



*“Responsabilidad con pensamiento positivo”*

**UNIVERSIDAD TECNOLÓGICA ISRAEL**

**TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:**

**INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES**

**TEMA:**

CONTROL ELECTRÓNICO PARA ENCENDIDO/BLOQUEO Y SEGURIDAD DE UN VEHÍCULO.

**AUTOR:**

RICARDO RAY RAMOS MONTERO

**TUTOR:** Ing. LUIS MONTOYA LARA, Mgs

**QUITO, ECUADOR  
2019**

## **DECLARACIÓN**

Yo, Ricardo Ray Ramos Montero declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondiente a este trabajo a la Universidad Tecnológica Israel, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

Ricardo Ray Ramos Montero

# UNIVERSIDAD TECNOLÓGICA ISRAEL

## APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación certifico:

Que el trabajo de titulación “**Control electrónico para encendido/bloqueo y seguridad de un vehículo.**”, presentado por el **Sr. Ricardo Ray Ramos Montero**, estudiante de la carrera de Electrónica Digital y Telecomunicaciones, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito DM, febrero del 2019

TUTOR

---

Ing. Luis Montoya Lara, Mg.

## **AGRADECIMIENTO**

El presente trabajo va dirigido con una expresión de gratitud a mi madre que con su sacrificio, sabiduría y consejos impulsó en mí una meta de estudio.

Para mis distinguidos maestros, mi tutor Ing. Luis Montoya y mis lectores Ing. Wilmer Albarracín, Ing. Flavio Morales, que, con nobleza y entusiasmo, vertieron todo su apostolado en mí.

A mi querida Universidad, porque en sus aulas recibí la ciencia más grande, el conocimiento.

## **DEDICATORIA**

Mi tesis la dedico con todo mi amor y cariño a mi amada madre por toda su entereza en darme aliento para perseverar en lo que me he propuesto en la vida, por creer en mi capacidad y aun que hemos pasado momentos difíciles en nuestras vidas, siempre me demostró estar alado mío brindándome su amor y comprensión.

También la presente es dedicada a una persona muy especial que ya no está conmigo para poder ver este logro, pero donde quiera que se encuentre sé que estará feliz por verme culminar esta etapa en mi vida.

## TABLA DE CONTENIDO

DECLARACIÓN.....	i
APROBACIÓN DEL TUTOR.....	ii
AGRADECIMIENTO .....	iii
DEDICATORIA.....	iv
TABLA DE CONTENIDO.....	v
LISTA DE FIGURAS.....	viii
LISTA DE TABLAS .....	x
RESUMEN.....	xi
ABSTRACT.....	xii
INTRODUCCIÓN.....	13
Antecedentes de la situación objeto de estudio.....	13
Planteamiento del problema.....	13
Justificación.....	15
Objetivo General.....	15
Objetivos Específicos.....	15
Alcance.....	15
Descripción de los capítulos.....	16
CAPÍTULO 1 .....	17
FUNDAMENTACIÓN TEÓRICA .....	17
1.1    Sistemas electrónicos de seguridad en llaves inteligentes.....	17
1.1.1 Llaves inteligentes.....	18
1.1.2 Aplicaciones en el campo vehicular.....	21
1.1.3 Importancia.....	26
1.1.4 Ventajas.....	27
1.2    Microcontroladores.....	27
1.2.1 Introducción.....	27
1.2.2 Microcontroladores AVR de ATMEL.....	30
1.2.3 Microcontrolador AVR 328P.....	30
1.2.4 Características AVR 328P.....	31
1.2.5 Programación mediante Arduino.....	32
1.2.6 Entorno de desarrollo.....	33
1.3    Tecnología de comunicación inalámbrica Bluetooth.....	34
1.3.1 Introducción.....	34

1.3.2 Definición .....	35
1.3.3 Características .....	35
1.3.4 Módulo Bluetooth HC-06 .....	36
1.4 Tecnología de comunicación GSM .....	39
1.4.1 Introducción .....	39
1.4.2 Módulo GSM/GPRS SIM800 .....	42
1.5 Módulo GPS UBLOX 6 .....	42
1.6 Detector de ruptura de vidrio .....	43
1.6.1 Introducción .....	43
1.6.2 Características .....	43
1.6.3 Sensor de vibración mecánica .....	44
1.6.4 Sensor de vibración piezoeléctrico .....	44
1.7 Aplicaciones para teléfonos inteligentes .....	45
1.7.1 Introducción .....	45
1.7.2 Definición .....	46
1.7.3 Características .....	47
1.7.4 Sistema Operativo Android .....	47
CAPÍTULO 2 .....	49
MARCO METODOLÓGICO .....	49
2.1 Modelos de investigación .....	49
2.2 Técnica de recolección de datos .....	50
CAPITULO 3 .....	51
PROPUESTA .....	51
3.1 Diseño del hardware .....	54
3.1.1 Etapa de entrada .....	54
3.1.2 Etapa de proceso y control .....	57
3.1.3 Etapa de salida .....	58
3.1.4 APP .....	59
3.2 Diseño del software .....	59
3.3 Presupuesto y materiales .....	60
3.4 Ventajas del control electrónico para encendido/bloqueo y seguridad de un vehículo .....	61
CAPITULO 4 .....	62
IMPLEMENTACIÓN .....	62
4.1 Desarrollo .....	62

4.1.1 Desarrollo del aplicativo.....	62
4.1.2 Desarrollo del software para microcontrolador 328P. ....	68
4.1.3 Desarrollo del hardware. ....	71
4.2 Implementación.....	74
4.3 Pruebas de funcionamiento. ....	82
4.3.1 Pruebas Locales por bluetooth. ....	82
4.3.2 Pruebas remotas por GSM/GPRS ....	83
4.4 Análisis de resultados .....	86
4.4.1 Análisis de resultados locales por bluetooth.....	86
4.4.2 Análisis de resultados remotos o por GPRS.....	87
4.4.3 Análisis de resultados remotos por GPS .....	88
CONCLUSIONES.....	89
RECOMENDACIONES .....	90
REFERENCIAS BIBLIOGRÁFICAS.....	91
ANEXOS.....	92



## LISTA DE FIGURAS

Figura. 1.1. Llave con transpondedor .....	19
Figura. 1.2. Transponder de vehículo .....	19
Figura. 1.3. Vista interna del transponder en una llave de auto. ....	20
Figura. 1.4. Esquema de funcionamiento del transponder. ....	21
Figura. 1.5. Ubicación de antenas. ....	22
Figura. 1.6. Llave electrónica Renault Laguna. ....	23
Figura. 1.7. Apertura de Puerta con llave inteligente. ....	24
Figura. 1.8. Coberturas de antenas externas. ....	24
Figura. 1.9. Cobertura de antenas Internas. ....	25
Figura. 1.10. Botón de encendido con llave inteligente. ....	26
Figura. 1.11. Antena de RF para manija de vehículo marca PREMO. ....	26
Figura. 1.12. Diagrama interno de bloques de un Microcontrolador. ....	28
Figura. 1.13. Microcontrolador PIC16F628A. ....	29
Figura. 1.14. Módulo Arduino. ....	30
Figura. 1.15. Distribución de pines ATmega328. ....	32
Figura. 1.16. Entorno IDE. ....	33
Figura. 1.17. Adafruit Blufuit. ....	37
Figura. 1.18. SparkFun ESP32. ....	37
Figura. 1.19. Módulo HC-06. ....	38
Figura. 1.20. Módulo HC-05. ....	39
Figura. 1.21. Módulo SIM800. ....	41
Figura. 1.22. Módulo GPS UBLOX 6 .....	43
Figura. 1.23. Sensor de vibración mecánico SW-18015P. ....	44
Figura. 1.24. Sensor de vibración Glass BREAK 5150. ....	45
Figura. 1.25. Aplicaciones para smartphone. ....	46
Figura. 3.26. Diagrama de bloques del software y hardware del dispositivo de seguridad. ....	53
Figura. 3.27. Diseño etapa de entrada, módulo bluetooth. ....	55
Figura. 3.28. Diseño etapa de entrada, módulo GPRS. ....	56
Figura. 3.29. Diseño etapa entrada, módulo GPS. ....	56
Figura. 3.30. Diagrama esquemático de conexión de sensores de ruptura con el microcontrolador. ....	57
Figura. 3.31. Diseño de la etapa de control, microcontrolador Atmega 328P. ....	58
Figura. 3.32. Flujograma del funcionamiento del dispositivo de seguridad. ....	59
Figura. 4.33. Muestra los dispositivos bluetooth cercanos al smartphone. ....	63
Figura. 4.34. Conexión con el bluetooth seleccionado. ....	63
Figura. 4.35. Botón para seleccionar bluetooth. ....	63
Figura. 4.36. Lista de dispositivos bluetooth disponibles. ....	64
Figura. 4.37. Programación botón abrir seguros del vehículo. ....	65
Figura. 4.38. Programación botón cerrar seguros del vehículo. ....	65
Figura. 4.39. Programación botón para bajar una ventana del vehículo. ....	66
Figura. 4.40. Programación botón desconectar. ....	66
Figura. 4.41. Programación botón cerrar aplicación. ....	67
Figura. 4.42. Programación para alerta audible por desconexión entre el smartphone y el dispositivo de seguridad. ....	68

Figura. 4.43. Aplicativo instalado en smartphone. ....	68
Figura. 4.44. Interfaz de programación portable versión 1.6.11 de Arduino. ....	69
Figura. 4.45. Mensaje de compilación exitosa en el IDE de Arduino. ....	70
Figura. 4.46. Carga de programación al Atmega 328P. ....	71
Figura. 4.47. Diseño de placa PCB. ....	73
Figura. 4.48. Simulación 3D de la placa del dispositivo de seguridad. ....	74
Figura. 4.49. Soldadura de los elementos del dispositivo de seguridad. ....	74
Figura. 4.50. Montaje de módulos en placa PCB. ....	75
Figura. 4.51. Módulo Sim800 con <i>Sim Card</i> . ....	75
Figura. 4.52. Módulo <i>Step Down</i> LM2596. ....	76
Figura. 4.53. Módulo de relés de 8 canales. ....	77
Figura. 4.54. Placa PCB montada en superficie plana para pruebas. ....	77
Figura. 4.55. Vehículo de pruebas e implementación. ....	78
Figura. 4.56. Instalación provisional para verificar funcionamiento del dispositivo. ....	78
Figura. 4.57. Diseño del <i>enclosure</i> para placa ABS. ....	79
Figura. 4.58. Parte posterior de la guantera. ....	79
Figura. 4.59. Instalación sensor de vibración. ....	80
Figura. 4.60. Conexión a módulo de bloqueo central. ....	80
Figura. 4.61. Circuitos de bocina y ventana del conductor. ....	81
Figura. 4.62. Bomba de gasolina del vehículo. ....	82
Figura. 4.63. Pruebas remotas o GSM/GPRS. ....	84
Figura. 4.64. Pruebas GSM/GPRS con las tres operadoras celulares. ....	86
Figura. 4.65. Pruebas de alcance de conexión módulo bluetooth. ....	86

## LISTA DE TABLAS

Tabla. 1.1. Parámetros básicos de funcionamiento ATmega328P. ....	32
Tabla. 1.2. Tabla comparativa dispositivos bluetooth. ....	38
Tabla. 1.3. Comparación económica Sim800 – Sim900.....	41
Tabla. 1.4. Diferencia entre Android e iOS.....	48
Tabla. 3.5. Consumo de corriente de los dispositivos del módulo de seguridad.....	52
Tabla. 3.6. Tabla de materiales y costos de los elementos electrónicos. ....	61
Tabla. 4.7. Pruebas de distancia módulo Bluetooth HC-06 .....	87
Tabla. 4.8. Verificación de funcionamiento remoto del dispositivo de control electrónico. .....	87
Tabla. 4.9. Señal celular en subsuelos. ....	88
Tabla. 4.10. Pruebas de cobertura GPS.....	88

## **RESUMEN**

Para los usuarios que tiene vehículos es de mucha importancia reducir al mínimo el riesgo de robo de sus autos, debido a que un vehículo es una inversión económicamente alta siempre se está en una búsqueda constante de algún dispositivo electrónico que permita tener una mayor fiabilidad en seguridad para proteger el bien.

