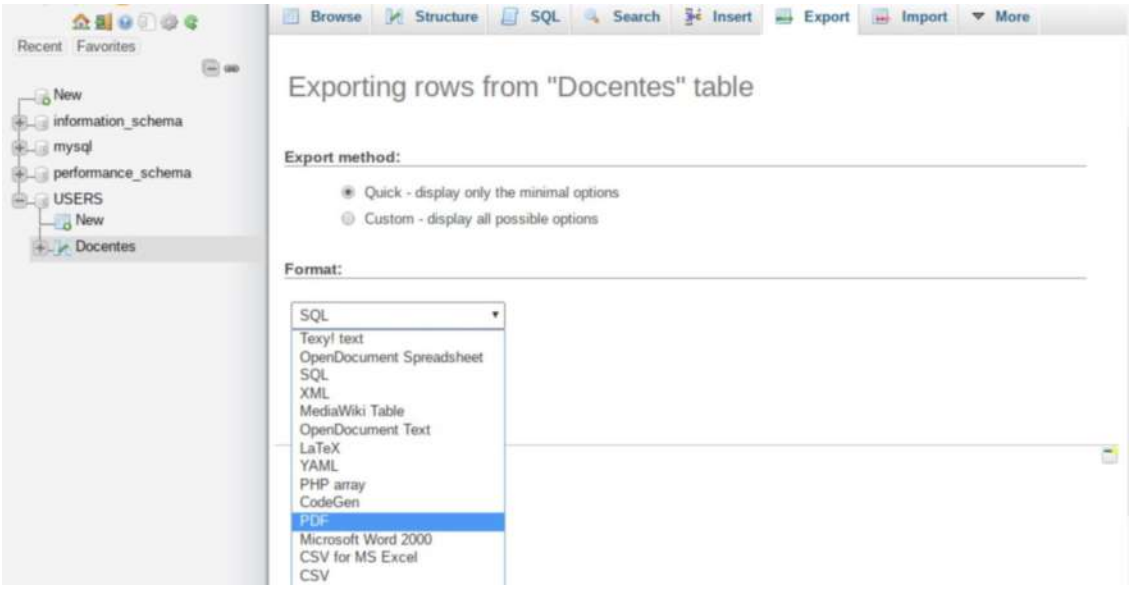
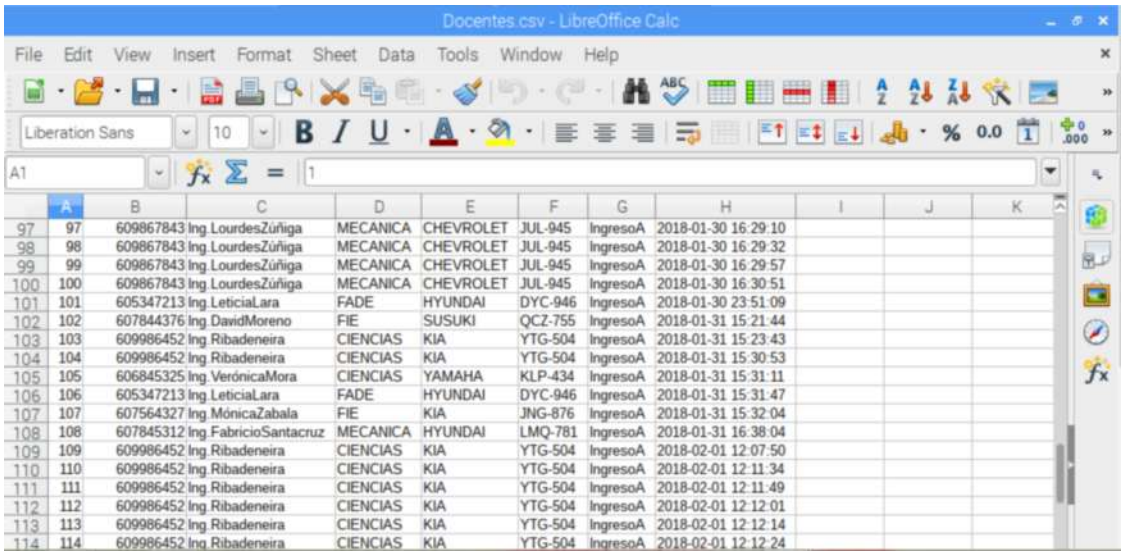


Figura 10-3: Formatos para exportar los registros

***Fuente*:** Omar Delgado B., 2018

De las múltiples opciones con las que cuenta el gestor de base de datos usado phpMyAdmin hay que dar mayor relevancia la de exportar su función es importante debido a que se puede utilizar como respaldo de la base de datos ya sea en papel o en la nube, entre los formatos para exportar están word, pdf, sql, látex, excel, xml, txt, entre los más importantes, como se muestra en las imágenes x-x.



	A	B	C	D	E	F	G	H	I	J	K
97	97	609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-30 16:29:10			
98	98	609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-30 16:29:32			
99	99	609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-30 16:29:57			
100	100	609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-01-30 16:30:51			
101	101	605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA	2018-01-30 23:51:09			
102	102	607844376	Ing.DavidMoreno	FIE	SUSUKI	QCZ-755	IngresoA	2018-01-31 15:21:44			
103	103	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-01-31 15:23:43			
104	104	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-01-31 15:30:53			
105	105	606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-01-31 15:31:11			
106	106	605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA	2018-01-31 15:31:47			
107	107	607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-01-31 15:32:04			
108	108	607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-01-31 16:38:04			
109	109	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:07:50			
110	110	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:11:34			
111	111	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:11:49			
112	112	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:12:01			
113	113	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:12:14			
114	114	609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-01 12:12:24			

Figura 11-3: Registro de la base de datos exportada a otro formato

***Fuente*:** Omar Delgado B., 2018

3.3.4 Pruebas de funcionamiento con tráfico

Tabla 15-3: Escenarios de pruebas del prototipo

1	Mejor Escenario	Un carro ingresa o sale
2	Escenario Medio	Un Carro ingresa al mismo otro sale o viceversa
3	Peor Escenario	Dos carros ingresa y Dos salen

Realizado por: Omar Delgado B., 2018

Se efectúan pruebas de tráfico en los escenarios para probar el funcionamiento del prototipo empezando desde el mejor escenario donde se considera que un solo vehículo ingrese o salga por algún acceso, después un escenario donde se considera a dos vehículos que pueden ingresar o salir al mismo tiempo y finalmente un considerado peor de los casos en donde se usan los cuatro acceso simultáneamente donde dos vehículos ingresan y a la vez dos vehículos salen por los accesos.

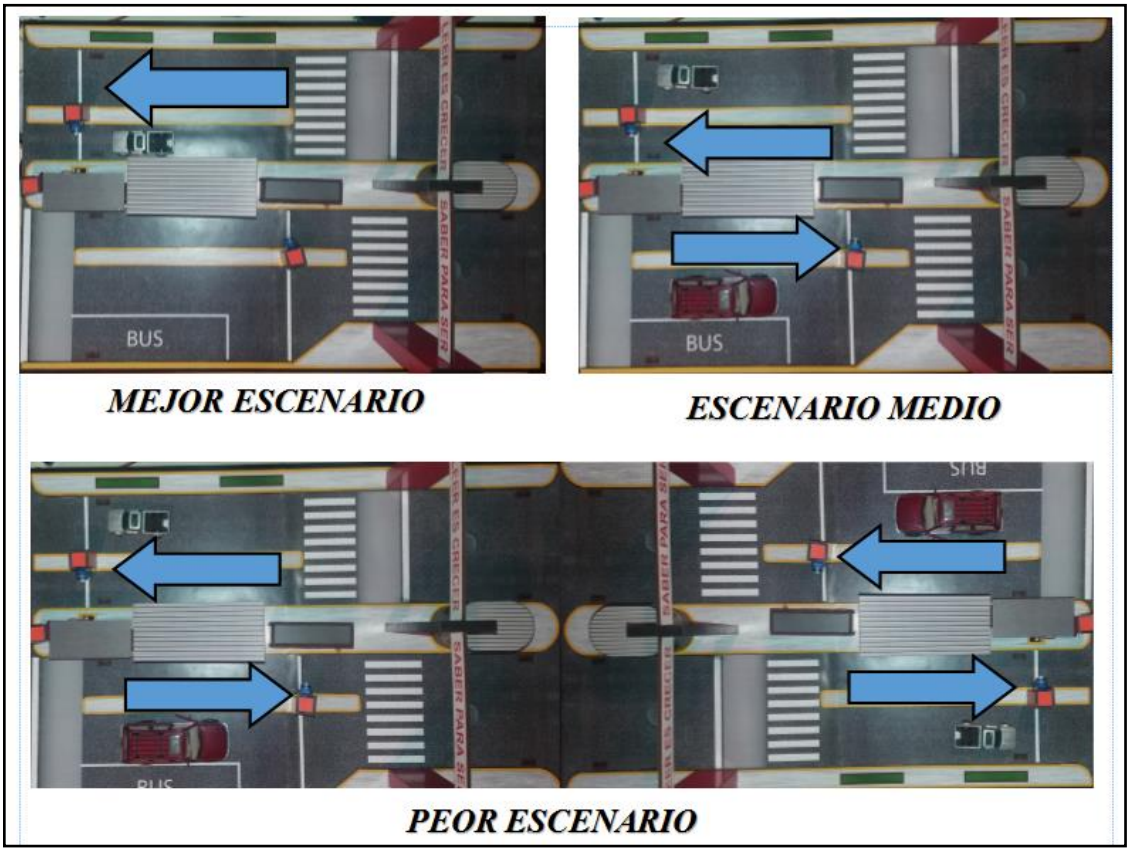


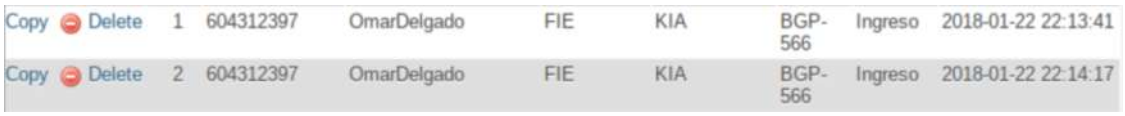
Figura 12-3: Escenarios de pruebas del prototipo

***Fuente*:** Omar Delgado B., 2018

3.3.4.1 Escenario número 1 funcionamiento con tráfico vehicular

Para esta prueba se toma el escenario número uno que se puede apreciar en la figura 12-3, en donde se ejecuta el funcionamiento del prototipo accionando un solo módulo es decir un solo vehículo ingresando o saliendo.

Como se muestra en la figura 13-3 se realiza la lectura en los lectores, utilizando un tag a la vez correspondiente a los distintos usuarios de forma aleatoria, donde se obtuvo que los registros se guardan de manera correcta.