La importancia de un control electrónico para encendido/bloqueo y seguridad de un vehículo, para prevenir un eventual robo es brindar al propietario la confianza y tranquilidad de que su vehículo está protegido mediante un dispositivo electrónico que proporcionará las acciones necesarias para alertar e impedir el hurto del vehículo.

En este escrito se presenta información relevante de los componentes que conforman el control electrónico para encendido/bloqueo y seguridad de un vehículo, el desarrollo y la implementación del dispositivo para el trabajo asignado.

**Palabras clave:** Microcontrolador, GSM, GPS, Bluetooth, APP, Arduino, Android.

## **ABSTRACT**

For the users that have vehicles, it is very important to minimize the risk of theft of their cars, because a vehicle is an economically high investment, it is always in a constant search of some electronic device that allows to have a greater reliability in security to protect it.

The importance of an electronic control for ignition / locking and security of a vehicle, to prevent an eventual theft is to provide the owner with the confidence and tranquility that his vehicle is protected by an electronic device that will provide the necessary actions to alert and prevent theft vehicle.

In this document, relevant information is presented on the components that make up the electronic control for ignition / blocking and safety of a vehicle, the development and implementation of the device for the assigned work.

**Keyword:** Microcontroller, GSM, GPS, Bluetooth, APP, Arduino, Android

## **INTRODUCCIÓN**

En la evolución de la humanidad existen muchos momentos históricos, los cuales han sido el punto de partida del nacimiento de nuevas tecnologías que han sido diseñadas por la exigencia del ser humano en proteger sus bienes.

A medida que la sociedad se actualiza tecnológicamente, la seguridad electrónica crece constantemente, la cual se basa en diversos productos que sustentan dispositivos que permiten tener un mayor control sobre los bienes a proteger.

El objeto de estudio del presente proyecto es brindar al público en general que poseen vehículos, tener el control local y remoto de la seguridad de su auto por medio de la seguridad electrónica.

### **Antecedentes de la situación objeto de estudio**

Los consumidores en el país no cuentan con un dispositivo electrónico capaz de reunir varios servicios de seguridad en uno solo y de bajo costo comercial que pueda alertar y prevenir el robo de vehículos, razón por la cual los usuarios están en una constante búsqueda del dispositivo que pueda integrar varias funciones en un mismo módulo sin tener que adquirir por separado la prestación de un servicio de seguridad.

### **Planteamiento del problema**

Ecuador actualmente es uno de los países en los cuales el parque automotor ha crecido considerablemente, es muy común que, con este crecimiento, también aumente el robo de vehículos.

Cuando sucede el robo de un vehículo lo primero que las personas tienden a hacer es llamar a la policía para recibir la ayuda respectiva, obviamente en este proceso se pierden minutos importantes en los que la policía comienza a pedir datos como placas, marca, modelo color, nombre del propietario y la dirección donde ocurrió el hecho. Estos minutos son muy importantes posterior al robo del vehículo ya que los delincuentes tienen más tiempo para huir y por ende para llegar más lejos.

Así también, es muy común que los usuarios de vehículos tienden a olvidar las llaves dentro del mismo. Se pierde tiempo y dinero en buscar auxilio para poder abrir el seguro de la puerta o una ventana para poder ingresar y obtener la llave, además de que se pueden causar daños de pintura, cerraduras y molduras del auto por tratar de abrir a la fuerza el vehículo.

Todos estos inconvenientes como robo u olvidar las llaves dentro del vehículo son situaciones diarias que suceden en la ciudad y en el país, por lo que las personas que poseen vehículo están propensas a este tipo de calamidades en su cotidiano vivir.

En estos días, las personas usuarias de dispositivos móviles no se despojan de su teléfono celular, por lo que es un dispositivo electrónico que puede ser muy útil y que siempre lo tiene cerca para muchos fines como son llamadas telefónicas, juegos y una de las más comunes que es el uso de la cámara de fotos. En este caso se va a direccionar este dispositivo móvil para tener un uso adicional como es el bloqueo del vehículo y la apertura del vehículo en el caso de haber olvidado las llaves dentro de él, así se tendrá una herramienta instantánea para solucionar este tipo de eventos.

El presente proyecto de tesis de grado titulado Control electrónico para encendido/bloqueo y seguridad de un vehículo, se enfoca en el diseño de un dispositivo de seguridad electrónico capaz de prevenir y alertar el robo vehicular, con la capacidad de ser instalado en cualquier tipo de vehículo que exista en el mercado, adicionalmente el desarrollo de un aplicativo para ser instalado en cualquier tipo de teléfono celular que posea sistema operativo Android.

## Justificación

El presente proyecto busca ser un aporte a la sociedad, la seguridad es de suma importancia para proteger los bienes que las personas adquieren con sacrificio, es por eso que mediante el dispositivo de control electrónico para encendido/bloqueo y seguridad de un vehículo se quiere reducir en lo mínimo posible el hurto de cualquier tipo de vehículo donde el dispositivo sea instalado, teniendo también bondades adicionales las cuales pretende ser un dispositivo de seguridad completo que resguarde el vehicule ante cualquier eventualidad de robo.

## Objetivo General

Desarrollar un control electrónico para encender/bloquear y monitorear la seguridad de un vehículo mediante distintos módulos electrónicos que indican vía SMS al usuario cuando el vehículo se encuentra en riesgo de robo.

## Objetivos Específicos

- Definir los parámetros y dispositivos que van a ser utilizados para la ejecución del sistema.
- Diseñar la tarjeta de control utilizando el microcontrolador AVR328P.
- Desarrollar la etapa de comunicación vía *bluetooth* y GSM/GPRS del sistema electrónico hacia el *smartphone*.
- Programar una aplicación en el *smartphone* en Android para la ejecución de comando locales y la recepción de los eventos de seguridad del vehículo vía SMS.
- Implementar pruebas de valoración y funcionamiento del control electrónico en el vehículo.

## Alcance

Esta investigación forma parte del desarrollo de sistemas electrónicos y TIC aplicados a la necesidad de la producción y di dispositivos electrónicos de seguridad vehicular, es vinculante con el área de Ciencias de la Ingeniería, el cual consiste en la elaboración de un



dispositivo de control electrónico encendido/apagado y seguridad de un vehículo, el cual estará en la capacidad de permitir encender o apagar un vehículo por medio de un *smartphone*, el cual realiza las funciones de una llave inteligente, por medio de comunicación *bluetooth*.

Además, permitirá la apertura y cierre de los seguros de la puerta del conductor, bajar una ventana del vehículo en caso de haber dejado dentro las llaves. Así también permitirá conocer cuando una de las ventanas del vehículo haya sido rota, también enviará vía mensaje de texto la alerta de luces encendidas

El dispositivo también está en la capacidad de gestionar que se active el pito en caso de no poder encontrarlo en determinada área, conocer la ubicación geográfica del vehículo por medio del posicionamiento global y por último podrá remotamente bloquear la bomba de gasolina del vehículo para que no pueda movilizarse.

### **Descripción de los capítulos**

La investigación tiene una introducción que detalla la situación objeto del estudio, así como el planteamiento del problema, su justificación, el objetivo general, los objetivos específicos y el alcance del presente proyecto.

A continuación, trae el Capítulo I que contiene la fundamentación teórica del proyecto, el Capítulo II que describe el marco metodológico utilizado en dirección a la consecución del proyecto. El Capítulo III se encuentra la propuesta que se presenta hacia la elaboración del proyecto y por último el Capítulo IV, la implementación del Proyecto.

Al finalizar se detallan las conclusiones, recomendaciones las referencias bibliográficas y los anexos del proyecto.

# CAPÍTULO 1

## FUNDAMENTACIÓN TEÓRICA

### 1.1 Sistemas electrónicos de seguridad en llaves inteligentes

Los sistemas electrónicos de seguridad electrónica pueden ser definidos como el conjunto de elementos e instalaciones necesarias para evitar y proporcionar robo, atracos o sabotaje de bienes materiales.

La seguridad electrónica en el resguardo de edificaciones, vehículos y personas funciona a través de elementos como circuitos telefónicos, cámaras de seguridad, controles de acceso, etc. Mismos que son controlados a través de diferentes tipos de infraestructuras como lo son, redes locales a través de cableado estructurado, redes WAN por medio de fibra óptica, e infraestructuras inalámbricas, la más extensa la telefonía celular.

La expresión “sistemas electrónicos de seguridad” comúnmente se la relaciona con alarmas contra robos para domicilios, pues, a decir verdad, ese concepto es muy simple y deteriora el verdadero significado de un sistema de seguridad.

Con el avance de la tecnología la seguridad física se ha apoyado en la seguridad electrónica ya que por medio de dispositivos electrónicos se puede tener un control de los diferentes sitios u objetos que se quiere resguardar. De este modo la seguridad electrónica proporciona una variedad de posibilidades para ser integradas al cotidiano vivir.

Actualmente se puede decir que ya no es un lujo sino una necesidad el proteger los bienes, por lo que el sector automotriz ha desarrollado las llaves inteligentes llamadas Smart Keys, esto con el fin de dar seguridad al propietario del vehículo en el aspecto de que sólo se encenderá cuando la llave inteligente esté cerca del auto.

Este dispositivo de seguridad electrónica es instalado en el vehículo para ofrecer al usuario la posibilidad de llevar la *Smart Key* en el bolsillo, sin necesidad de usarla como comúnmente se realiza en la mayoría de los autos, es decir sacar la llave, ingresarla en la cerradura y girarla para accionar el encendido del vehículo.

Hay que tener en cuenta que solo ciertos vehículos traen esta tecnología, que va ligada a un botón de encendido del auto. Por lo general, los autos que son los más vendidos y de tamaño pequeño son los que traen equipamiento básico, incluyendo el tema de seguridad.

Uno de los factores que hace que no todos los vehículos puedan tener esta tecnología es el costo, ya que al agregar más dispositivos de seguridad y de tecnología más avanzada hacen que el costo del vehículo sea mayor, por tal motivo los fabricantes no lo agregan ya que mientras un vehículo tenga un menor valor para su venta, tendrán más ventas y por ende más utilidades.