Copy Delete	1	604312397	OmarDelgado	FIE	KIA	BGP-566	Ingreso	2018-01-22 22:13:41
Copy Delete	2	604312397	OmarDelgado	FIE	KIA	BGP-566	Ingreso	2018-01-22 22:14:17

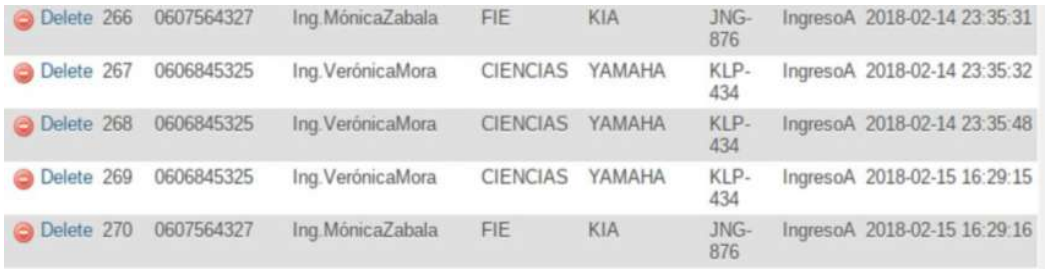
Figura 13-3: Registro de lectura única

***Fuente*:** Omar Delgado B., 2018

3.3.4.2 Escenario número 2 funcionamiento con tráfico vehicular

Para esta prueba se toma el escenario número dos, escenario medio, en donde se ejecuta las pruebas con dos accesos (ingreso, salida) siendo utilizados al mismo instante es decir un vehículo entra por un ingreso y otro sale por otro acceso o en su caso dos vehículos ingresando al mismo tiempo en dos accesos simultáneamente o viceversa.

Como se muestra en la figura 14-3 se realiza la lectura en dos lectores, utilizando al mismo tiempo dos tags correspondientes a los distintos usuarios de forma aleatoria, donde se obtuvo que en ocasiones los dos registros no se guardan de manera correcta, es decir casualmente se guardan los dos registros y en otras se guarda solamente un solo registro.



Delete	266	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-02-14 23:35:31
Delete	267	0606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-02-14 23:35:32
Delete	268	0606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-02-14 23:35:48
Delete	269	0606845325	Ing.VerónicaMora	CIENCIAS	YAMAHA	KLP-434	IngresoA	2018-02-15 16:29:15
Delete	270	0607564327	Ing.MónicaZabala	FIE	KIA	JNG-876	IngresoA	2018-02-15 16:29:16

Figura 14-3: Registro de dos lecturas simultáneas

Fuente: Omar Delgado B., 2018

Esto se debe a que los campos de cada registro son únicos y la base de datos no permite tener dos registros iguales en la misma tabla al intentar realizar la lectura simultánea en dos lectores al mismo tiempo da un error que se puede observar en la figura 15-3, para que esto no suceda se debe agregar un retardo de 800ms al establecer conexión con la base de datos en los dos módulos que se esté ejecutando las lecturas simultáneas.

Figura 15-3: Mensaje de consulta doble simultáneas

***Fuente*:** Omar Delgado B., 20

3.4.3.2 Escenario número 3 funcionamiento con tráfico vehicular

Para esta prueba se toma el escenario número tres, peor escenario, en donde se ejecuta las pruebas con los cuatro accesos siendo usados simultáneamente es decir dos vehículos ingresando y dos vehículos saliendo al mismo tiempo.

Como se muestra en la figura 16-3 se realiza la lectura en los cuatro lectores, utilizando al mismo tiempo cuatro tags correspondientes a los distintos usuarios de forma aleatoria, donde se obtuvo resultados muy similares a los obtenidos en el escenario dos donde los registros no se guardan de manera correcta, es decir casualmente se guardan los cuatro registros y en otras se guarda solamente uno, dos o tres registros.

Delete	272	0609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-02-15 16:52:02
Delete	273	0607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-02-15 16:55:20
Delete	274	0609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-15 16:55:21
Delete	275	0609867843	Ing.LourdesZúñiga	MECANICA	CHEVROLET	JUL-945	IngresoA	2018-02-15 16:58:30
Delete	276	0604675669	Ing.FaustoCabrera	FIE	MAZDA	HGF-221	IngresoA	2018-02-15 16:58:31
Delete	277	0609986452	Ing.Ribadeneira	CIENCIAS	KIA	YTG-504	IngresoA	2018-02-15 16:58:32
Delete	278	0607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA	2018-02-15 16:58:33

Figura 16-3: Registro de cuatro lecturas simultáneas

Fuente: Omar Delgado B., 2018

Este error nuevamente se debe a que los campos de cada registro son únicos y no permite tener dos registros iguales, mucho menos cuatro registros iguales en la misma tabla, al intentar realizar la lectura simultánea en cuatro lectores al mismo tiempo da un error que se puede observar en la figura 17-3, para que esto no suceda se debe agregar un retardo de 800ms al establecer conexión con la base de datos en todos los módulos que se esté ejecutando las lecturas simultáneas.

Figura 17-3: Mensaje de consulta de cuatro simultáneas

***Fuente*:** Omar Delgado B., 2018

CONCLUSIONES

- Se realizó la propuesta de un sistema automatizado para controlar el acceso vehicular en la ESPOCH utilizando tecnologías inalámbricas mediante los respectivos análisis tanto de la tecnología que se utilizó, dispositivos empleados para su elaboración.

- Por medio del estudio y desarrollo del sistema propuesto en cada etapa que se realizó, debido a que la tecnología y demás componentes que utiliza el sistema propuesto, son de bajo costo, su adquisición en el país es posible, por lo tanto el sistema es viable.

- Con el diseño y la implementación del prototipo se demuestra que el sistema propuesto SAVEO es operativo, basando su funcionamiento en dos de los tres accesos de la ESPOCH, cumple los requisitos exigidos dentro de la institución.

- El almacenamiento de los registro en la base datos bajo condiciones de tráfico vehicular presenta problemas por lo que es necesario insertar un retardo de 800 ms debido a que la base de datos no acepta campos duplicados en una misma tabla y por este retardo el campo de tiempo no son iguales.

- La distancia de lectura máxima de una tarjeta de identificación vehicular es de 3,5cm que difiere con los llaveros que actúa a una distancia máxima de 2,5cm, evidenciando la diferencia en la lectura de éste respecto a la tarjeta.

- SAVEO está compuesto por las etapas entrada, control y salida en el que se evidencia el tiempo de retardo de petición es de 0.43 segundos para los llaveros, en la tarjeta es de 0.21 segundos y para el almacenamiento de los datos se tiene un retardo 1.125 segundos en la hora que se realiza la lectura con la hora que se almacena el registro.

- Debido a los componentes y dispositivos del sistema, basados en las características y las prestaciones que ofrece incluyendo garantía y asistencia técnica, se evalúa el rendimiento general del sistema teniendo un promedio de 54.81seg que es un valor aceptable para los sistemas de control vehicular debido a que tiene un 99% disponibilidad, 99% escalabilidad, 99% factibilidad, y 99% fiabilidad por lo tanto el sistema es confiable para el objetivo que fue diseñado.

RECOMENDADIONES

- Manejar tarjetas como etiquetas de identificación debido a que cuentan con mayor rango de lectura con respecto a los llaveros, de esa manera se reduce la posibilidad de realizar una mala lectura.

- Utilizar una red virtual privada (vpn) para el sistema o asignar una dirección ip estática, para tener una menor latencia y mayor seguridad al momento de enviar los registros a la base de datos.

- Disponer de alimentación eléctrica propia para el sistema como panales solares, baterías u otras tecnologías similares, para no tener problemas de pérdidas de información sobre los registros generados en caso de pérdida temporal de la energía eléctrica es recomendable.

- Realizar respaldos periódicamente de los registros de la base de datos ya sea en papel o en la nube en caso de tener problemas para ingresar al administrador de la base datos o posibles fallos *software* tener un respaldo de la información.

- Ampliar los campos de identificación de los usuarios, de manera que la forma de filtración de información mejore a la hora de realizar búsquedas por uno o más campos.

- Para un mayor alcance de lectura se recomienda cambiar de antena por una de mayor potencia de esa manera extender la distancia para realizar la lectura de las etiquetas.

- Implementar mecanismos de seguridad a la red ya se existe la posibilidad de ser víctima de ataques, del mismo modo integrar mecanismos de protección.

- Se recomienda utilizar barras vehiculares que cuenten con un sensor para detectar si un vehículo se quedó en el área de control.

- Es recomendable la construcción de la estructura física necesaria para el acceso lateral vehicular de la institución para que el sistema opere en ese acceso.

- Se recomienda para trabajos futuros tener la posibilidad de trabajar con monitorización, cámaras de video o un circuito cerrado de televisión en cada acceso de la institución.

BIBLIOGRAFÍA

Acevedo J. and Perez L., *Autómatas Programables y Sistemas de Automatización* [en linea]. 2009. [Consulta Consulta: 12 Septiembre 2017]. Disponible en: https://books.google.com.ec/books?id=5jp3bforBB8C&printsec=frontcover&dq=automatizacion+de+sistemas&hl=es419&sa=X&ved=0ahUKEwjS29_R3_nYAhWGvVMKHZZaDAcQ6AEILTABv=onepage&q=automatizaciondesistemas&f=false.

Andreu, Joaquin, *Servicios en Red* [en linea]. 2011. [Consulta: 20 Sptiembre 2017]. Disponible en: https://books.google.com.ec/books?id=Gc_TAwAAQBAJ&pg=PA166&dq=servidor+web&hl=es-419&sa=X&ved=0ahUKEwjH48PHz_vYAhVNba0KHbanBN4Q6AEIMTAC#v=onepage&q=servidorweb&f=false.

Arias, Miguel, *Aprende Propgramación con PHP y MYSQL [en linea]*. *2015*.[Consulta 1 Octubre 2017]. Disponible en: https://books.google.com.ec/books?id=1kXKCgAAQBAJ&printsec=frontcover&dq=mysql&hl=es419&sa=X&ved=0ahUKEwjctYb0rvzYAhUDu1MKHariBscQ6AEILjAB#v=onepage&q=mysql&=false.

Asensi, Vivina, *Introducción a la automatización de los servicios de información*. [en linea]. 1995 [Consulta 21 Septiembre 2017], p. 141. Disponible en : https://books.google.com.ec/books?id=7Zw6lGX7iqsC&pg=PA67&dq=automatizacion+de+sistemas&hl=es419&sa=X&ved=0ahUKEwjS29_R3_nYAhWGvVMKHZZaDAcQ6AEIPDAD#v=onepage&q=automatizaciondesistemas&f=false.

Belloch, Consuelo, *Las tecnologías de la información y comunicación* [en linea]. 2010. [Consulta 3 Octubre 2017] p. 7. Disponible en : https://www.uv.es/~bellochc/pdf/pwtic1.pdf.

Caicedo, Antonio, *Arduino para Principiantes [en linea]*. *2017. [Consulta 5 Octubre 2017]*. *Disponible en:* https://books.google.com.ec/books?id=Fw_RDgAAQBAJ&pg=PA9&dq=arduino&hl=es419&sa=X&ved=0ahUKEwix2NeyxvvYAhVBba0KHeTICY8Q6AEIMTAB#v=onepage&q=arduno&f=false

Carballar, José, *Wi-Fi Lo que necesita conocer* [en linea]. 2010. [Consulta 5 Octubre 2017] Disponible en: https://books.google.com.ec/books?id=rQmH6IKyvigC&printsec=frontcover&dq=wifi&hl=es-419&sa=X&ved=0ahUKEwj88aTElvvYAhUF11MKHd34DcsQ6AEIJjAA#v=onepage&q=wifi&f=false.

Date, C. J. ,*Introducción a los Sistemas de Base de Datos*.[en linea] 2010. [Consulta 8 Octubre 2017] Disponible en: https://books.google.com.ec/books?id=Vhum351TK8C&printsec=frontcover&dq=base+de+datos&hl=es419&sa=X&ved=0ahUKEwil5v7LzfvYAhVEEawKHUVJCR8Q6AEIJjAA#v=onepage&q=basededatos&f=false.

Departamento de Tecnologías de la información y Comunicación, *Redes Eduroam*.[en linea]. 2017. [Consulta 10 Octubre 2017] Disponible en: http://redes.espoch.edu.ec/images/pdf/manual-registro-sawe-uso-wless_v2.pdf).

Departamento de Tecnologías de la información y Comunicación, *Redes ESPOCH*. [en linea]. 2017. [Consulta 10 Octubre 2017] Disponible en: http://redes.espoch.edu.ec/index.php/redes/wifi.

François M., *Raspberry pi 2 Utilice todo el potencial de su nano-ordenador*. [en linea]. 2016. [Consulta 15 Octubre 2017]. Disponible en: https://books.google.com.ec/books?id=zll9Cw8WmaYC&pg=PA27&dq=galileo+tarjeta&hl=es-419&sa=X&ved=0ahUKEwiW1tyxx_vYAhVSL6wKHQGdAesQ6AEILDAB#v=onepage&q=galileotarjeta&f=false.

Fulfuts Corporation., *Apache HTTP Server*. [en linea]. 2010. [Consulta 16 Octubre 2017]. Disponible en: https://books.google.com.ec/books?id=L9pbKAHfc34C&printsec=frontcover&dq=server+apache&hl=es419&sa=X&ved=0ahUKEwjo_6egq_zYAhXCoFMKHQClBkMQ6AEIJjAA#v=onepage&q=serverapache&f=false.

Huang S. and Rudolph L., *Bluetooth essentials for programmers*. [en linea]. 2007. [Consulta 4 Noviembre 2017] Disponible en: https://books.google.com.ec/books?id=s_djgV7_sXAC&pg=PA67&dq=bluetooth&hl=es-

ed=0ahUKEwiq35uwlPvYAhXS6lMKHffGA0Q6AEIKTAA#v=onepage&q=bluetooth&f=false.

Hunt D. and Puglia A., *RFID a guide to radio frecuency identification*, p. 201. [en linea]. 2007. [Consulta 12 Octubre 2017]. Disponible en: https://books.google.com.ec/books?id=ZCHiHqL6QKkC&printsec=frontcover&dq=RFID&hl=es-419&sa=X&ved=0ahUKEwj5g6_VjfvYAhUBtlMKHcWhBqEQ6AEIJjAA#v=onepage&q=RFID&f=false.

Ibáñez L. y Raya J., *Administración de sistemas gestores de bases de datos*. [en linea]. 2011. [Consulta 20 Octubre 2017]. Disponible en: https://books.google.com.ec/books?id=V7O7pwAACAAJ&dq=gestor+de+base+de+datos&hl=es-419&sa=X&ved=0ahUKEwj-ts31zvvYAhUDTKwKHW2pAF8Q6AEILTAB.

Intel, *Galileo*, [en linea]. 2017. [Consulta 23 Octubre 2017]. Disponible en: http://arduino.cl/intel-galileo/.

Isolve Mariana, *Historia de la Ciencia y la Tecnología*. [en linea]. 2002. [Consulta 30 Octubre 2017] Disponible en: https://books.google.com.ec/books?id=UMhadmakgioC&pg=PA14&dq=historia+estados+unidos+vehiculos&hl=es419&sa=X&ved=0ahUKEwj2mJ3UlIHZAhVJ61MKHTqiDVAQ6AEIJjAA#v=onepage&q=historiaestadosunidosvehiculos&f=false.

Kurniawan Agus, *Getting Started with Scratch for PcDuino*. [en linea]. 2015. [Consulta 7 Noviembre 2017] Disponible en: https://books.google.com.ec/books?id=_EIIBgAAQBAJ&pg=PT135&dq=pcduino&hl=es-419&sa=X&ved=0ahUKEwizu8r3yvvYAhUKA6wKHXFyCikQ6AEIJjAA#v=onepage&q=pcduino&f=false.

Kurniawan Agus, *NodeMCU Development Workshop*. [en linea]. 2015. [Consulta 8 Noviembre 2017] Disponible en: https://books.google.com.ec/books?id=XP9ICgAAQBAJ&printsec=frontcover&dq=nodeMCU&hl=es419&sa=X&ved=0ahUKEwif176OyvvYAhVSeKwKHT4qBgoQ6AEIJjAA#v=onepage&q=nodeMCU&f=false.

Lara Eduard, *Protocolo HTTP y Servidores WEB*, p. 39. [en linea]. 2011. [Consulta 13 Noviembre 2017] Disponible en: http://elara.site.ac.upc.edu/documentacion/INTERNET - UD8 - Protocolo HTTP y servidores WEB.pdf.

LOTAIP, *Ley de Transparencia*. [en linea]. 2017. [Consulta 10 Noviembre 2017] Disponible en: http://lotaip.espoch.edu.ec/index.php?option=com_content&view=article&id=89&Itemid=61.

Malhotra Naresh, *Investigación de Mercados un Enfoque Aplicado*. [en linea]. 2004. [Consulta 20 Noviembre 2017] Disponible en: https://books.google.com.ec/books?id=SLmEblVK2OQC&pg=PA258&dq=escala+de+likert&hl=es-419&sa=X&ved=0ahUKEwiPqrvmo_zYAhUP7lMKHTxyAIYQ6AEIJjAA#v=onepage&q=escala de likert&f=false.

McLaughlin Brian, *The BeagleBone Black Primer*. [en linea]. 2016. [Consulta 22 Noviembre 2017] Disponible en: https://books.google.com.ec/books?id=W2OkCgAAQBAJ&printsec=frontcover&dq=beaglebone&hl=es419&sa=X&ved=0ahUKEwi4vuvZy_vYAhULKqwKHWOGC20Q6AEIOTAC#v=onepage&q=beaglebone&f=false.

Medina César, *Los Sistemas Automáticos de Identificación*. [en linea]. 1994. [Consulta 2 Diciembre 2017] Disponible en: https://www.azc.uam.mx/publicaciones/enlinea2/num1/1-1.htm.

Mifsuf Elvira, *Apache*. [en linea]. 2012. [Consulta 5 Diciembre 2017] Disponible en: https://books.google.com.ec/books?id=Kg8bAgAAQBAJ&printsec=frontcover&dq=apache&hl=es-419&sa=X&ved=0ahUKEwiQ5aOE0fvYAhUJeawKHRoUBQAQ6AEIJjAA#v=onepage&q=apache&f=false.

Monsó Julia, *Sistemas de identificación y Control automáticos*. [en linea]. 1994. [Consulta 17 Diciembre 2017] Disponible en: https://books.google.com.ec/books?id=nGgmObQH2r0C&pg=PA119&dq=sistema+de+tarjetas+magnéticas&hl=es-419&sa=X&ved=0ahUKEwjpnZOVvnYAhVNzVMKHeKMDB8Q6AEILTAB#v=onepage&q=sist

emadetarjetasmagnéticas&f=false.

Rios, *Diseño de un sistema de control vehicular basado en el acceso de espacios libres y ubicación en estacionamientos usando rfi*', p. 65. [en linea]. 2011. [Consulta 18 Diciembre 2017] Disponible en: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/910/RIOS_VIDALON_JORGE_CONTROL_VEHICULAR_RFID.pdf?sequence=1&isAllowed=y.

Ruiz A. and Sánchez N., Tecnologías de la información y la comunicación para la innovación educativa. [en linea]. 2013. [Consulta 5 Enero 2018] Disponible en: https://books.google.com.ec/books?id=V4DqpHlVJTAC&pg=PA328&dq=topologia+estrella&hl=es419&sa=X&ved=0ahUKEwig0MuM9vnYAhUM0VMKHQHJABAQ6AEIJjAA#v=onepage&q=topologiaestrella&f=false.

Taylor et al., *Wimax Taking Wireless to the MAX*. [en linea]. 2006. [Consulta 8 Enero 2018] Disponible en: https://books.google.com.ec/books?id=PWfLBQAAQBAJ&pg=PA149&dq=wimax&hl=es-419&sa=X&ved=0ahUKEwjei86Tl_vYAhUF0lMKHbVoCj0Q6AEIJjAA#v=onepage&q=wimax&f=false.

Torrente Oscar, *Arduino curso práctico de información*. [en linea]. 2013. [Consulta 5 Enero 2018] Disponible en: https://books.google.com.ec/books?id=6cZhDmf7suQC&pg=PA132&dq=ide+arduino&hl=es-419&sa=X&ved=0ahUKEwiqqY--qfzYAhXJ2lMKHVvKBu4Q6AEIOzAC#v=onepage&q=ide arduino&f=false.

Uinovi, S., *Tecnologías para la automatización*. [en linea]. 2013. [Consulta 5 Enero 2018] Disponible en: http://isa.uniovi.es/docencia/autom3m/Temas/Tema3.pdf.

UNDP, *Cedatos*. [en linea]. 2017. [Consulta 9 Agosto 2018] Disponible en: http://www.undp.org/.

Wexler Joanie, *Protocolo ZigBee (IEEE 802.15.4)*, p. 38. [en linea]. 2013. [Consulta 15 Enero 2018] Disponible en: https://rua.ua.es/dspace/bitstream/10045/1109/1/InformeTecZB.pdf.