Este tipo de tecnología esta echa para tener cierta seguridad vehicular, es decir si no hay llave inteligente el vehículo no enciende, pero esto no quiere decir que no se pueda hacer un *bypass* en el circuito del arranque para encenderlo, con lo cual en una acción de robo el vehículo podrá ser movilizado.

El funcionamiento de las llaves electrónicas de diferentes casas comerciales de vehículos es similar, pero como ya se ha mencionado, no se va a impedir un robo, por lo que es necesario ir más allá de un simple encendido para poder desarrollar una herramienta que sirva como una verdadera llave electrónica que resguarde el vehículo cuando el dueño no esté cerca del mismo.

### **1.1.1 Llaves inteligentes**

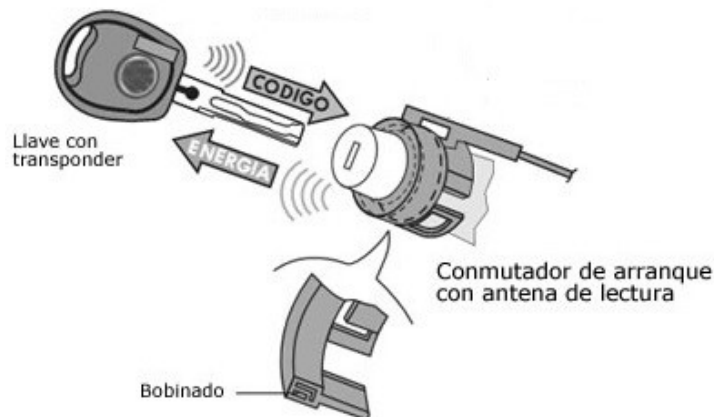
Los sistemas de llaves inteligentes o Smart Keys fueron introducidos en el mercado automotriz en el año de 1994 como un sistema antirrobo asociado a la llave de encendido como se puede observar en la Figura 1.1. La llave del vehículo contenía un chip electrónico llamado transponder en la carcasa de manera que cuando se ponía en contacto el auto, éste

leía la información del chip, si la reconocía iba a permitir el arranque del auto (Duplirapid, 2019).



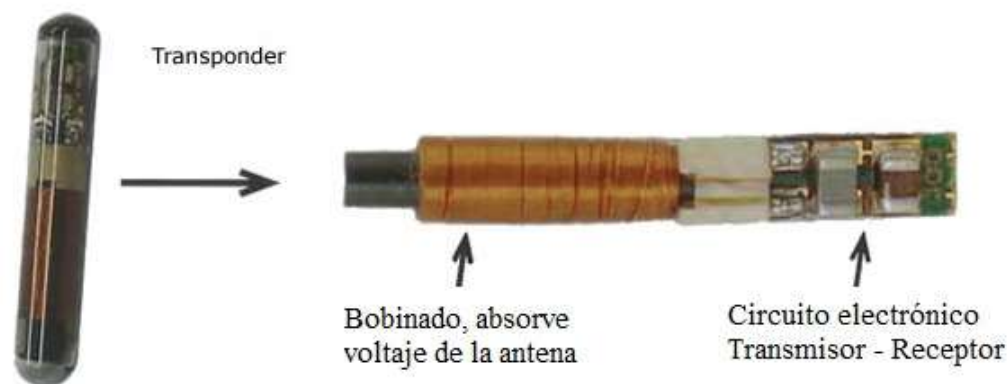
**Figura. 1.1. Llave con transpondedor**  
Fuente: (Mundo llaves, 2018).

Un Transpondedor o *transponder* es un dispositivo electrónico inalámbrico de control que recibe y responde automáticamente una señal entrante emitida por una antena lectora, como se puede observar en la Figura 1.2. En los vehículos la antena lectora es el aro alrededor de la bocallave de la cerradura de arranque, esta señal es leída y va al cerebro del vehículo para permitir el encendido.



**Figura. 1.2. Transponder de vehículo**  
Fuente: (Aficionados a la mecánica, 2016).

La antena que se encuentra en la cerradura del arranque del vehículo funciona como una fuente de bajo voltaje que emite al transponder cuando está cerca, como se observa en la Figura 1.3, de esta manera alimenta otro al bobinado que recoge esta señal eléctrica para encender el circuito transmisor - receptor del *transponder* y así poder leer la información que tiene.



**Figura. 1.3. Vista interna del transponder en una llave de auto.**  
Fuente: (Aficionados a la mecánica, 2016).

Un *transponder* de este tipo no cuenta con batería para alimentar los circuitos que lleva internamente, la alimentación se la hace como se lo describió anteriormente, el rango de proximidad para tener la alimentación de la antena al transponder es de 1 a 15cm. A esta distancia el campo magnético que se crea por la antena es suficiente para encenderlo y establecer la comunicación que se requería, como se observa en la Figura 1.4 (Dani, 2016).

Existen tres tipos de transponder:

### 1. Transponder con código fijo

Son los que en cada ocasión que son interrogados por el inmovilizador del vehículo, responden al mismo código.

### 2. Transponder Crypto

Son los mismos *transponder* de código fijo, pero cuando son interrogados por el inmovilizador responden al mismo código con la diferencia de que va encriptado. En este caso se podrán activar o programar *transponders* iguales a los de la llave original mediante equipos especiales.

### 3. Transponder de código evolutivo

Son *transponders* que en cada ocasión que son interrogados por el inmovilizador del vehículo, responden con un código diferente en base a un algoritmo de evolución. Éste es el sistema más seguro por lo que hasta la actualidad la usan varias marcas.

De esta manera en aquellos tiempos el auto disponía de un doble sistema de seguridad, cuando el transponder tomaba lectura del código que la llave llevaba y era comparado con el código que tenía almacenado en la unidad del inmovilizador, éste permitía el arranque del auto; así mientras la llave no tenga el *transponder* en el mango de ésta el auto emitiría un testigo de arranque en el panel que estaría indicando que no se puede encender el vehículo.

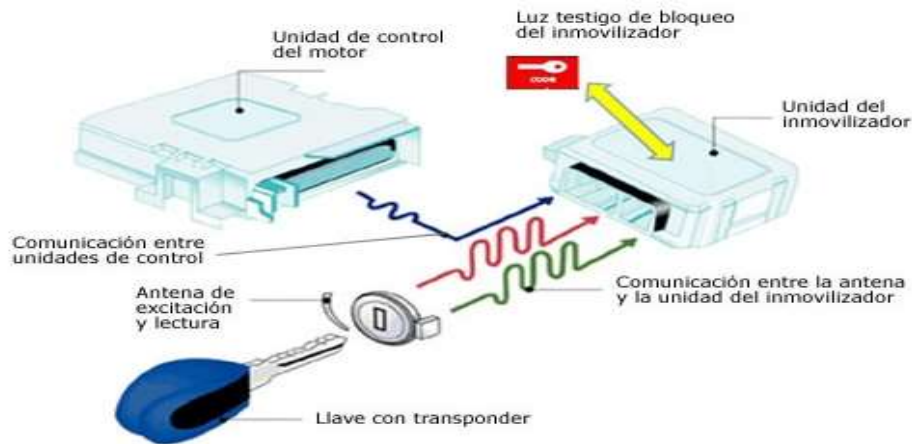


Figura. 1.4. Esquema de funcionamiento del transponder.  
Fuente: (Aficionados a la mecánica, 2016).

Prácticamente los autos posteriores a 1994 traían este tipo de tecnología, la cual fue base para el funcionamiento de las actuales *Smart keys* que existen en el mercado.

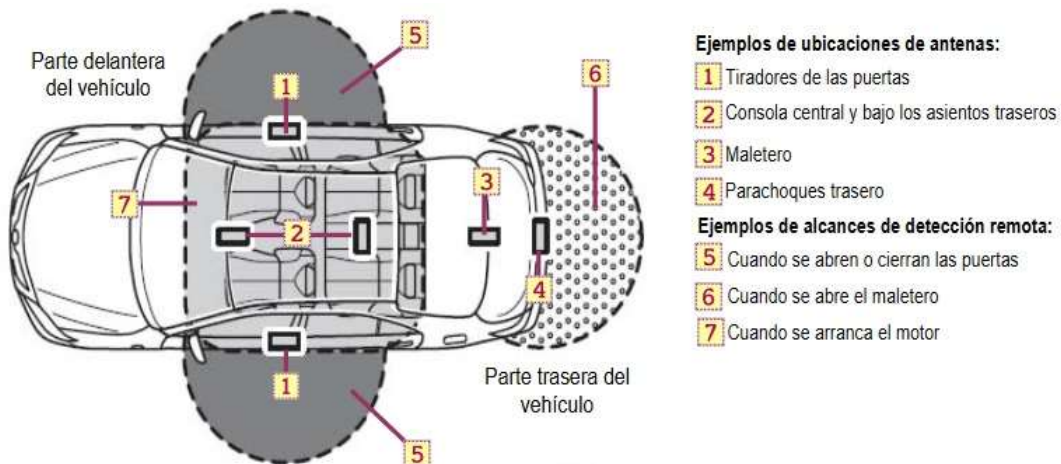
#### 1.1.2 Aplicaciones en el campo vehicular.

Las llaves inteligentes o *Smart keys* permiten abrir o cerrar puertas y arrancar el motor del vehículo sin la necesidad de utilizar una llave tradicional. Funciona mediante un circuito que está alojado en la *Smart Key* y un sistema de antenas especiales que están distribuidas en todo el vehículo.

Los sistemas de llave inteligente trabajan mediante una comunicación bidireccional entre la *Smart Key* y dichas antenas. La llave inteligente transmite ciertas señales al vehículo cuando se seleccionan manualmente, es decir, si presiono el botón que se encuentra en las manijas de las puertas del auto se puede abrir los seguros para poder acceder a él.

Esta comunicación va a estar activa siempre y cuando la llave inteligente se encuentre dentro del alcance operativo especificado en las antenas del sistema, es decir cuando se establece la comunicación es cuándo inician las acciones descritas anteriormente.

En la figura 1.5, se puede ver una distribución común de las antenas para la llave inteligente dentro de un automóvil.



**Figura. 1.5. Ubicación de antenas.**  
Fuente: (Boston Scientific, 2008).

Renault, fue la primera empresa automotriz en apostar por esta tecnología, en su auto modelo Laguna como se aprecia en la Figura 1.6. En sus inicios este sistema dio muchos inconvenientes ya que se provocaban muchas interferencias con otros dispositivos de radiofrecuencia y más aún si el vehículo estaba cerca de inhibidores de frecuencia. Durante el proceso de perfeccionamiento del sistema hubo varios fabricantes que alertaban con posibles interferencias con teléfonos móviles sino también con marcapasos.



**Figura. 1.6. Llave electrónica Renault Laguna.**  
Fuente: (SoliDrop, 2019).

Actualmente este sistema ha evolucionado y es muy raro que se den estos inconvenientes y ahora las llaves inteligentes son compatibles con los teléfonos celulares o con manos libres, en fin, la compatibilidad es extensa con los diferentes dispositivos que funcionan a través de radiofrecuencia.

Este inconveniente se lo resuelve a través del funcionamiento de los sistemas RFID, los cuales tienen un sistema anticolidión en caso de existir más dispositivos que emitan señales de radio frecuencia en la misma frecuencia que se está trabajando.

Una vez superados los inconvenientes de funcionamiento, la utilización de este dispositivo electrónico de seguridad ha venido a ser un instrumento de comodidad y seguridad, esto se debe a que el usuario solo debe llevar la *Smart Key* en su bolsillo para acceder a las funciones que este posee.

- Apertura de puertas

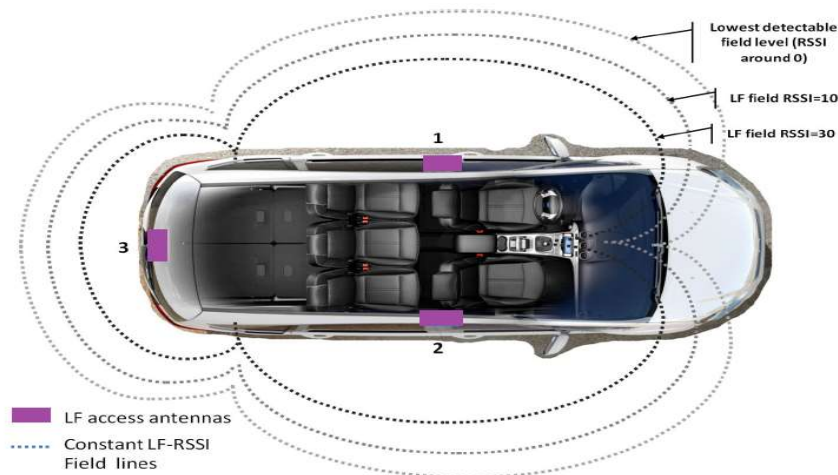
La simplicidad de esta función se basa en acercarse al vehículo y presionar el botón que se encuentra en la manija para poder ingresar al auto. La llave inteligente solo debe estar en el bolsillo, cartera, etc. Aunque también se la puede abrir de la manera tradicional que es presionando el botón de apertura de la *Smart Key* tal como se aprecia en la Figura 1.7.





**Figura. 1.7. Apertura de Puerta con llave inteligente.**  
**Fuente: (Holis brothers auto repair, 2019).**

Para este fin existen antenas colocadas en las manijas de las puertas, en la mayoría de los vehículos actuales las antenas vienen instaladas en la puerta del chofer, del copiloto y de la puerta del baúl, como se muestra en la Figura 1.8.

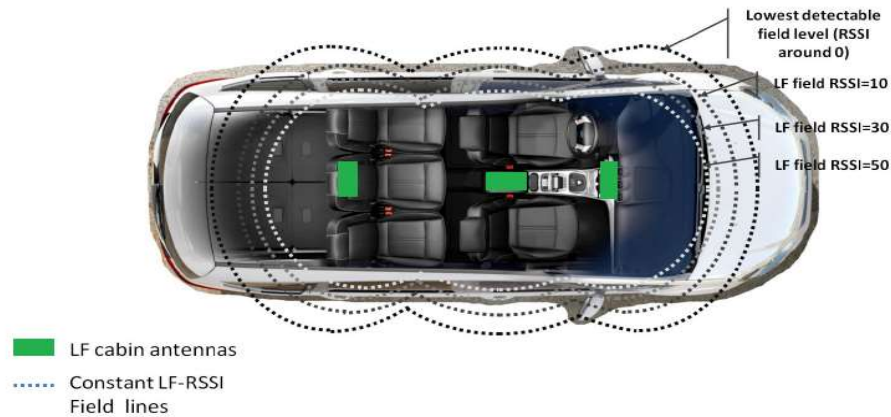


**Figura. 1.8. Coberturas de antenas externas.**  
**Fuente: (Jorge Rodríguez, 2016).**

De esta manera, el acceder al interior del vehículo es una forma muy sencilla y simple de poder hacerlo, más aún cuando se tiene algún tipo de objeto que se lo está cargando, elimina completamente la necesidad de sacar el control del auto para emitir la señal y que las puertas se abran. Basta con presionar el botón de la manija y la puerta se abrirá instantáneamente.

- Encendido del vehículo

Esta acción también se la desarrolla de manera muy sencilla, una vez dentro del vehículo, las antenas internas del mismo sabrán que la llave inteligente es portada por el usuario y que está listo para arrancar el vehículo, como se muestra en la Figura 1.9.



**Figura. 1.9. Cobertura de antenas Internas.**  
Fuente: (Jorge Rodríguez, 2016).

Para vehículos de transmisión manual, se debe presionar el embrague con lo cual el led indicador del botón de arranque pasara de un color rojo a verde, esto indica que puede presionar el botón para encender el vehículo, como se aprecia en la Figura 1.10.

En cambio, para vehículos con transmisión automática, debe presionar el freno del vehículo siempre y cuando la palanca se encuentre en modo *Parking*, de la misma manera el led indicador en el botón de arranque pasará de color rojo a verde indicando que se puede encender el auto con tan solo presionarlo.

Lo anteriormente descrito es el proceso para todos los vehículos, sean de transmisión manual o automática debido a que el usuario no puede llegar y presionar directamente el encendido del vehículo porque podría causar algún tipo de accidente.



**Figura. 1.10. Botón de encendido con llave inteligente.**  
Fuente: (Chevrolet, 2019).

Dependiendo del fabricante las antenas que reciben la información de la llave inteligente varía, un ejemplo es la antena de la marca Premo, como se aprecia en la Figura 1.11, dependiendo del modelo existen variantes como la distancia de recepción que varía entre los 30 y 50cm, alto impacto de absorción mecánica y sobre todo que trabaja en forma *wake up*, lo que significa que tiene un ahorro muy bajo de consumo hasta entrar en contacto con la *Smart Key*.



**Figura. 1.11. Antena de RF para manija de vehículo marca PREMO.**  
Fuente: PREMO (2019).

### 1.1.3 Importancia

Con el avance de la tecnología, la electrónica pretende simplificar acciones que el ser humano tiene en su vida diaria. La llave inteligente es uno de ellos, a nivel mundial este sistema cobra cada día más fuerza ya que aparte de ser una de las últimas tecnologías en los automóviles en cuanto a seguridad, permite que solo con un toque se pueda acceder y encender, generando un confort para el usuario (Premo, 2019).

Este tipo de seguridad electrónica es de suma importancia porque reduce el proceso de lidiar con la llave para la apertura de las puertas, así como también para encender el vehículo.

Esta herramienta de confort se enfoca en el hecho de que el vehículo no se va a encender si no se tiene la llave inteligente dentro del área de cobertura, lo cual implica que es un sistema de seguridad que el vehículo posee en caso de querer ser hurtado, el mismo que desactivará alguna función específica del automotor (ignición, bomba de gasolina, etc.) y que no permitirá que éste se encienda.

Actualmente es difícil poder clonar una llave inteligente por lo que se convierte en una herramienta eficaz en proteger a los vehículos que traen este sistema, es uno de los dispositivos inmovilizadores de anti-atraco que más seguridad brinda al vehículo en caso de querer ser sustraído, es por eso la mayoría de fabricantes lo empieza a implementar gradualmente.

#### **1.1.4 Ventajas**

Una de las ventajas principales es la incapacidad de encender el vehículo si no se tiene la llave inteligente, a decir verdad, es la característica más importante de este sistema, al ser una señal de radiofrecuencia codificada es casi imposible de duplicarla, esto hace que la llave inteligente sea un método eficaz para la inmovilización del vehículo.

Otra ventaja muy característica del sistema es que cuando el usuario se aleja del vehículo y olvida poner los seguros, el dispositivo lo cerrará automáticamente, con esto se tendrá la tranquilidad de que el auto se encuentra protegido.

### **1.2 Microcontroladores**

#### **1.2.1 Introducción**

Un microcontrolador (abreviado  $\mu\text{C}$ , UC o MCU) es un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria. Está compuesto de

varios bloques funcionales, los cuales cumplen una tarea específica. Un microcontrolador incluye en su interior las tres principales unidades funcionales de una computadora: unidad central de procesamiento, memoria y periféricos de entrada/salida, tal cual se aprecia en la Figura 1.12.

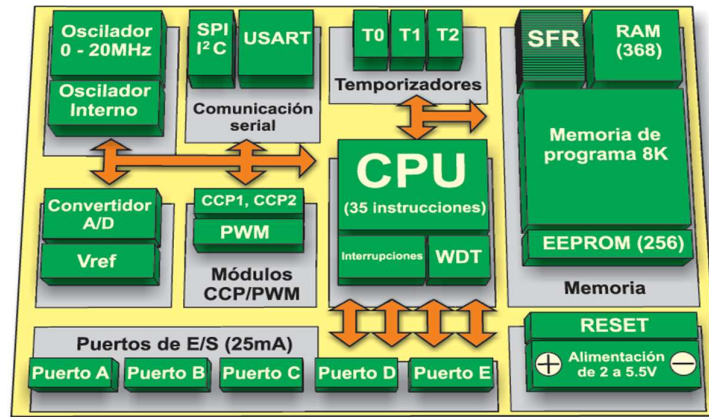


Figura. 1.12. Diagrama interno de bloques de un Microcontrolador.  
Fuente: (MikroElektronika, 2019).

Como el *hardware* ya viene integrado en un solo chip, para ser usado se debe especificar su funcionamiento por *software* a través de algoritmos que indiquen las instrucciones que el microcontrolador debe ejecutar. En una memoria se guardan los programas y la CPU se encarga de procesar paso por paso las instrucciones del programa.

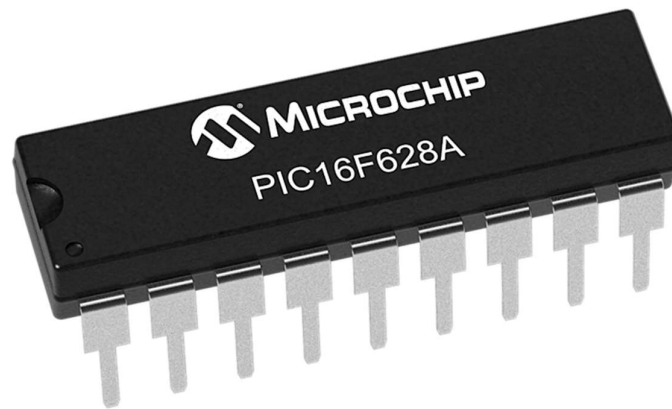
Los lenguajes de programación típicos que se usan para este fin son ensamblador y C, pero antes de grabar un programa al microcontrolador hay que compilarlo a hexadecimal que es el formato de lectura con el que microcontrolador entiende lo programado.

Para realizar proyectos electrónicos con microcontroladores se necesita básicamente tres cosas:

1. Una computadora
2. *Software* de programación (incluyendo un compilador).
3. Un circuito programador

La computadora, a través del *software* de grabación, se encarga de enviar el programa que se desea grabar al microcontrolador por intermedio del circuito programador que trae cada fabricante.

*Microchip Technology*, denominada comúnmente *Microchip*, es una de las empresas líderes en la fabricación de microcontroladores como el que se observa en la Figura 1.13. Para esta empresa, los microcontroladores se conocen con el nombre de PIC por sus siglas en inglés, *Programmable Interrupt Controller*. Debido a su bajo costo, desempeño eficiente, gran documentación y fácil adquisición de desarrollo, los microcontroladores de *Microchip*, son muy comunes de encontrar en tiendas electrónicas.