ANEXOS

Anexo A

Hoja de especificaciones técnicas raspberry pi 2 B

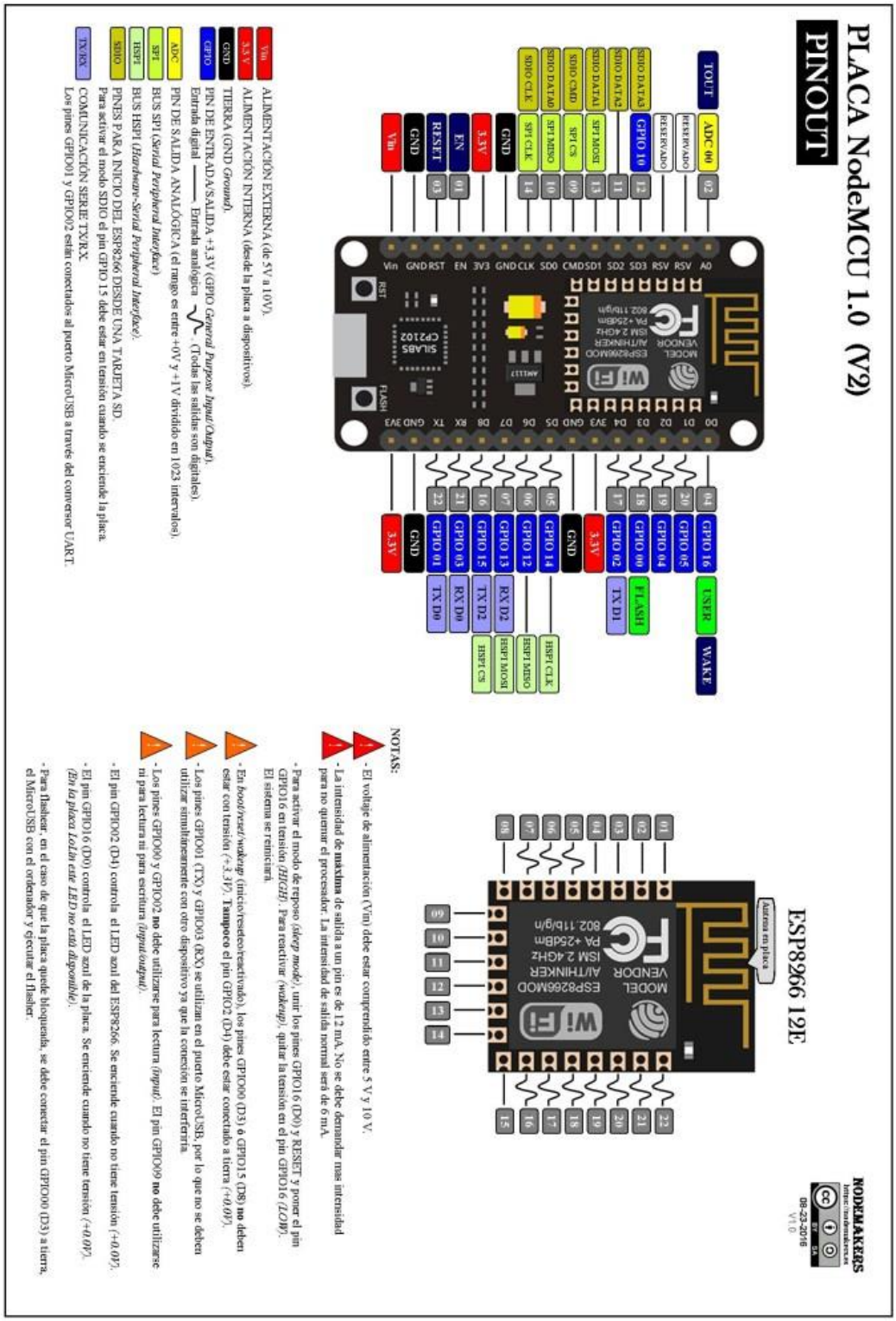
Raspberry Pi

Raspberry Pi 2, Model B

Product Name	**Raspberry Pi 2, Model B**
Product Description	The Raspberry Pi 2 delivers 6 times the processing capacity of previous models. This second generation Raspberry Pi has an upgraded Broadcom BCM2836 processor, which is a powerful ARM Cortex-A7 based quad-core processor that runs at 900MHz. The board also features an increase in memory capacity to 1Gbyte.
Specifications	
Chip	Broadcom BCM2836 SoC
Core architecture	Quad-core ARM Cortex-A7
CPU	900 MHz
GPU	Dual Core VideoCore IV® Multimedia Co-Processor Provides Open GL ES 2.0, hardware-accelerated OpenVG, and 1080p30 H.264 high-profile decode Capable of 1Gpixel/s, 1.5Gtexel/s or 24GFLOPs with texture filtering and DMA infrastructure
Memory	1GB LPDDR2
Operating System	Boots from Micro SD card, running a version of the Linux operating system
Dimensions	85 x 56 x 17mm
Power	Micro USB socket 5V, 2A
Connectors:	
Ethernet	10/100 BaseT Ethernet socket
Video Output	HDMI (rev 1.3 & 1.4)
Audio Output	3.5mm jack, HDMI
USB	4 x USB 2.0 Connector
GPIO Connector	40-pin 2.54 mm (100 mil) expansion header: 2x20 strip Providing 27 GPIO pins as well as +3.3 V, +5 V and GND supply lines
Camera Connector	15-pin MIPI Camera Serial Interface (CSI-2)
JTAG	Not populated
Display Connector	Display Serial Interface (DSI) 15 way flat flex cable connector with two data lanes and a clock lane
Memory Card Slot	Micro SDIO

Anexo B

Hoja de especificaciones técnicas NodeMCU v2.



Anexo C

Hoja de especificaciones técnicas lector RFID RC522

RFID Quick Start Guide: Arduino

Understanding RFID

RFID, or Radio Frequency Identification, is a system for transferring data over short distances (typically less than 6 inches). Often only one of the two devices needs to be powered, while the other is a passive device. This allows for easy use in such things as credit cards, key fobs, and pet collars as there is no need to worry about battery life. The downside is that the reader and the information holder (ie credit card) must be very close, and can only hold small amounts of data.

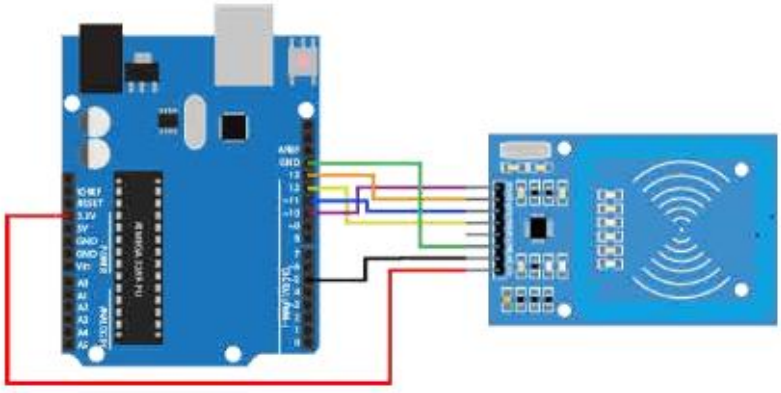
In this tutorial we will be using the MFRC522 13.56Mhz IC by MIFARE, as described at https://www.addicore.com/product-p/126.htm.
If you would like to purchase additional RFID cards of fobs they can be found at the following:

- RFID Cards 13.56 MHz MF1ICS50
- RFID Key Fobs 13.56 MHz MF1ICS50

Wiring

The following table shows the needed connections between the RFID and the Arduino Uno
Cautions:
*On the Arduino many of the pins are not swappable. Because this device uses the SPI bus, who's pins cannot be moved around, pins 11, 12, 13 must remain as shown. RST and IRQ are user specified.
*This device is NOT a 5 volt powered device. You MUST power it with 3.3 volts. If you do not, you risk overheating the RFID. Most Arduino boards include a 3.3V supply pin which can be used to power the RFID module. If 3.3 volts is not accessible, there are LD33V regulators available at Addicore.com that supply 3.3 volts.

RFID-RC522 Module	Arduino Uno
1 - SDA	Digital 10
2 - SCK	Digital 13
3 - MOSI	Digital 11
4 - MISO	Digital 12
5 - IRQ	--unconnected--
6 - GND	Gnd
7 - RST	Digital 5
8 - 3.3V	3.3v



Adding the Library

If you haven't already done so, the AddicoreRFID library needs to be added to your Arduino library depository.