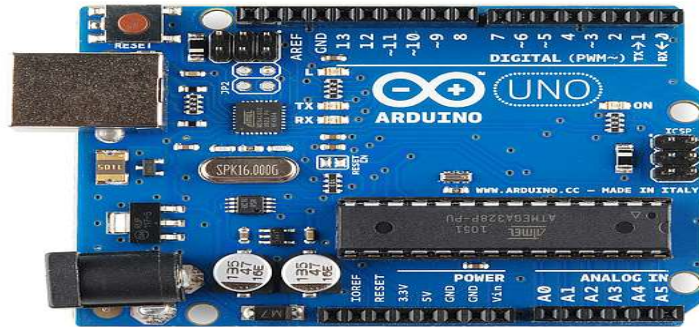
**Figura. 1.13. Microcontrolador PIC16F628A.**  
**Fuente: (Microchip, 2019).**

Atmel, otra empresa líder en este campo es famosa por crear los microcontroladores sobre los que se basan los Arduinos. Los microcontroladores AVR son una familia de microcontroladores RISC del fabricante estadounidense Atmel.

Los Arduinos usan principalmente microcontroladores de la gama AVR de Atmel, pero también de otras gamas de Atmel y de Intel.

Es importante saber que Arduino no es el único microcontrolador ni la única plataforma. Lo mismo que se hace con Arduino se puede hacer con otros microcontroladores

y otras plataformas de desarrollo, pero Arduino es la más extendida, con más documentación y soporte. En la Figura 1.14, se observa el Arduino Uno.



**Figura. 1.14. Módulo Arduino.**  
Fuente: (eSparkfun, 2019).

### 1.2.2 Microcontroladores AVR de ATMEL

Son una familia muy amplia de Microcontroladores de la compañía ATMEL, que se dedica a la fabricación de semiconductores, se caracteriza por su gran desempeño y rapidez en tiempo de ejecución.

El concepto y arquitectura fue pensando por dos estudiantes de arquitectura de *microchip* los cuales vieron la necesidad de crear una familia que compitiera con la desarrollada familia PIC la cual para la década de los 90 eran el gran gigante de los Microcontroladores. Esta familia fue desarrollada en una subdivisión de compañía de Atmel, la cual más tarde mejoró el diseño patento por dichos estudiantes. Esta familia no solo abarca Microcontroladores de 8 bits, sino que también abarca de hasta 32 bits.

### 1.2.3 Microcontrolador AVR 328P

El Atmega328 es un chip microcontrolador creado por la empresa ATMEL, es comúnmente usado en múltiples proyectos y sistemas autónomos donde es requerido por su bajo costo, así mismo está diseñado para el uso en la automatización industrial y sirve como microcontrolador principal del funcionamiento de equipos domésticos.

Este microcontrolador tiene una implementación muy común en todo el mundo y es que se lo utiliza para el funcionamiento de la plataforma Arduino en los modelos nano y uno.

#### 1.2.4 Características AVR 328P

Es un circuito integrado de alto rendimiento basado en un microcontrolador RISC (*Reduce Instruction Set Computer*), es decir, es un conjunto de instrucciones simples y pequeñas que toman menor tiempo en ejecutarse, posee una memoria flash de 32 Kbytes para lectura y escritura al mismo tiempo.

Es capaz de ejecutar instrucciones de gran tamaño en un solo ciclo de reloj, permitiendo que el microcontrolador logre rendimientos que se aproximan a 1 MIPS (*millón of instruction per second*) mientras a la vez es capaz de equilibrar el consumo y la velocidad de procesamiento.

Contiene un núcleo AVR cuya frecuencia de trabajo máxima es de 20MHz y que también posee una memoria RAM de 2Kb, así mismo, su voltaje de funcionamiento está entre los 1.8 a 5.5 Vdc, posee un máximo de 23 entradas-salidas las cuales funcionarán dependiendo de nuestro requerimiento.

El microcontrolador posee muchas características que dependiendo del uso es el que se escogerá para un fin determinado, en este caso de acuerdo a las funcionalidades que el sistema de seguridad poseerá es el indicado para usarlo en este proyecto, en la Tabla 1.1, se muestran los parámetros de funcionamiento del Atmega328P.



Tabla. 1.1. Parámetros básicos de funcionamiento ATmega328P.

Microcontrolador	ATmega328
Voltaje de funcionamiento	5V
Alimentación	7-12V
Voltaje máximo de entrada	20V
Pines digitales I/O	14 (6 con salida PWM)
Pines de entrada analógica	6
Corriente DC por I/O Pin	40 mA
Corriente DC para el pin 3.3V	50 mA
Memoria Flash	32 KB
SRAM	2 KB
EEPROM	1 KB
Velocidad de reloj	16 MHz

Fuente: (Pérez R., 2016)

También en la Figura 1.15, muestra la distribución de los pines que posee el microcontrolador AVR 328, con la que se elige que pines se utilizan.

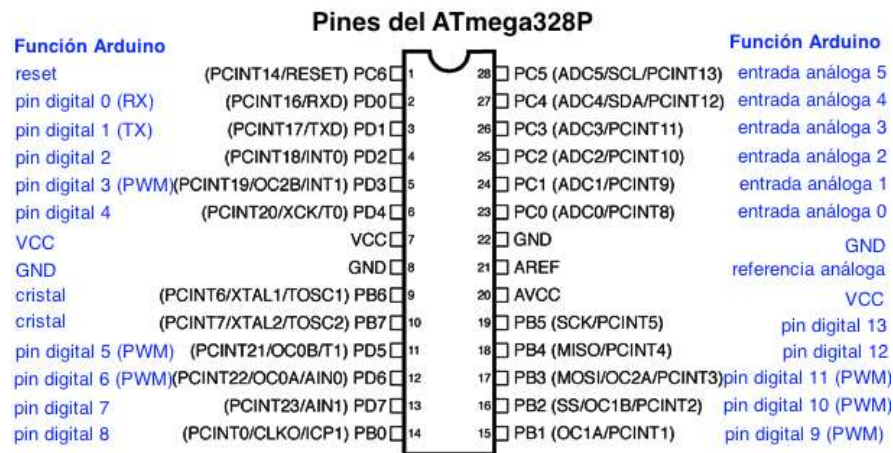


Figura. 1.15. Distribución de pines ATmega328.

Fuente: (Manosaloscables, 2016).

### 1.2.5 Programación mediante Arduino

La programación de un Arduino no es más que programar un microcontrolador por lo que programar Arduino consiste en traducir a líneas de código las tareas automatizadas que se desea hacer, leyendo de los sensores, datos obtenidos del medio y en función de las condiciones del entorno programar la interacción con el mundo exterior mediante unos actuadores.

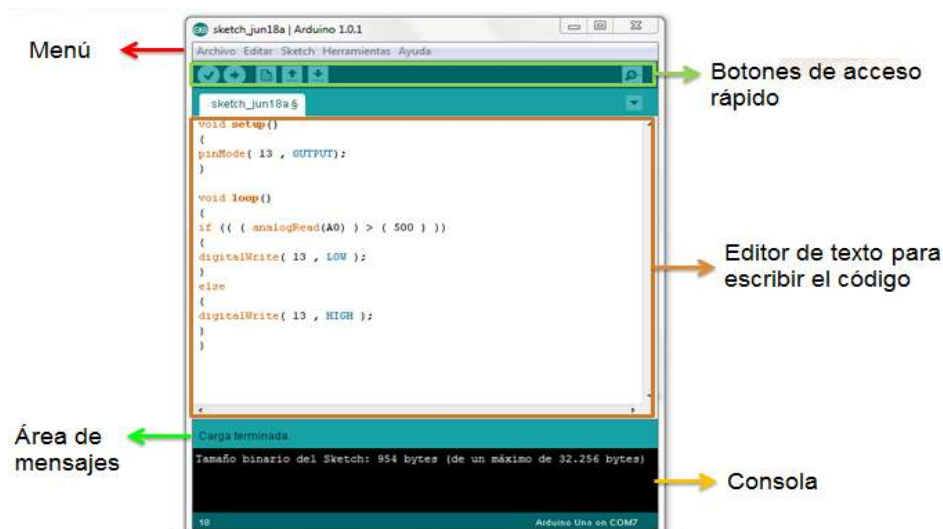
Arduino proporciona un entorno de programación sencillo y potente para programar, pero además incluye las herramientas necesarias para compilar el programa y “quemar” el programa ya compilado en la memoria flash del microcontrolador. Además, el IDE (Entorno de desarrollo integrado), ofrece un sistema de gestión de librerías y placas muy práctico, siendo muy sencillo pero suficiente para realizar programaciones.

El programa se implementará haciendo uso del entorno de programación propio de Arduino y se transferirá empleando un cable USB. Si bien en el caso de la placa USB no es preciso utilizar una fuente de alimentación externa, ya que el propio cable USB la proporciona, para la realización de algunos de los experimentos prácticos sí será necesario disponer de una fuente de alimentación externa ya que la alimentación proporcionada por el USB puede no ser suficiente.

### 1.2.6 Entorno de desarrollo

Para programar la placa es necesario descargarse de la página web de Arduino el entorno de desarrollo (IDE). Se dispone de versiones para Windows, Linux y para IOS, así como las librerías que se vayan a necesitar para el proceso de programación

En la Figura 1.16, se aprecia las partes que conforman el entorno IDE.



**Figura. 1.16. Entorno IDE.**  
Fuente: (Club de Arduino, 2019).

- Menú: Aquí puede encontrar todas las funciones que el IDE permite ejecutar, es decir aquí se encuentran todas las funcionalidades de la interfaz para ser utilizadas en el momento de programar
- Botones de acceso rápido: En esta barra están las funciones más utilizadas para poder tener un acceso rápido a las mismas.
- Editor de texto: En este apartado es donde la programación toma un orden y donde se escriben las líneas de comando a ser ejecutadas posteriormente.
- Área de mensajes: Aquí puede observar mensajes de la interfaz como si la descarga de la programación fue realizada, el estado de la compilación, entre otras.
- Consola: La consola brinda un resumen del espacio de almacenamiento del programa, que espacio utilizaron las variables globales y la disponibilidad de espacio que aún falta por programar para llenar la memoria del microcontrolador.

### 1.3 Tecnología de comunicación inalámbrica Bluetooth

#### 1.3.1 Introducción

*Bluetooth* es una tecnología inalámbrica de corto alcance que permite la comunicación inalámbrica de datos entre dispositivos digitales, como un computador o una cámara digital. La tecnología inalámbrica *bluetooth* funciona en un rango de aproximadamente de 10 metros.

Lo habitual es establecer una conexión entre 2 dispositivos, pero algunos dispositivos pueden conectarse simultáneamente a varios dispositivos.

No es necesario orientar los dispositivos frente a frente como ocurre con la tecnología de infrarrojos. Por ejemplo, puede utilizar los dispositivos dentro de una bolsa o bolsillo. El estándar bluetooth es un estándar internacional admitido y empleado por miles de empresas en todo el mundo.