1. Download the AddicoreRFID library

Anexo D

Configuración en el IDE de Arduino de los mecanismos del sistema

/******** Modulo ingreso A **********/**

```
#include <ESP8266WiFi.h>

#include <SPI.h>

#include <MFRC522.h>

#include <Servo.h>

#include <LiquidCrystal_I2C.h>

#include <Wire.h>


#define SS_PIN 4     //D2

#define RST_PIN 5    //D1

#define Led 16  //D0


LiquidCrystal_I2C lcd(0x27, 16, 2);


MFRC522 mfrc522(SS_PIN, RST_PIN);       // Crea la instancia MRFC522

Servo servoMotor;

WiFiServer server(80);


const char* ssid = "LAURA";

const char* password = "0602083693";

const char* host = "controlaccesoespoch.ddns.net";

//const char* host = "172.25.200.199";

//const char* url = "http://192.168.1.60/users.php";

//IPAddress server(192,168,1,60);

//const char* host = "www.google.com";


const int numcards=8;
//numero de tarjetas rfids que hay definidas


//definimos los códigos de las tarjetas (4 primeros digitos en formato hexadecimal)


unsigned long rfid[numcards]={0xB0C90274,0xC0631F83,0x10D59775,0x808E8B75,0xE0AA9975,0x86528FBB,0xC6482A9E,0x56B9B0BB};
//{0xB0C90274,0xC0631F83}


//aquí podemos introducir las personas a la que pertenecen los tarjetas


char* individuo1[numcards]={"0607564327","0609867843","0605347213","0606845325","0607844376","0604675669","0607845312","0609986452"};

char* individuo2[numcards]={"Ing. MónicaZabala","Ing.LourdesZúñiga","Ing.LeticiaLara","Ing. VerónicaMora","Ing.DavidMoreno","Ing.FaustoCabrera","Ing.FabricioSantacruz","Ing.Ribadeneira"};

char* individuo3[numcards]={"FIE","MECANICA","FADE","CIENCIAS","FIE","FIE","MECANICA","CIENCIAS"};

char* individuo4[numcards]={"KIA","CHEVROLET","HYUNDAI","YAMAHA","SUSUKI","MAZDA","HYUNDAI","KIA"};

char* individuo5[numcards]={"JNG-876","JUL-945","DYC-946","KLP-434","QCZ-755","HGF-221","LMQ-781","YTG-504"};

char* individuo6[numcards]={"Ing. Monica","Ing. Lourdes","Ing. Leticia","Ing. Veronica","Ing. David","Ing. Fausto","Ing. Fabricio","Ing. Jefferson"};

char* individuo7[numcards]={"Zabala","Zuñiga","Lara","Mora","Moreno","Cabrera","Santacruz","Ribadeneira"};


void setup()

{

    Serial.begin(9600);       // Inicializa la comunicacion serial con la PC

    SPI.begin();              // Inicializa el SPI bus

    mfrc522.PCD_Init();       // Inicializa el lector MFRC522
```

```
      servoMotor.attach(D8);
//D8
      pinMode(Led,OUTPUT);
      digitalWrite(Led,HIGH);
      conectar();
      Wire.begin(D4, D3);
      lcd.begin();
      lcd.clear();
      lcd.setCursor(0,0);
      lcd.print("PASE SU
TARJETA");
      lcd.setCursor(3,1);
      lcd.print("POR
FAVOR");
      Serial.println(" ");
      Serial.println("PASE SU
TARJETA POR FAVOR ");
      Serial.println(" ");


}


void conectar() {


  // Connect to WiFi network
  Serial.println();
  Serial.println();
  Serial.print("Conectando a
");
  Serial.println(ssid);


  WiFi.begin(ssid, password);


  while (WiFi.status() !=
WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
 Serial.println("");
 Serial.println("WiFi
connected");
 Serial.println("IP address: ");
 Serial.println(WiFi.localIP());


}



void saludo()
{
  Serial.println("Acceso
Autorizado.");
  lcd.clear();
  lcd.setCursor(5,0);
  lcd.print("ACCESO");
  lcd.setCursor(3,1);
  lcd.print("AUTORIZADO");
  delay(2000);
  Serial.println("Bienvenido");
  lcd.clear();
  lcd.setCursor(3,0);
  lcd.print("BIENVENIDO");
  lcd.setCursor(2,1);
  lcd.print("TEN BUEN
DIA");
  delay(2000);
  Serial.println("Ten Buen Día
");
}

void autorizado ()
{
  int pos;
  int dist = 0;
  dist = analogRead(0);
  digitalWrite(Led,LOW);
  // Desplazamos a la posición
100º
  for(pos = 0; pos <= 100; pos
+= 1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  // Esperamos 3 segundo
  //delay(5000);
  for (int i = 0; i<=20; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
  // Desplazamos a la posición
180º
  if(dist < 300)
  {
  for(pos = 100; pos>=0; pos-
=1)
  {
    servoMotor.write(pos);
    delay(15);
```

```
  }
  }
  else
  {
  for(pos = 0; pos <= 100; pos += 1)
  {
   servoMotor.write(pos);
   delay(15);
  }
  }
  for (int i = 0; i<=8; i++)
   {
    digitalWrite(Led, HIGH);
    delay(150);
    digitalWrite(Led, LOW);
    delay(150);
   }
}



void no_autorizado()
{
  Serial.println("Acceso Denegado");
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print("ACCESO DENEGADO!");
  lcd.setCursor(0,1);
  lcd.print("SIN AUTORIZACION");
  Serial.println("No tiene Autorizacion");
for (int i = 0; i<=8; i++)
   {
    digitalWrite(Led, HIGH);
    delay(150);
    digitalWrite(Led, LOW);
    delay(150);
   }
}


void loop() {


      // Prepare key - all keys are set to FFFFFFFFFFFFh at chip delivery from the factory.

MFRC522::MIFARE_Key key;
      for (byte i = 0; i < 6; i++) key.keyByte[i] = 0xFF;


      // Look for new cards
      if ( ! mfrc522.PICC_IsNewCardPresent())
            {
             return;
            }


      // Select one of the cards
      if ( ! mfrc522.PICC_ReadCardSerial())    return;


      Serial.print("Tarjeta detectada");    //Dump UID
      Serial.println(" ");
      digitalWrite(Led, LOW);
      for (byte i = 0; i < mfrc522.uid.size; i++)
      {

//Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");

//Serial.print(mfrc522.uid.uidByte[i], HEX);
      }
      //Serial.print(" PICC type: ");   // Dump PICC type
      byte piccType = mfrc522.PICC_GetType(mfrc522.uid.sak);

//Serial.println(mfrc522.PICC_GetTypeName(piccType));


      byte buffer[18];
      byte block  = 0;
      byte status;


      status = mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, block, &key, &(mfrc522.uid));
      if (status != MFRC522::STATUS_OK)
       {

Serial.print("AUTENTICACION FALLIDA ");
        lcd.clear();
        lcd.setCursor(1,0);
```

```
lcd.print("AUTENTICACION
");
        lcd.setCursor(4,1);
        lcd.print("FALLIDA");
        for (int i = 0; i<=8; i++)
        {
         digitalWrite(Led,
HIGH);
         delay(150);
         digitalWrite(Led,
LOW);
         delay(150);
        }
        Serial.print("POR
FAVOR REINTENTE
NUEVAMENTE ");
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print("TRATE
NUEVAMENTE");
        lcd.setCursor(4,1);
        lcd.print("POR
FAVOR");

//Serial.println(mfrc522.GetSt
atusCodeName(status));
        return;
        }

      // Read block
   byte byteCount =
sizeof(buffer);

   status =
mfrc522.MIFARE_Read(bloc
k, buffer, &byteCount);
   if (status !=
MFRC522::STATUS_OK)
      {

Serial.print("MIFARE_Read()
failed: ");

//Serial.println(mfrc522.GetSt
atusCodeName(status));
      }
      else  // Dump data
   {


      //transforma los 4
primeros numeros del bloque
0 en una variable
      //de 4 bytes para poderla
comparar con las
numeraciones registradas
      unsigned long card=0;
      byte b=0;
      for (int a=3;a>-1;a--) {
      switch (a){
      case 3:  card +=
buffer[b]*16777216; break;
      case 2:  card +=
buffer[b]*65536; break;
      case 1:  card +=
buffer[b]*256; break;
      case 0:  card +=
buffer[b];break;
      }
      b++;}

      boolean
encontrada=false;
      for (byte
a=0;a<numcards;a++) {
      if (rfid[a]==card) {

        //subir();

Serial.print("connecting to ");

Serial.println("controlaccesoes
poch.ddns.net");

// Use WiFiClient class to
create TCP connections
WiFiClient client;
const int httpPort = 80;
if (!client.connect(host,
httpPort))
{
Serial.println("connection
failed");
return;
}
// We now create a URL for
the request
String url
="http://192.168.1.60/users.ph
p";
String dato1 = "?Id=";
String dato2 = "&Nombre=";
String dato3 = "&Facultad=";
String dato4 = "&Modelo=";
String dato5 = "&Placa=";
String dato6 =
"&Tipo=IngresoA";
String dato7 = individuo1[a];
String dato8 = individuo2[a];
```

```
 String dato9 = individuo3[a];
 String dato10 = individuo4[a];
 String dato11 = individuo5[a];
 String dato12 = individuo6[a];

 Serial.print("Accediendo a: ");

Serial.println("controlaccesoespoch.ddns.net");

 // This will send the request to the server
 client.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + " HTTP/1.1\r\n" +
 "Host: " + host + "\r\n" +
 "Connection: close\r\n\r\n");
//Serial.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + "Connection: close\r\n\r\n");
          saludo();
Serial.println(individuo6[a]);
          lcd.clear();
          lcd.setCursor(0,0);
lcd.print(individuo6[a]);
          lcd.setCursor(5,1);
lcd.print(individuo7[a]);
          delay(1500);
          autorizado();
          encontrada=true;}} //si el num de la tarjeta coincide
          //con alguno de los definidos nos dice el nombre o saludo
          if (encontrada) //autorizado();
          {Serial.println("PASE SU TARJETA POR FAVOR ");
          lcd.clear();
          lcd.setCursor(0,0);
          lcd.print("PASE SU TARJETA");
          lcd.setCursor(3,1);
          lcd.print("POR FAVOR");
digitalWrite(Led,HIGH);}
          else no_autorizado();
      for (byte index = 0; index < 18; index++)
      {
//Serial.print(buffer[index] < 0x10 ? " 0" : " ");
//Serial.print(buffer[index], HEX);
      if ((index % 4) == 3) Serial.print(" ");
      }
     }
      Serial.println(" ");
      mfrc522.PICC_HaltA(); // Halt PICC
mfrc522.PCD_StopCrypto1(); // Stop encryption on PCD
}
```

/******** Modulo ingreso B **********/**

```
#include <ESP8266WiFi.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <LiquidCrystal_I2C.h>
#include <Wire.h>
#define SS_PIN 4     //D2
#define RST_PIN 5    //D1
#define Led 16  //D0
LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 mfrc522(SS_PIN, RST_PIN);       // Crea la instancia MRFC522
```

```
Servo servoMotor;

WiFiServer server(80);


const char* ssid = "LAURA";

const char* password = "0602083693";

const char* host = "controlaccesoespoch.ddns.net";

//const char* host = "172.25.200.199";

//const char* url = "http://192.168.1.60/users.php";

//IPAddress server(192,168,1,60);

//const char* host = "www.google.com";


const int numcards=8;
//numero de tarjetas rfids que hay definidas


//definimos los códigos de las tarjetas (4 primeros digitos en formato hexadecimal)


unsigned long rfid[numcards]={0xB0C90274,0xC0631F83,0x10D59775,0x808E8B75,0xE0AA9975,0x86528FBB,0xC6482A9E,0x56B9B0BB};
//{0xB0C90274,0xC0631F83}


//aquí podemos introducir las personas a la que pertenecen los tarjetas

char* individuo1[numcards]={"0607564327","0609867843","0605347213","0606845325","0607844376","0604675669","0607845312","0609986452"};

char* individuo2[numcards]={"Ing.MónicaZabala","Ing.LourdesZúñiga","Ing.LeticiaLara","Ing.VerónicaMora","Ing.DavidMoreno","Ing.FaustoCabrera","Ing.FabricioSantacruz","Ing.Ribadeneira"};

char* individuo3[numcards]={"FIE","MECANICA","FADE","CIENCIAS","FIE","FIE","MECANICA","CIENCIAS"};

char* individuo4[numcards]={"KIA","CHEVROLET","HYUNDAI","YAMAHA","SUSUKI","MAZDA","HYUNDAI","KIA"};

char* individuo5[numcards]={"JNG-876","JUL-945","DYC-946","KLP-434","QCZ-755","HGF-221","LMQ-781","YTG-504"};

char* individuo6[numcards]={"Ing. Monica","Ing. Lourdes","Ing. Leticia","Ing. Veronica","Ing. David","Ing. Fausto","Ing. Fabricio","Ing. Jefferson"};

char* individuo7[numcards]={"Zabala","Zuñiga","Lara","Mora","Moreno","Cabrera","Santacruz","Ribadeneira"};


void setup()

{

      Serial.begin(9600);       // Inicializa la comunicacion serial con la PC

      SPI.begin();              // Inicializa el SPI bus

      mfrc522.PCD_Init();       // Inicializa el lector MFRC522

      servoMotor.attach(D8);    //D8

      pinMode(Led,OUTPUT);

      digitalWrite(Led,HIGH);

      conectar();

      Wire.begin(D4, D3);

      lcd.begin();

      lcd.clear();

      lcd.setCursor(0,0);

      lcd.print("PASE SU TARJETA");

      lcd.setCursor(3,1);

      lcd.print("POR FAVOR");

      Serial.println(" ");

      Serial.println("PASE SU TARJETA POR FAVOR ");

      Serial.println(" ");


}


void conectar() {


  // Connect to WiFi network

  Serial.println();

  Serial.println();

  Serial.print("Conectando a ");
```

```
  Serial.println(ssid);


  WiFi.begin(ssid, password);


  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
 Serial.println("");
 Serial.println("WiFi connected");
 Serial.println("IP address: ");
 Serial.println(WiFi.localIP());


}



void saludo()
{
  Serial.println("Acceso Autorizado.");
  lcd.clear();
  lcd.setCursor(5,0);
  lcd.print("ACCESO");
  lcd.setCursor(3,1);
  lcd.print("AUTORIZADO");
  delay(2000);
  Serial.println("Bienvenido");
  lcd.clear();
  lcd.setCursor(3,0);
  lcd.print("BIENVENIDO");
  lcd.setCursor(2,1);
  lcd.print("TEN BUEN DIA");
  delay(2000);
  Serial.println("Ten Buen Día ");
}


void autorizado ()
{
  int pos;
  int dist = 0;
  dist = analogRead(0);
  digitalWrite(Led,LOW);
  // Desplazamos a la posición 100º
  for(pos = 0; pos <= 100; pos += 1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  // Esperamos 3 segundo
  //delay(5000);
  for (int i = 0; i<=20; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
  // Desplazamos a la posición 180º
  if(dist < 300)
  {
  for(pos = 100; pos>=0; pos-=1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  }
  else
  {
  for(pos = 0; pos <= 100; pos += 1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  }
  for (int i = 0; i<=8; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
}


void no_autorizado()
{
  Serial.println("Acceso Denegado");
  lcd.clear();
  lcd.setCursor(0,0);
```

```
  lcd.print("ACCESO
DENEGADO!");
  lcd.setCursor(0,1);
  lcd.print("SIN
AUTORIZACION");
  Serial.println("No tiene
Autorizacion");
for (int i = 0; i<=8; i++)
   {
     digitalWrite(Led, HIGH);
     delay(150);
     digitalWrite(Led, LOW);
     delay(150);
   }
}

void loop() {

      // Prepare key - all keys
are set to FFFFFFFFFFFFh at
chip delivery from the factory.

MFRC522::MIFARE_Key
key;
      for (byte i = 0; i < 6; i++)
key.keyByte[i] = 0xFF;

      // Look for new cards
      if ( !
mfrc522.PICC_IsNewCardPre
sent())
            {
             return;
            }

      // Select one of the cards
      if ( !
mfrc522.PICC_ReadCardSeri
al())    return;

      Serial.print("Tarjeta
detectada");    //Dump UID
      Serial.println(" ");
      digitalWrite(Led, LOW);
      for (byte i = 0; i <
mfrc522.uid.size; i++)
      {

//Serial.print(mfrc522.uid.uid
Byte[i] < 0x10 ? " 0" : " ");

//Serial.print(mfrc522.uid.uid
Byte[i], HEX);
      }
      //Serial.print(" PICC
type: ");   // Dump PICC type
      byte piccType =
mfrc522.PICC_GetType(mfrc
522.uid.sak);

//Serial.println(mfrc522.PICC
_GetTypeName(piccType));

      byte buffer[18];
      byte block  = 0;
      byte status;

      status =
mfrc522.PCD_Authenticate(
MFRC522::PICC_CMD_MF_
AUTH_KEY_A, block, &key,
&(mfrc522.uid));
      if (status !=
MFRC522::STATUS_OK)
       {
Serial.print("AUTENTICACI
ON FALLIDA ");
        lcd.clear();
        lcd.setCursor(1,0);

lcd.print("AUTENTICACION
");
        lcd.setCursor(4,1);
        lcd.print("FALLIDA");
        for (int i = 0; i<=8; i++)
        {
         digitalWrite(Led,
HIGH);
         delay(150);
         digitalWrite(Led,
LOW);
         delay(150);
        }
        Serial.print("POR
FAVOR REINTENTE
NUEVAMENTE ");
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print("TRATE
NUEVAMENTE");
        lcd.setCursor(4,1);
        lcd.print("POR
FAVOR");

//Serial.println(mfrc522.GetSt
atusCodeName(status));
        return;
       }

      // Read block
```

```
   byte byteCount =
sizeof(buffer);


   status =
mfrc522.MIFARE_Read(bloc
k, buffer, &byteCount);
   if (status !=
MFRC522::STATUS_OK)
     {

Serial.print("MIFARE_Read()
failed: ");

//Serial.println(mfrc522.GetSt
atusCodeName(status));
     }
      else  // Dump data
   {



      //transforma los 4
primeros numeros del bloque
0 en una variable
      //de 4 bytes para poderla
comparar con las
numeraciones registradas
      unsigned long card=0;
      byte b=0;
      for (int a=3;a>-1;a--) {
      switch (a){
      case 3:  card +=
buffer[b]*16777216; break;
      case 2:  card +=
buffer[b]*65536; break;
      case 1:  card +=
buffer[b]*256; break;
      case 0:  card +=
buffer[b];break;
      }
      b++;}

      boolean
encontrada=false;
       for (byte
a=0;a<numcards;a++) {
        if (rfid[a]==card) {

          //subir();

 Serial.print("connecting to ");

Serial.println("controlaccesoes
poch.ddns.net");

 // Use WiFiClient class to
create TCP connections
 WiFiClient client;
 const int httpPort = 80;
 if (!client.connect(host,
httpPort))
 {
 Serial.println("connection
failed");
 return;
 }
// We now create a URL for
the request
 String url
="http://192.168.1.60/users.ph
p";
 String dato1 = "?Id=";
 String dato2 = "&Nombre=";
 String dato3 = "&Facultad=";
 String dato4 = "&Modelo=";
 String dato5 = "&Placa=";
 String dato6 =
"&Tipo=IngresoB";
 String dato7 = individuo1[a];
 String dato8 = individuo2[a];
 String dato9 = individuo3[a];
 String dato10 =
individuo4[a];
 String dato11 =
individuo5[a];
 String dato12 =
individuo6[a];

 Serial.print("Accediendo a:
");

Serial.println("controlaccesoes
poch.ddns.net");
 delay(700);
 // This will send the request to
the server
 client.print(String("GET ") +
url + dato1 + dato7 + dato2 +
dato8  + dato3 + dato9 + dato4
+ dato10 + dato5 + dato11 +
dato6 + " HTTP/1.1\r\n" +
 "Host: " + host + "\r\n" +
 "Connection: close\r\n\r\n");
//Serial.print(String("GET ") +
url + dato1 + dato7 + dato2 +
dato8  + dato3 + dato9 + dato4
+ dato10 + dato5 + dato11 +
dato6 + "Connection:
close\r\n\r\n");
          saludo();

Serial.println(individuo6[a]);
          lcd.clear();
          lcd.setCursor(0,0);
```

```
lcd.print(individuo6[a]);
        lcd.setCursor(5,1);

lcd.print(individuo7[a]);
        delay(1500);
        autorizado();


        encontrada=true;}} //si el num de la tarjeta coincide
        //con alguno de los definidos nos dice el nombre o saludo
        if (encontrada) //autorizado();
        {Serial.println("PASE SU TARJETA POR FAVOR ");
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print("PASE SU TARJETA");
        lcd.setCursor(3,1);
        lcd.print("POR FAVOR");

digitalWrite(Led,HIGH);}
        else no_autorizado();


    for (byte index = 0; index < 18; index++)
    {

//Serial.print(buffer[index] < 0x10 ? " 0" : " ");
//Serial.print(buffer[index], HEX);
    if ((index % 4) == 3) Serial.print(" ");
    }

    }
    Serial.println(" ");
    mfrc522.PICC_HaltA(); // Halt PICC

mfrc522.PCD_StopCrypto1(); // Stop encryption on PCD

}
```

/**************** Modulo salida A **********************/**

```
#include <ESP8266WiFi.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <LiquidCrystal_I2C.h>
#include <Wire.h>

#define SS_PIN 4     //D2
#define RST_PIN 5    //D1
#define Led 16  //D0

LiquidCrystal_I2C lcd(0x27, 16, 2);

MFRC522 mfrc522(SS_PIN, RST_PIN);       // Crea la instancia MRFC522
Servo servoMotor;
WiFiServer server(80);

const char* ssid = "LAURA";
const char* password = "0602083693";
const char* host = "controlaccesoespoch.ddns.net";
//const char* host = "172.25.200.199";
//const char* url = "http://192.168.1.60/users.php";
//IPAddress server(192,168,1,60);
//const char* host = "www.google.com";

const int numcards=8; //numero de tarjetas rfids que hay definidas

//definimos los códigos de las tarjetas (4 primeros digitos en formato hexadecimal)
```

```
unsigned long
rfid[numcards]={0xB0C9027
4,0xC0631F83,0x10D59775,0
x808E8B75,0xE0AA9975,0x8
6528FBB,0xC6482A9E,0x56
B9B0BB};
//{0xB0C90274,0xC0631F83}


//aquí podemos introducir las
personas a la que pertenecen
los tarjetas


char*
individuo1[numcards]={"0607
564327","0609867843","0605
347213","0606845325","0607
844376","0604675669","0607
845312","0609986452"};

char*
individuo2[numcards]={"Ing.
MónicaZabala","Ing.LourdesZ
úñiga","Ing.LeticiaLara","Ing.
VerónicaMora","Ing.DavidMo
reno","Ing.FaustoCabrera","In
g.FabricioSantacruz","Ing.Rib
adeneira"};

char*
individuo3[numcards]={"FIE"
,"MECANICA","FADE","CIE
NCIAS","FIE","FIE","MECA
NICA","CIENCIAS"};

char*
individuo4[numcards]={"KIA
","CHEVROLET","HYUND
AI","YAMAHA","SUSUKI",
"MAZDA","HYUNDAI","KI
A"};

char*
individuo5[numcards]={"JNG
-876","JUL-945","DYC-
946","KLP-434","QCZ-
755","HGF-221","LMQ-
781","YTG-504"};

char*
individuo6[numcards]={"Ing.
Monica","Ing. Lourdes","Ing.
Leticia","Ing. Veronica","Ing.
David","Ing. Fausto","Ing.
Fabricio","Ing. Jefferson"};

char*
individuo7[numcards]={"Zaba
la","Zuñiga","Lara","Mora","
Moreno","Cabrera","Santacru
z","Ribadeneira"};


void setup()

{

      Serial.begin(9600);      //
Inicializa la comunicacion
serial con la PC

      SPI.begin();             //
Inicializa el SPI bus

      mfrc522.PCD_Init();
// Inicializa el lector
MFRC522

      servoMotor.attach(D8);
//D8

      pinMode(Led,OUTPUT);

      digitalWrite(Led,HIGH);

      conectar();

      Wire.begin(D4, D3);

      lcd.begin();

      lcd.clear();

      lcd.setCursor(0,0);

      lcd.print("PASE SU
TARJETA");

      lcd.setCursor(3,1);

      lcd.print("POR
FAVOR");

      Serial.println(" ");

      Serial.println("PASE SU
TARJETA POR FAVOR ");

      Serial.println(" ");

}


void conectar() {


  // Connect to WiFi network

  Serial.println();

  Serial.println();

  Serial.print("Conectando a
");

  Serial.println(ssid);


  WiFi.begin(ssid, password);


  while (WiFi.status() !=
WL_CONNECTED) {

    delay(500);

    Serial.print(".");

  }

 Serial.println("");

 Serial.println("WiFi
connected");

 Serial.println("IP address: ");

 Serial.println(WiFi.localIP());


}



void saludo()

{

  Serial.println("Acceso
Autorizado.");

  lcd.clear();

  lcd.setCursor(5,0);
```

```
  lcd.print("ACCESO");
  lcd.setCursor(3,1);
  lcd.print("AUTORIZADO");
  delay(2000);
  Serial.println("Bienvenido");
  lcd.clear();
  lcd.setCursor(2,0);
  lcd.print("HASTA
LUEGO");
  lcd.setCursor(2,1);
  lcd.print("TEN BUEN
DIA");
  delay(2000);
  Serial.println("Ten Buen Día
");
}


void autorizado ()
{
  int pos;
  int dist = 0;
  dist = analogRead(0);
  digitalWrite(Led,LOW);
  // Desplazamos a la posición
100º
  for(pos = 0; pos <= 100; pos
+= 1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  // Esperamos 3 segundo
  //delay(5000);
  for (int i = 0; i<=20; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
  // Desplazamos a la posición
180º
  if(dist < 300)
  {
  for(pos = 100; pos>=0; pos-
=1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  }
  else
  {
  for(pos = 0; pos <= 100; pos
+= 1)
  {
    servoMotor.write(pos);
    delay(15);
  }
  }
  for (int i = 0; i<=8; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
}


void no_autorizado()
{
  Serial.println("Acceso
Denegado");
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print("ACCESO
DENEGADO!");
  lcd.setCursor(0,1);
  lcd.print("SIN
AUTORIZACION");
  Serial.println("No tiene
Autorizacion");
for (int i = 0; i<=8; i++)
    {
      digitalWrite(Led, HIGH);
      delay(150);
      digitalWrite(Led, LOW);
      delay(150);
    }
}


void loop() {


        // Prepare key - all keys
are set to FFFFFFFFFFFFh at
chip delivery from the factory.

MFRC522::MIFARE_Key
key;
        for (byte i = 0; i < 6; i++)
key.keyByte[i] = 0xFF;
```

```
      // Look for new cards
      if ( ! mfrc522.PICC_IsNewCardPresent())
            {
             return;
            }

      // Select one of the cards
      if ( ! mfrc522.PICC_ReadCardSerial())    return;

      Serial.print("Tarjeta detectada");    //Dump UID
      Serial.println(" ");
      digitalWrite(Led, LOW);
      for (byte i = 0; i < mfrc522.uid.size; i++)
      {

//Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");

//Serial.print(mfrc522.uid.uidByte[i], HEX);
      }
      //Serial.print(" PICC type: ");   // Dump PICC type
      byte piccType = mfrc522.PICC_GetType(mfrc522.uid.sak);

//Serial.println(mfrc522.PICC_GetTypeName(piccType));

      byte buffer[18];
      byte block  = 0;
      byte status;

      status = mfrc522.PCD_Authenticate(MFRC522::PICC_CMD_MF_AUTH_KEY_A, block, &key, &(mfrc522.uid));
      if (status != MFRC522::STATUS_OK)
        {

Serial.print("AUTENTICACION FALLIDA ");
          lcd.clear();
          lcd.setCursor(1,0);

lcd.print("AUTENTICACION ");
          lcd.setCursor(4,1);
          lcd.print("FALLIDA");
          for (int i = 0; i<=8; i++)
          {
           digitalWrite(Led, HIGH);
           delay(150);
           digitalWrite(Led, LOW);
           delay(150);
          }
        Serial.print("POR FAVOR REINTENTE NUEVAMENTE ");
          lcd.clear();
          lcd.setCursor(0,0);
          lcd.print("TRATE NUEVAMENTE");
          lcd.setCursor(4,1);
          lcd.print("POR FAVOR");

//Serial.println(mfrc522.GetStatusCodeName(status));
          return;
        }

      // Read block
    byte byteCount = sizeof(buffer);

    status = mfrc522.MIFARE_Read(block, buffer, &byteCount);
    if (status != MFRC522::STATUS_OK)
      {

Serial.print("MIFARE_Read() failed: ");

//Serial.println(mfrc522.GetStatusCodeName(status));
      }
      else  // Dump data
    {

      //transforma los 4 primeros numeros del bloque 0 en una variable
      //de 4 bytes para poderla comparar con las numeraciones registradas
      unsigned long card=0;
      byte b=0;
```

```
      for (int a=3;a>-1;a--) {
      switch (a){
      case 3:  card += buffer[b]*16777216; break;
      case 2:  card += buffer[b]*65536; break;
      case 1:  card += buffer[b]*256; break;
      case 0:  card += buffer[b];break;
      }
      b++;}

      boolean encontrada=false;
       for (byte a=0;a<numcards;a++) {
        if (rfid[a]==card) {

          //subir();

 Serial.print("connecting to ");

Serial.println("controlaccesoespoch.ddns.net");

 // Use WiFiClient class to create TCP connections
 WiFiClient client;
 const int httpPort = 80;
 if (!client.connect(host, httpPort))
 {
 Serial.println("connection failed");
 return;
 }
// We now create a URL for the request
 String url ="http://192.168.1.60/users.php";
 String dato1 = "?Id=";
 String dato2 = "&Nombre=";
 String dato3 = "&Facultad=";
 String dato4 = "&Modelo=";
 String dato5 = "&Placa=";
 String dato6 = "&Tipo=SalidaA";
 String dato7 = individuo1[a];
 String dato8 = individuo2[a];
 String dato9 = individuo3[a];
 String dato10 = individuo4[a];
 String dato11 = individuo5[a];
 String dato12 = individuo6[a];

 Serial.print("Accediendo a: ");

Serial.println("controlaccesoespoch.ddns.net");
 delay(1400);
 // This will send the request to the server
 client.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + " HTTP/1.1\r\n" +
 "Host: " + host + "\r\n" +
 "Connection: close\r\n\r\n");
//Serial.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + "Connection: close\r\n\r\n");
        saludo();

Serial.println(individuo6[a]);
        lcd.clear();
        lcd.setCursor(0,0);

lcd.print(individuo6[a]);
        lcd.setCursor(5,1);

lcd.print(individuo7[a]);
        delay(1500);
        autorizado();

        encontrada=true;}} //si el num de la tarjeta coincide
        //con alguno de los definidos nos dice el nombre o saludo
        if (encontrada) //autorizado();
        {Serial.println("PASE SU TARJETA POR FAVOR ");
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print("PASE SU TARJETA");
        lcd.setCursor(3,1);
        lcd.print("POR FAVOR");

digitalWrite(Led,HIGH);}
```

```
        else no_autorizado();


      for (byte index = 0; index
< 18; index++)
      {

//Serial.print(buffer[index] <
0x10 ? " 0" : " ");
//Serial.print(buffer[index],
HEX);
        if ((index % 4) == 3)
Serial.print(" ");
        }


       }
        Serial.println(" ");
            mfrc522.PICC_HaltA();
// Halt PICC

mfrc522.PCD_StopCrypto1();
// Stop encryption on PCD

}
```