El término *Bluetooth* (“Diente azul” en inglés, aunque el nombre proviene del rey danés y noruego *Harald Blatand*, traducido como *Harold Bluetooth*) es la denominación

comercial y popular del estándar de comunicación inalámbrica IEEE 802.15.1. La primera empresa en investigar esta tecnología fue Ericsson, encargada de liderar un grupo que, con el tiempo, sumó a IBM, Nokia, Microsoft, Motorola y otras compañías que apoyaron el estándar.

Las computadoras, los teléfonos móviles y las cámaras digitales son algunos de los dispositivos que pueden comunicarse mediante la tecnología *Bluetooth* (siempre que sus modelos se lo permitan).

### 1.3.2 Definición

*Bluetooth* es una especificación tecnológica para redes inalámbricas que permite la transmisión de voz y datos entre distintos dispositivos mediante una frecuencia en el rango de 2,4 GHz. Esta tecnología, por lo tanto, permite las comunicaciones sin cables ni conectores y la posibilidad de crear redes inalámbricas domésticas para sincronizar y compartir la información que se encuentra almacenada en diversos equipos.

### 1.3.3 Características

El *Bluetooth* posee un hardware que se compone de un dispositivo de radio que modula y transmite la señal, mientras que un controlador digital se encarga de procesar las señales digitales entre los distintos dispositivos. Dependiendo de si es maestro o esclavo, el controlador digital se encarga del envío y recepción de datos, determina las conexiones, el tipo de enlace, ubica el dispositivo y se encarga de las peticiones dadas por el usuario.

Existen tres clases de *Bluetooth*: Clase 1 (con un alcance aproximado de 100 metros), Clase 2 (10 metros) y Clase 3 (1 metro). Los especialistas consideran que, en los próximos años, todos los equipos tecnológicos tendrán la capacidad de comunicarse entre sí gracias al estándar.

Los principales objetivos que este estándar pretende son:

- Facilitar las comunicaciones entre equipos móviles.

- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas.

### 1.3.4 Módulo Bluetooth HC-06

El futuro es inalámbrico y la tecnología *Bluetooth* es una de las más utilizadas en el mundo de la electrónica, donde el enlace de datos es decir su vínculo físico debe ser robusto, confiable y seguro; el módulo *Bluetooth HC-06* es un dispositivo muy fácil de obtener, económico y sencillo de utilizar.

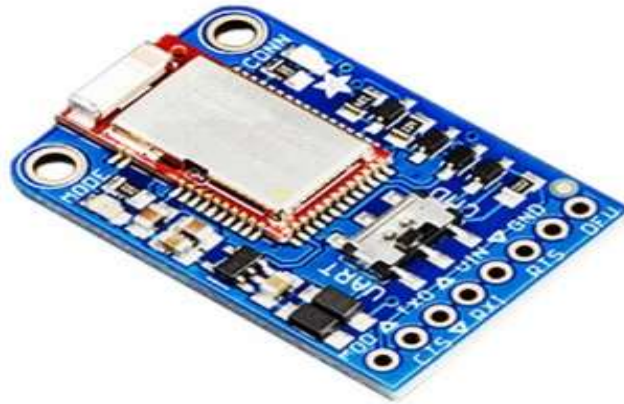
Con dimensiones tan pequeñas como un conector USB, el módulo *Bluetooth HC-06* es una de las piezas de mercado más utilizadas en este tipo de conectividad. La mayoría de los programadores que requieren trabajar con una conexión inalámbrica *bluetooth*, encuentran en este pequeño dispositivo todo lo necesario para resolver sus conexiones inalámbricas y a un costo que no alcanza a la quinta parte de lo que hay que pagar por otros dispositivos de las mismas características.

Existen varios módulos *bluetooth* que tienen características similares y técnicamente realizan las mismas funciones, se configuran de la misma manera, pero difieren en dos puntos muy importantes a diferencia del HC-06.

La primera es el tema del costo, como ya se había mencionado anteriormente, al ser muy popular el módulo HC-06 posee la ventaja de ser un dispositivo muy vendido y por ende con un costo bajo de venta, lo que hace atractivo para realizar cualquier tipo de proyecto.

La segunda ventaja del módulo HC-06, es que se lo encuentra fácilmente en el mercado local, a diferencia de otros dispositivos que al no ser conocidos no tienen buena notoriedad en el mercado local.

Como se puede apreciar en la Figura 1.17 y Figura 1.18, los diferentes tipos de dispositivos electrónicos del tipo *bluetooth*.



**Figura. 1.17. Adafruit Bluefruit.**

Fuente: (Amazon, 2019.)



**Figura. 1.18. SparkFun ESP32.**

Fuente: (BricoGeeks, 2019.)

En la Tabla 1.2, se puede apreciar las características de los diferentes módulos *bluetooth* que se presentaron en las figuras anteriores, si bien es cierto no existe mucha diferencia marcada entre uno y otro, la diferencia principal radica en el costo y existencia en el mercado local, por lo que el módulo HC-06 es la mejor opción que podemos tener.

Tabla. 1.2. Tabla comparativa dispositivos bluetooth.

CARACTERÍSTICA	HC-06	ADAFRUIT BLUFRUIT	SPARKFUN ESP32
PROCESADOR	BC417143	ARM Cortex M0 a 16Mhz	Dual Core Tensilica LX6
SRAM	32 Kb	32 Kb	520Kb
FLASH	8Mb	256 Kb	4Mb
ALIMENTACIÓN	3.3 a 6v	5v	2.2 a 3.6v
COSTO	\$ 5	\$ 29,95	\$ 27,95
MERCADO LOCAL	SI	NO	NO

Fuente: Elaborado por el autor

Actualmente, en el mercado local existen dos módulos que proporcionan la funcionalidad de trabajar con un módulo *bluetooth*, estos son el HC-05 y el HC-06, ambas son compatibles para la tarjeta electrónica programable de Arduino.

La diferencia entre ambas radica en un solo punto, a simple vista ambas son prácticamente idénticas, como se aprecia en la Figura 1.19, pero el módulo HC-06 trabaja únicamente en modo *slave* o esclavo, es decir, solo recibe conexiones de otros dispositivos como PC, *tablets*, *smarthphones*, etc.

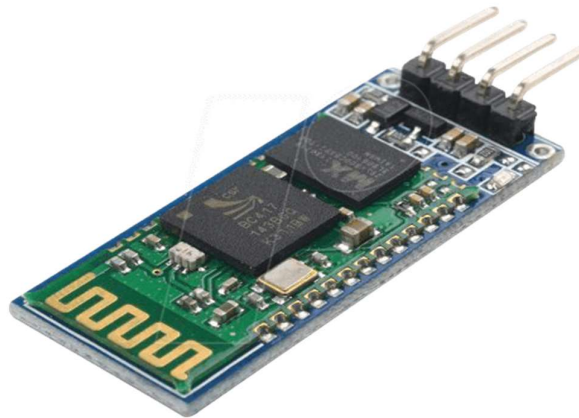


Figura. 1.19. Módulo HC-06.  
Fuente: (Nylamp Mechatronics, 2019).

A diferencia del módulo HC-06, el HC-05 tiene una ligera mejora y es que puede trabajar como, *master/slave* o maestro/esclavo, lo cual significa que el dispositivo puede aparte de sólo recibir conexiones de otros dispositivos también las puede realizar, es decir,

que está en la capacidad de buscar dispositivos *bluetooth* que estén dentro del rango de cobertura y engancharse con ellos.

Justamente al estar en la capacidad de trabajar como maestro incorpora un botón, el cual tiene la función de explorar el entorno en búsqueda de otros dispositivos a los que se podría realizar una conexión, esto se puede apreciar en la Figura 1.20.



**Figura. 1.20. Módulo HC-05.**  
**Fuente: (Nylam Mechatronics, 2019).**

Debido a que no se requiere tener una capacidad de enlazar dos dispositivos desde el módulo *bluetooth* hacia otro dispositivo, se realiza la elección de diseñar el dispositivo de seguridad con el HC-06, el cual es el ideal para el trabajo que se desee realizar.

## **1.4 Tecnología de comunicación GSM**

### **1.4.1 Introducción**

La red GSM es, a comienzos del siglo XXI, el estándar más usado de Europa. Se denomina estándar "de segunda generación" (2G) porque, a diferencia de la primera generación de teléfonos portátiles, las comunicaciones se producen de un modo completamente digital.



En 1982, cuando fue estandarizado por primera vez, fue denominado "*Groupe Spécial Mobile*" y en 1991 se convirtió en un estándar internacional llamado "Sistema Global de Comunicaciones Móviles".

En Europa, el estándar GSM usa las bandas de frecuencia de 900MHz y 1800 MHz. Sin embargo, en los Estados Unidos se usa la banda de frecuencia de 1900 MHz. Por esa razón, los teléfonos portátiles que funcionan tanto en Europa como en los Estados Unidos se llaman tribanda y aquellos que funcionan sólo en Europa se denominan bibanda.

El estándar GSM permite un rendimiento máximo de 9,6 kbps, que permite transmisiones de voz y de datos digitales de volumen bajo, por ejemplo, mensajes de texto (SMS, Servicio de mensajes cortos) o mensajes multimedia (MMS, Servicio de mensajes multimedia).

Por lo demás, decir sobre el GSM que realmente supuso un salto definitivo en las plataformas móviles en el mundo. Las personas ya no sólo podían estar comunicadas desde cualquier lugar, sino que no necesitaban un terminal fijo para acceder a cualquier información existente en la red. Las aplicaciones prácticas de todo esto han sido enormes y aún continuarán sorprendiéndonos durante unas cuantas décadas, aunque el nombre de GSM vaya cayendo cada vez más en desuso.

Sin embargo, estos nuevos sistemas no han desbancado del todo las antiguas redes GSM, sino que conviven con ellas. La mayor parte de los operadores y móviles permiten el uso dual de estas redes, de modo que, si no hay cobertura en un lugar de 3G, pueden usar la red 2G (GSM) sin ningún problema. Esto se debe a que las infraestructuras 3G y 4G se han realizado sobre las ya existentes 2G, siguiendo en funcionamiento estas últimas. En general se puede decir que un móvil 4G puede funcionar con 3G y con 2G también, siendo compatible con las redes más antiguas.

La Figura 1.21, muestra el módulo SIM800, que se encuentra localmente en cualquier electrónica.

Si indagamos en el mercado local del mundo de la electrónica se observa que existen dos módulos GSM/GPRS de el mismo fabricante que siempre están presentes en las diferentes tiendas que comercializan este tipo de dispositivos y son el SIM800 y SIM900, la diferencia más significativa que se puede encontrar es que la SIM900 trae un procesador de un solo chip que el SIM800, pero en tamaño y prestaciones son iguales.

Ideal para sistemas remotos, comunicación recursiva, puntos de control, mandar mensajes de texto a celulares, etc. El módulo GSM-GPRS-SMS-SIM900 se utiliza en el proyecto para enviar los mensajes cortos, SMS. (Iza, 2018)

En la Tabla 1.3, se observa la comparación de costos entre la SIM800 y SIM900, de acuerdo con el mercado local.