/**************** Modulo salida B **********************/**

```
#include <ESP8266WiFi.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include
<LiquidCrystal_I2C.h>
#include <Wire.h>


#define SS_PIN 4     //D2
#define RST_PIN 5    //D1
#define Led 16  //D0


LiquidCrystal_I2C lcd(0x27,
16, 2);


MFRC522 mfrc522(SS_PIN,
RST_PIN);        // Crea la
instancia MRFC522
Servo servoMotor;
WiFiServer server(80);


const char* ssid = "LAURA";
const char* password =
"0602083693";
const char* host =
"controlaccesoespoch.ddns.net
";
//const char* host =
"172.25.200.199";
//const char* url =
"http://192.168.1.60/users.php
";
//IPAddress
server(192,168,1,60);
//const char* host =
"www.google.com";


const int numcards=8;
//numero de tarjetas rfids que
hay definidas


//definimos los códigos de las
tarjetas (4 primeros digitos en
formato hexadecimal)


unsigned long
rfid[numcards]={0xB0C9027
4,0xC0631F83,0x10D59775,0
x808E8B75,0xE0AA9975,0x8
6528FBB,0xC6482A9E,0x56
B9B0BB};
//{0xB0C90274,0xC0631F83}
//aquí podemos introducir las
personas a la que pertenecen
los tarjetas


char*
individuo1[numcards]={"0607
564327","0609867843","0605
347213","0606845325","0607
844376","0604675669","0607
845312","0609986452"};
char*
individuo2[numcards]={"Ing.
MónicaZabala","Ing.LourdesZ
úñiga","Ing.LeticiaLara","Ing.
VerónicaMora","Ing.DavidMo
reno","Ing.FaustoCabrera","In
g.FabricioSantacruz","Ing.Rib
adeneira"};
char*
individuo3[numcards]={"FIE"
,"MECANICA","FADE","CIE
NCIAS","FIE","FIE","MECA
NICA","CIENCIAS"};
char*
individuo4[numcards]={"KIA
","CHEVROLET","HYUND
AI","YAMAHA","SUSUKI",
"MAZDA","HYUNDAI","KI
A"};
char*
individuo5[numcards]={"JNG
-876","JUL-945","DYC-
```

```
946","KLP-434","QCZ-755","HGF-221","LMQ-781","YTG-504"};

char* individuo6[numcards]={"Ing. Monica","Ing. Lourdes","Ing. Leticia","Ing. Veronica","Ing. David","Ing. Fausto","Ing. Fabricio","Ing. Jefferson"};

char* individuo7[numcards]={"Zabala","Zuñiga","Lara","Mora","Moreno","Cabrera","Santacruz","Ribadeneira"};


void setup()

{

      Serial.begin(9600);       // Inicializa la comunicacion serial con la PC

      SPI.begin();              // Inicializa el SPI bus

      mfrc522.PCD_Init();   // Inicializa el lector MFRC522

      servoMotor.attach(D8); //D8

      pinMode(Led,OUTPUT);

      digitalWrite(Led,HIGH);

      conectar();

      Wire.begin(D4, D3);

      lcd.begin();

      lcd.clear();

      lcd.setCursor(0,0);

      lcd.print("PASE SU TARJETA");

      lcd.setCursor(3,1);

      lcd.print("POR FAVOR");

      Serial.println(" ");

      Serial.println("PASE SU TARJETA POR FAVOR ");

      Serial.println(" ");


}


void conectar() {


  // Connect to WiFi network

  Serial.println();

  Serial.println();

  Serial.print("Conectando a ");

  Serial.println(ssid);


  WiFi.begin(ssid, password);


  while (WiFi.status() != WL_CONNECTED) {

    delay(500);

    Serial.print(".");

  }

 Serial.println("");

 Serial.println("WiFi connected");

 Serial.println("IP address: ");

 Serial.println(WiFi.localIP());


}



void saludo()

{

  Serial.println("Acceso Autorizado.");

  lcd.clear();

  lcd.setCursor(5,0);

  lcd.print("ACCESO");

  lcd.setCursor(3,1);

  lcd.print("AUTORIZADO");

  delay(2000);

  Serial.println("Bienvenido");

  lcd.clear();

  lcd.setCursor(2,0);

  lcd.print("HASTA LUEGO");

  lcd.setCursor(2,1);

  lcd.print("TEN BUEN DIA");

  delay(2000);

  Serial.println("Ten Buen Día ");

}


void autorizado ()

{

  int pos;

  int dist = 0;

  dist = analogRead(0);

  digitalWrite(Led,LOW);

  // Desplazamos a la posición 100º

  for(pos = 0; pos <= 100; pos += 1)

  {

    servoMotor.write(pos);
```

```
  delay(15);
 }
 // Esperamos 3 segundo
 //delay(5000);
 for (int i = 0; i<=20; i++)
  {
   digitalWrite(Led, HIGH);
   delay(150);
   digitalWrite(Led, LOW);
   delay(150);
  }
 // Desplazamos a la posición 180º
 if(dist < 300)
 {
 for(pos = 100; pos>=0; pos-=1)
 {
  servoMotor.write(pos);
  delay(15);
 }
 }
 else
 {
 for(pos = 0; pos <= 100; pos += 1)
 {
  servoMotor.write(pos);
  delay(15);
 }
 }
 for (int i = 0; i<=8; i++)
  {
   digitalWrite(Led, HIGH);
   delay(150);
   digitalWrite(Led, LOW);
   delay(150);
  }
}
void no_autorizado()
{
 Serial.println("Acceso Denegado");
 lcd.clear();
 lcd.setCursor(0,0);
 lcd.print("ACCESO DENEGADO!");
 lcd.setCursor(0,1);
 lcd.print("SIN AUTORIZACION");
 Serial.println("No tiene Autorizacion");
for (int i = 0; i<=8; i++)
  {
   digitalWrite(Led, HIGH);
   delay(150);
   digitalWrite(Led, LOW);
   delay(150);
  }
}

void loop() {

      // Prepare key - all keys are set to FFFFFFFFFFFFh at chip delivery from the factory.
MFRC522::MIFARE_Key key;
      for (byte i = 0; i < 6; i++) key.keyByte[i] = 0xFF;

      // Look for new cards
      if ( ! mfrc522.PICC_IsNewCardPresent())
            {
             return;
            }

      // Select one of the cards
      if ( ! mfrc522.PICC_ReadCardSerial())   return;

      Serial.print("Tarjeta detectada");   //Dump UID
      Serial.println(" ");
      digitalWrite(Led, LOW);
      for (byte i = 0; i < mfrc522.uid.size; i++)
      {
//Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
//Serial.print(mfrc522.uid.uidByte[i], HEX);
      }
      //Serial.print(" PICC type: ");   // Dump PICC type
      byte piccType = mfrc522.PICC_GetType(mfrc522.uid.sak);
```

```
//Serial.println(mfrc522.PICC
_GetTypeName(piccType));


      byte buffer[18];

      byte block  = 0;

      byte status;


      status =
mfrc522.PCD_Authenticate(
MFRC522::PICC_CMD_MF_
AUTH_KEY_A, block, &key,
&(mfrc522.uid));

      if (status !=
MFRC522::STATUS_OK)

       {


erial.print("AUTENTICACIO
N FALLIDA ");

        lcd.clear();

        lcd.setCursor(1,0);


lcd.print("AUTENTICACION
");

        lcd.setCursor(4,1);

        lcd.print("FALLIDA");

        for (int i = 0; i<=8; i++)

        {

         digitalWrite(Led,
HIGH);

         delay(150);

         digitalWrite(Led,
LOW);

         delay(150);

        }

        Serial.print("POR
FAVOR REINTENTE
NUEVAMENTE ");

        lcd.clear();

        lcd.setCursor(0,0);

        lcd.print("TRATE
NUEVAMENTE");

        lcd.setCursor(4,1);

        lcd.print("POR
FAVOR");


//Serial.println(mfrc522.GetSt
atusCodeName(status));

        return;

       }

          // Read block

   byte byteCount =
sizeof(buffer);

   status =
mfrc522.MIFARE_Read(bloc
k, buffer, &byteCount);

   if (status !=
MFRC522::STATUS_OK)

     {


Serial.print("MIFARE_Read()
failed: ");


//Serial.println(mfrc522.GetSt
atusCodeName(status));

      }

       else  // Dump data

   {



      //transforma los 4
primeros numeros del bloque
0 en una variable

      //de 4 bytes para poderla
comparar con las
numeraciones registradas

      unsigned long card=0;

      byte b=0;

      for (int a=3;a>-1;a--) {

      switch (a){

      case 3:  card +=
buffer[b]*16777216; break;

      case 2:  card +=
buffer[b]*65536; break;

      case 1:  card +=
buffer[b]*256; break;

      case 0:  card +=
buffer[b];break;

      }

      b++;}


      boolean
encontrada=false;

       for (byte
a=0;a<numcards;a++) {

        if (rfid[a]==card) {


          //subir();


 Serial.print("connecting to ");


Serial.println("controlaccesoes
poch.ddns.net");


 // Use WiFiClient class to
create TCP connections

 WiFiClient client;

 const int httpPort = 80;

 if (!client.connect(host,
httpPort))

 {
```

```
 Serial.println("connection failed");
 return;
 }
// We now create a URL for the request
 String url ="http://192.168.1.60/users.php";
 String dato1 = "?Id=";
 String dato2 = "&Nombre=";
 String dato3 = "&Facultad=";
 String dato4 = "&Modelo=";
 String dato5 = "&Placa=";
 String dato6 = "&Tipo=SalidaA";
 String dato7 = individuo1[a];
 String dato8 = individuo2[a];
 String dato9 = individuo3[a];
 String dato10 = individuo4[a];
 String dato11 = individuo5[a];
 String dato12 = individuo6[a];

 Serial.print("Accediendo a: ");

Serial.println("controlaccesoespoch.ddns.net");
 delay(1400);
 // This will send the request to the server
 client.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + " HTTP/1.1\r\n" +
 "Host: " + host + "\r\n" +
 "Connection: close\r\n\r\n");
//Serial.print(String("GET ") + url + dato1 + dato7 + dato2 + dato8  + dato3 + dato9 + dato4 + dato10 + dato5 + dato11 + dato6 + "Connection: close\r\n\r\n");
          saludo();

rial.println(individuo6[a]);
          lcd.clear();
          lcd.setCursor(0,0);

lcd.print(individuo6[a]);
          lcd.setCursor(5,1);

lcd.print(individuo7[a]);
          delay(1500);
          autorizado();

          encontrada=true;}} //si el num de la tarjeta coincide
          //con alguno de los definidos nos dice el nombre o saludo
          if (encontrada) //autorizado();
          {Serial.println("PASE SU TARJETA POR FAVOR ");
          lcd.clear();
          lcd.setCursor(0,0);
          lcd.print("PASE SU TARJETA");
          lcd.setCursor(3,1);
          lcd.print("POR FAVOR");

digitalWrite(Led,HIGH);}
          else no_autorizado();


      for (byte index = 0; index < 18; index++)
      {

//Serial.print(buffer[index] < 0x10 ? " 0" : " ");

//Serial.print(buffer[index], HEX);
      if ((index % 4) == 3) Serial.print(" ");
      }

     }
      Serial.println(" ");
      mfrc522.PICC_HaltA(); // Halt PICC

mfrc522.PCD_StopCrypto1(); // Stop encryption on PCD

}
```

Anexo E

Configuración en php de phpMyAdmin

```
# phpMyAdmin default Apache configuration

Alias /phpmyadmin /usr/share/phpmyadmin

<Directory /usr/share/phpmyadmin>
   Options SymLinksIfOwnerMatch
   DirectoryIndex index.php

   <IfModule mod_php5.c>
      <IfModule mod_mime.c>
         AddType application/x-httpd-php .php
      </IfModule>
      <FilesMatch ".+\.php$">
         SetHandler application/x-httpd-php
      </FilesMatch>

      php_value include_path .
      php_admin_value upload_tmp_dir /var/lib/phpmyadmin/tmp
      php_admin_value open_basedir /usr/share/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/usr/share/php/php-gettext/:/usr/share/php/php-php-gettext/:/usr/share/javascript/:/usr/share/php/tcpdf/:/usr/share/doc/phpmyadmin/:/usr/share/php/phpseclib/
      php_admin_value mbstring.func_overload 0
   </IfModule>
   <IfModule mod_php.c>
      <IfModule mod_mime.c>
         AddType application/x-httpd-php .php
      </IfModule>
      <FilesMatch ".+\.php$">
         SetHandler application/x-httpd-php
      </FilesMatch>

      php_value include_path .
      php_admin_value upload_tmp_dir /var/lib/phpmyadmin/tmp
      php_admin_value open_basedir /usr/share/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/usr/share/php/php-gettext/:/usr/share/php/php-gettext/:/usr/share/javascript/:/usr/share/php/tcpdf/:/usr/share/doc/phpmyadmin/:/usr/share/php/phpseclib/
      php_admin_value mbstring.func_overload 0
   </IfModule>

</Directory>

# Authorize for setup
```

```
<Directory
/usr/share/phpmyadmin/setup>
    <IfModule mod_authz_core.c>
      <IfModule mod_authn_file.c>
        AuthType Basic
        AuthName          "phpMyAdmin
Setup"
        AuthUserFile
/etc/phpmyadmin/htpasswd.setup
      </IfModule>
      Require valid-user
    </IfModule>
</Directory>

# Disallow web access to directories that
don't need it
<Directory
/usr/share/phpmyadmin/templates>
    Require all denied
</Directory>
<Directory
/usr/share/phpmyadmin/libraries>
    Require all denied
</Directory>
<Directory
/usr/share/phpmyadmin/setup/lib>
    Require all denied
</Directory>
```

Anexo F

Configuración en php de las páginas para establecer conexión con el servidor

```
<?php
//config.php para establecer comunicacion
//credenciales
$dbhost = 'localhost';
$dbuser = 'phpmyadmin';
$dbpass = 'raspbery';
$dbname = 'USERS';
//conexion con la base de datos
$con = mysqli_connect($dbhost, $dbuser, $dbpass, $dbname);
echo "DarioDB<br />";
echo "Pagina para establecer comunicación<br /> ";
echo "Modulo de comunicación --> DB phpMyadmin";
?>
```

```
<?php
//ingresoA.php para establecer comunicacion
//credenciales
$dbhost = 'localhost';
$dbuser = 'phpmyadmin';
$dbpass = 'raspbery';
$dbname = 'USERS';
//conexion con la base de datos
$con = mysqli_connect($dbhost, $dbuser, $dbpass, $dbname);
echo "DarioDB<br />";
echo "Pagina para establecer comunicación<br /> ";
echo "Modulo de comunicación --> DB phpMyadmin";
?>
```

```
<?php
//ingresoB.php para establecer comunicacion
//credenciales
$dbhost = 'localhost';
$dbuser = 'phpmyadmin';
$dbpass = 'raspbery';
$dbname = 'USERS';
//conexion con la base de datos
$con = mysqli_connect($dbhost, $dbuser, $dbpass, $dbname);
echo "DarioDB<br />";
echo "Pagina para establecer comunicación<br /> ";
echo "Modulo de comunicación --> DB phpMyadmin";
?>
```

```
<?php
//salidaA.php para establecer comunicacion
//credenciales
$dbhost = 'localhost';
$dbuser = 'phpmyadmin';
```

```
$dbpass = 'raspbery';
$dbname = 'USERS';
//conexion con la base de datos
$con = mysqli_connect($dbhost, $dbuser, $dbpass, $dbname);
echo "DarioDB<br />";
echo "Pagina para establecer comunicación<br /> ";
echo "Modulo de comunicación --> DB phpMyadmin";
?>
```

```
<?php
//salidaB.php para establecer comunicacion
//credenciales
$dbhost = 'localhost';
$dbuser = 'phpmyadmin';
$dbpass = 'raspbery';
$dbname = 'USERS';
//conexion con la base de datos
$con = mysqli_connect($dbhost, $dbuser, $dbpass, $dbname);
echo "DarioDB<br />";
echo "Pagina para establecer comunicación<br /> ";
echo "Modulo de comunicación --> DB phpMyadmin";
?>
```

Anexo G

Configuración en php de las páginas para subir los datos a la base de datos

```
<?php
//users.php
//importamos la configuracion
require("config.php");
//leemos los datos que nos llegan desde GET
$Id = mysqli_real_escape_string($con, $_GET['Id']);
$Nombre = mysqli_real_escape_string($con, $_GET['Nombre']);
$Facultad = mysqli_real_escape_string($con, $_GET['Facultad']);
$Modelo = mysqli_real_escape_string($con, $_GET['Modelo']);
$Placa = mysqli_real_escape_string($con, $_GET['Placa']);
$Tipo = mysqli_real_escape_string($con, $_GET['Tipo']);
//Se insertan los valores en la tabla
$query = "INSERT INTO Docentes(Id, Nombre, Facultad, Modelo, Placa, Tipo) VALUES('$Id', '$Nombre', '$Facultad', '$Modelo', '$Placa', '$Tipo')";
// Ejecutamos la instrucción
mysqli_query($con, $query);
mysqli_query($con);
echo "Pagina para almacenar BD<br />";
echo "<br />";
echo "<br />Id = $Id <br />";
echo "<br />Nombre = $Nombre <br />";
echo "<br />Facultad =$Facultad <br />";
echo "<br />Modelo = $Modelo <br />";
echo "<br />Placa = $Placa <br />";
echo "<br />Tipo = $Tipo <br />";
?>
```

Anexo H

Registros de la base de datos generados por el sistema

33	604675669	Ing.FaustoCabrera	CIENCIAS	MAZDA	HGF-221	IngresoA
34	605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoA
35	606845325	Ing.VerÃ³nicaMora	FIE	YAMAHA	KLP-434	IngresoA
36	604675669	Ing.FaustoCabrera	FIE	MAZDA	HGF-221	IngresoB
37	605347213	Ing.LeticiaLara	FADE	HYUNDAI	DYC-946	IngresoB
38	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB
39	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoB
40	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
41	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
42	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	SalidaA
43	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	SalidaA
47	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	SalidaA
48	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	SalidaA
49	607845312	Ing.FabricioSantacruz	MECANICA	HYUNDAI	LMQ-781	IngresoA
50	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
51	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
52	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
53	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
54	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
55	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoB
56	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB
57	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoB
58	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB
59	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB
60	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB
61	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
62	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
63	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
64	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoA
65	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
66	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	SalidaA
67	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	SalidaA
68	609867843	Ing.LourdesZÃºÃ±iga	MECANICA	CHEVROLET	JUL-945	IngresoA
69	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	SalidaA
70	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	SalidaB
71	607564327	Ing.MÃ³nicaZabala	FIE	KIA	JNG-876	IngresoB