**Figura. 1.21. Módulo SIM800.**  
Fuente: (Ebay, 2019).

En los costos de cada uno hay una diferencia de casi el doble, obviamente por la diferencia que el fabricante incorporo en la una y la otra, no obstante, este dispositivo es muy accesible económicamente. Por eso se va a utilizar la SIM800 para el proyecto.

**Tabla. 1.3. Comparación económica Sim800 – Sim900.**

SIM800	SIM900
\$ 19	\$ 33
Muy comercial	Poco comercial

Fuente: Elaborado por el Autor.

### 1.4.2 Módulo GSM/GPRS SIM800

Existen varias formas de conectar Arduino con el exterior, como *Ethernet*, *wifi*, *bluetooth*, pero ninguna de estas se encuentra tan disponible y con mucha cobertura como la celular.

Para este tipo de propósitos se puede utilizar un módulo GSM/GPRS con una tarjeta SIM, de forma que se pueda comunicar con él, como si se tratase de un teléfono móvil. Esta tarjeta basada en el módulo SIM800 permite enviar y recibir llamadas, SMS y conectarnos a Internet, transformando a un microcontrolador en un teléfono móvil.

EL GSM (*Global System for Global Communications*) es el sistema de comunicaciones que más se utiliza en teléfonos móviles y es un estándar en Europa. La primera funcionalidad de esta tecnología es la transmisión de voz, pero también permite la transmisión de datos (SMS, Internet), eso sí, a una velocidad muy baja de 9kb/s.

El GPRS (*General Packet Radio Service*) es una extensión del GSM basada en la transmisión por paquetes que ofrece un servicio más eficiente para las comunicaciones de datos, especialmente en el caso del acceso a Internet. La velocidad máxima (en teoría) del GPRS es de 171kb/s, aunque en la práctica es bastante más pequeña.

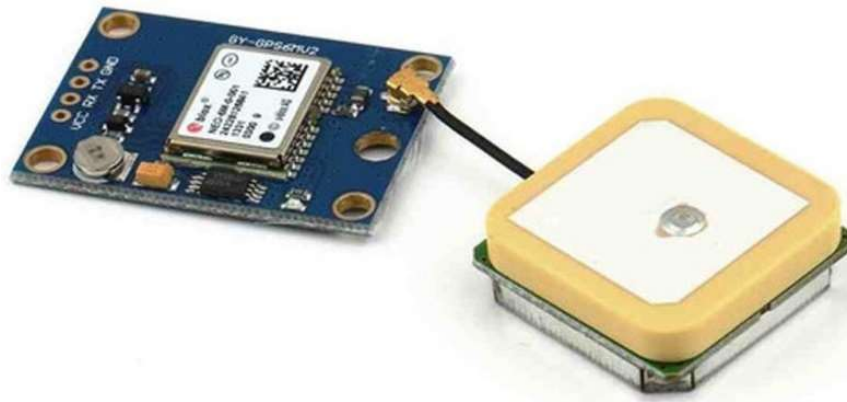
Una de las características del módulo SIM800, es ser cuatri banda, por lo que permite trabajar en las bandas de 850/900/1800/1900Mhz. Ecuador trabaja en las bandas de 850/1900Mhz en GSM, por lo que el módulo GSM/GPRS es compatible con la frecuencia de operación de las operadoras que prestan el servicio de telefonía.

### 1.5 Módulo GPS UBLOX 6

El sistema de Posicionamiento Global o GPS es un sistema de navegación que se basa en brindar la ubicación mediante coordenadas geográficas a través de distintos satélites, este sistema está disponible en cualquier parte del mundo, las 24 horas del día y sin la necesidad de pagar por el servicio.

El Ublox 6 es un receptor GPS compatible con los diferentes tipos microcontroladores existentes, viene listo para su funcionamiento con tan solo proveerlo de voltaje, su programación es muy sencilla con una lista corta de comandos para las instrucciones de lo que debe hacer con los datos que recolecta.

Este módulo es ideal para el presente proyecto ya que va a permitir al usuario saber la posición geográfica del vehículo en todo momento y más aún si el auto fuera hurtado y trasladado a otro sitio, el módulo es el que se muestra en la Figura 1.22.



**Figura. 1.22. Módulo GPS UBLOX 6**  
Fuente: (Potentiallabs, 2019).

## **1.6 Detector de ruptura de vidrio**

### **1.6.1 Introducción**

En los diferentes ámbitos en temas de seguridad existen los detectores de ruptura de vidrio, estos dispositivos sirven para alertar de una posible intrusión a una determinada área protegida.

### **1.6.2 Características**

Existen varias maneras en las que basan su funcionamiento y va a depender de la mecánica interna que cada uno de ellos posea.

### 1.6.3 Sensor de vibración mecánica

El sensor de vibración SW-18015P, es el más común de los módulos en las tiendas de electrónica, trabaja con microcontroladores y diferentes placas electrónicas como el Arduino.

El sensor de vibración mecánica por muelle tiene una sensibilidad alta, el sensor esta encapsulado en un pequeño circuito y actúa a modo de interruptor, como se aprecia en la Figura 1.23, cuando los contactos internos se tocan debido a una vibración emite una señal digital (INFOOTEC, 2018).

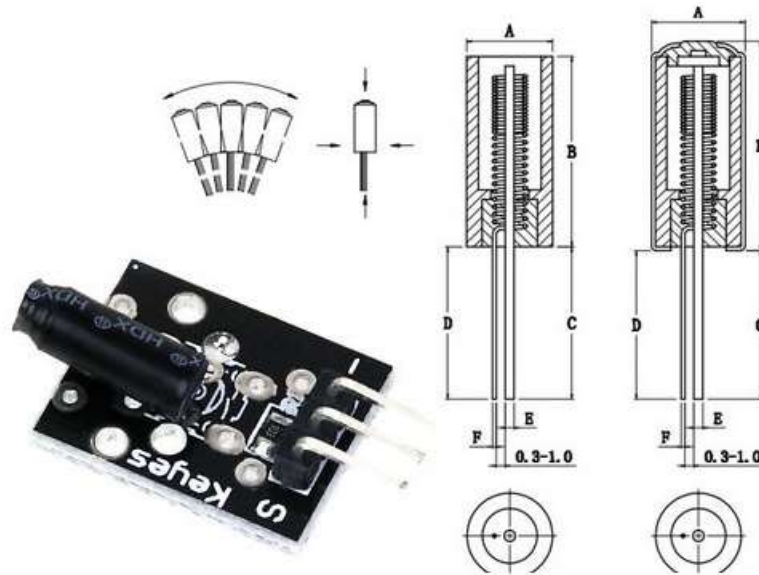


Figura. 1.23. Sensor de vibración mecánico SW-18015P.  
Fuente: (Infootec, 2019).

### 1.6.4 Sensor de vibración piezoeléctrico

Un sensor de vibración piezoeléctrico es aquel que se basa en el fenómeno de la piezoelectricidad.

Este fenómeno que ocurre en determinados cristales que, al ser sometidos a tensiones mecánicas, en su masa adquiere una polarización eléctrica y aparece una diferencia de potencial y cargas eléctricas en su superficie (Electronics, 2019).



**Figura. 1.24. Sensor de vibración Glass BREAK 5150**  
**Fuente: (Amazon, 2019).**

Para el diseño del sistema de seguridad se ha tomado en cuenta dos factores importantes por los cuales se va a trabajar con el *glass break 5150*, que se muestra en la Figura 1.24 y es que no va a ser necesario alimentar los sensores llevando cables de alimentación a cada ventana del auto y que este sensor es de fácil aplicación, tan solo con un adhesivo que viene incluido se adhiere al vidrio.

A diferencia del SW-18015P que necesita alimentar cada sensor y que se debería fabricar un encapsulado para proteger la electrónica del módulo que viene descubierta.

## **1.7 Aplicaciones para teléfonos inteligentes**

### **1.7.1 Introducción**

Hace tiempo que los móviles inteligentes llegaron para quedarse, en la actualidad cualquier persona pasa más tiempo con el teléfono que con cualquier ordenador o portátil. Basta con pensar que siempre el teléfono lo tenemos a mano, e incluso con él, en la mesita de noche. Es decir, nuestro móvil nos acompaña 24 horas, 7 días a la semana.



**Figura. 1.25. Aplicaciones para smartphone.**  
**Fuente: (Cuello J., 2017).**

En la Figura 1.25, se aprecia muchas de las aplicaciones que un *smartphone* puede contener, los programadores son muy diversos y a diario crean nuevas aplicaciones.

Un dato de la consultora *Flurry Analytics*, con oficinas en EE.UU., Reino Unido e India, ayuda a entender la relevancia de las 'apps': el 86% del tiempo que un usuario dedica a su *smartphone*, es para las aplicaciones; el 14% restante se va en usar un navegador de Internet (Maldonado, 2018).

Dada esta aplastante realidad, los móviles son una pieza fundamental en la vida diaria, y por tanto la creación de APPs se convierte en una forma para simplificar ciertas actividades o actividades a realizar.

### 1.7.2 Definición

“App” es el acrónimo de la palabra en inglés *application*, la cual se puede traducir como aplicación, en el contexto de la informática. Una definición sobre *App* sería programa informático ligero siendo este descargable por su pequeño tamaño, permite unas funciones determinadas, normalmente diseñado para equipos móviles como celulares y tabletas.

La difusión y uso del término *App* se debe principalmente al teléfono precursor de esta experiencia, el *Iphone* en el 2008 haciendo referencia al 3G y no a la primera versión del 2007, y al nombre que Apple le dio a su sitio de descargas para móviles llamada *App Store*.

### 1.7.3 Características

La aplicación trabajará de manera local, es decir la *APP* se conecta al módulo *bluetooth*, tomando en cuenta que la primera vez que se registren, se tendrá que registrar una combinación de 4 números que es la contraseña de emparejamiento y con la cual se establecerá la comunicación entre la *APP* de teléfono inteligente y el módulo *bluetooth*.

Las funciones que la *APP* tendrá serán las siguientes:

- Al momento de emparejarse, automáticamente se cerrará el circuito de voltaje de la bomba de gasolina o de la ignición, mediante un relé con lo cual el combustible fluirá hacia el motor o a su vez la ignición permitirá el arranque del vehículo, lo cual permitirá arrancar y empezar la conducción. Caso contrario cuando la *APP* se desconecte del módulo *bluetooth* el relé se abrirá para impedir el bombeo de gasolina al motor. Por seguridad una vez que se haya desconectado el módulo *bluetooth* de la *APP*, se considera que la apertura del relé se hará 1 minuto después del hecho.
- Mediante un botón de la interfaz de la *APP* se cerrará el seguro de la puerta del conductor.
- Mediante un botón de la interfaz de la *APP* se abrirá el seguro de la puerta del conductor.
- Mediante un botón de la interfaz de la *APP* se bajará el vidrio del conductor siempre y cuando el vehículo disponga de vidrios eléctricos.

La aplicación servirá como llave inteligente que gestionará el encendido o el bloqueo del vehículo, adicional de tener las funciones de apertura/cierre del seguro de la puerta o ventana.

### 1.7.4 Sistema Operativo Android

Android es el nombre de un sistema operativo que se emplea en dispositivos móviles, por lo general con pantalla táctil. De este modo, es posible encontrar tabletas (*tablets*), teléfonos móviles (celulares) y relojes equipados con Android, aunque el *software* también se usa en automóviles, televisores y otras máquinas (Pérez, 2017).



Una de las claves de la popularidad de Android es que, como Linux, es una plataforma de código abierto, permite a fabricantes, operadores y desarrolladores dar mayor funcionalidad, así como también la capacidad de crear aplicaciones de acuerdo con lo que se requiere para ser instalada de manera fácil en teléfonos inteligentes. Las diferencias se pueden observar en la Tabla 1.4.

**Tabla. 1.4. Diferencia entre Android e iOS.**

<b>FAMILIA DE OS</b>	<b>LINUX</b>	<b>OS X, UNIX</b>
<b>PERSONALIZACIÓN</b>	Mucha, se puede cambiar casi todo.	Poca, excepto cuando se desbloquea.
<b>LANZAMIENTO INICIAL</b>	23 de septiembre de 2008	29 de julio de 2007
<b>PROGRAMADO EN</b>	C, C++, Java.	C, C++, Objective-C
<b>DEPENDIENTE DE UNA PC O MAC</b>	No	No
<b>TRANSFERENCIA FACIL DE MEDIOS</b>	Depende del modelo del aparato celular.	Con Aplicaciones de Mac.
<b>TIPO DE MODELO</b>	Abierto ( <i>Open Source</i> )	Cerrado (propiedad de Apple)
<b>CÓDIGO ABIERTO</b>	Núcleo (Kernel), Interfaz y algunas aplicaciones básicas	El núcleo (kernel) de iOS no es código abierto, pero está basado en código abierto Darwin OS

**Fuente: (Diffen, 2019).**

## **CAPÍTULO 2**

### **MARCO METODOLÓGICO**

En este capítulo se menciona la metodología que se utilizó para el control electrónico del encendido/bloqueo y seguridad de un vehículo mediante las actividades y recursos utilizados en el desarrollo de la misma, así también se describe los tipos de estudio realizados para cumplir con los objetivos planteados.

#### **2.1 Modelos de investigación**

Existen varios modelos de investigación, estas son las herramientas que el investigador necesitará para cumplir con los objetivos trazados de una manera sencilla y de acuerdo con las necesidades que la investigación requiera.

Con la aplicación de los modelos de investigación se obtendrá una conclusión de todo el proceso de investigación que se habrá realizado, siendo este veraz y confiable para los resultados obtenidos.

La fundamentación teórica es de gran aporte por los diferentes tipos de información que se pueda encontrar con temas afines al tratado, mediante técnicas como revisión bibliográfica y revisión de artículos en internet para poder tener bases teóricas de la investigación.

Mediante la investigación aplicada se busca utilizar los conocimientos adquiridos a lo largo de la carrera, esta metodología se encuentra directamente relacionada con la investigación básica, es decir, los conocimientos previos, bases técnicas, bases teóricas, los cuales van a permitir tener una base sentada desde el planteamiento hasta la ejecución del proyecto.

De la realidad que se tiene en el planteamiento del problema, se la va a modificar para conseguir crear un objetivo nuevo y concreto, es decir, con la ayuda de la investigación experimental permitirá llegar al objetivo deseado para aprender de su funcionamiento y nuevas características que lo conforman.

Así también se caracterizó el objeto de estudio para brindar en las conclusiones, características y propiedades únicas del mismo con el afán de solucionar el problema planteado.

La validación de este vendrá de la mano con pruebas de campo, las cuales servirán para entender bondades y defectos del proyecto en cuestión, las cuales servirán para describir de mejor manera el uso del mismo y a su vez para la corrección de los defectos encontrados.

La implementación se considera una metodología de campo no experimental, ya que la recolección de datos fue extraída directamente de la realidad de donde se los ejecutó, éstos son conocidos como de primera mano. Este método es uno de los más utilizados por la facilidad que brinda al momento de comprender y solventar dudas por parte del investigador.

## **2.2 Técnica de recolección de datos**

Los métodos de recolección de datos en la Investigación cualitativa de mercados van desde entrevistas a profundidad a personas que pertenecen a un determinado segmento que se desee analizar, pasando por reuniones o sesiones grupales donde se analiza su opinión y comportamiento ante un tema relacionado al objeto de estudio, hasta las diferentes técnicas proyectivas y métodos de observación directa. El uso de una u otra técnica o de todas durante la investigación, dependerá del análisis previo que se realice al diseño de la investigación, durante la planificación. (Digital, 2019)

## **CAPITULO 3**

### **PROPUESTA**

En este capítulo se propone las diferentes funcionalidades que el dispositivo de control está en capacidad de realizar, teniendo en cuenta aspectos de funcionalidad y operatividad.

La implementación del control electrónico para encendido/bloqueo y seguridad de un vehículo consta de software y hardware que fueron diseñados a la medida que los objetivos fueron planteados.

El dispositivo tiene un microcontrolador Atmega AVR328P, el cual fue dimensionado para el diseño requerido, así mismo, este elemento electrónico es el que gestiona toda la programación que se elabora para que funcione de la manera requerida. Este microcontrolador tiene el suficiente número de entradas y salidas para conectar los diferentes módulos y sensores que protegerán al vehículo, así como la memoria necesaria para procesar la información insertada en el mismo.

A continuación, se detalla el listado de componentes utilizados en el proyecto.

Módulo *Bluetooth* HC-06, es el encargado de realizar la función de seguridad encendido/bloqueo en el vehículo, adicionalmente se encarga de la gestión local de las otras funciones de seguridad del vehículo como son, abrir/cerrar seguros y la apertura del vidrio del conductor.

Módulo NEO-6, o también llamado módulo GPS, éste va a brindar la ubicación del vehículo en tiempo real mediante la obtención de coordenadas geográficas, las cuales van a poder ser visualizadas por la aplicación de visualización de mapas que por defecto vienen en los celulares inteligentes.

Módulo SIM800, es el encargado de enviar la información que gestione el microcontrolador a la red celular, es un GPRS que puede albergar cualquier chip de las diferentes operadoras que existen en el mercado. Éste módulo es de gran importancia debido a que es el que alerta vía mensajes de texto a un número de celular definido eventos como, ruptura de vidrios, ubicación de coordenadas GPS, apertura de seguros en caso de no tener conexión local por bluetooth, notificación de luces encendidas, además de la recepción de comandos para apagar el vehículo en caso de pérdida o robo del vehículo con el celular adentro y la función de hacer que el vehículo suene su bocina para encontrarlo en caso de haberlo dejado en espacios grandes.

También dentro del diseño se encuentra contemplado un módulo llamado *Step Down* LM2596, el mismo que se añadió al diseño de circuito para tener una fuente de alimentación con capacidad de 3A, esto debido al consumo de corriente de cada uno de los elementos. De igual manera se incorporó un módulo de relés de 8 canales, el cual permite hacer el control de las funciones del dispositivo.

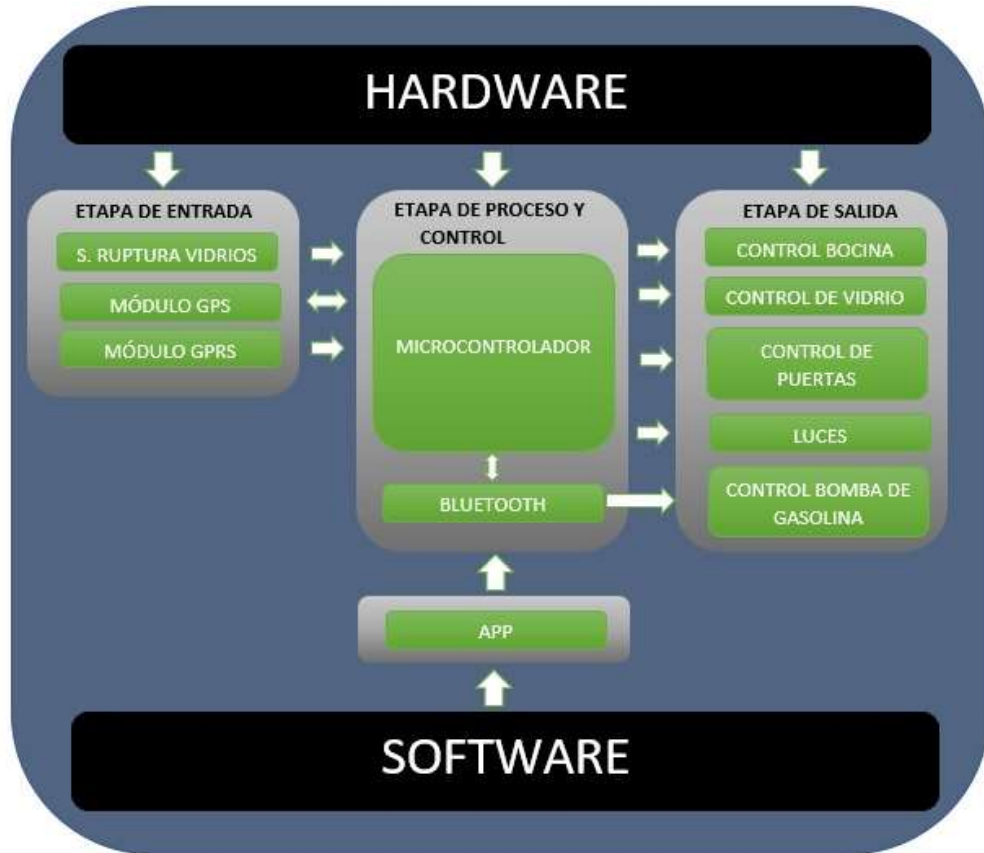
A continuación, se muestra en la Tabla 3.5, el consumo de corriente de cada dispositivo.

**Tabla. 3.5. Consumo de corriente de los dispositivos del módulo de seguridad.**

<b>Módulo</b>	<b>Consumo corriente mA</b>
SIM800	500
HC-06	40
GPS NEO-6	35
AVR328P	46

**Fuente: Elaborado por el Autor.**

A continuación, en la Figura 3.26, se muestra la estructura del diagrama de bloques básico del *software* y *hardware* con las etapas que conforman el dispositivo de seguridad del vehículo.



**Figura. 3.26. Diagrama de bloques del software y hardware del dispositivo de seguridad.**  
 Fuente: Elaborado por el Autor.

La etapa de entrada es la encargada de llevar información al microcontrolador de manera bidireccional como el GPS, el cual va a enviar información de posicionamiento al microcontrolador siempre y cuando el microcontrolador le solicite. Así también de manera unidireccional los dispositivos GSM/GPRS y los sensores de ruptura de vidrio alimentan con información al microcontrolador sin necesidad de que el microcontrolador lo solicite.

La etapa de proceso y control está regida por el microcontrolador Atmega 328P, el mismo que ejecutará las funciones programadas, así también el módulo *bluetooth* está

inmerso en este proceso ya que es quien se vincula directamente con el aplicativo para enviar y recibir la información del aplicativo y comunicarlo al microcontrolador.

En la etapa de salida, tenemos el control de varios de los dispositivos del vehículo como lo son el control de la bocina, de la ventana del conductor, el control de apertura y cierre de puertas, el control de la bomba de gasolina y la notificación de luces encendidas.

Dentro de lo que es el software se encuentra el diseño del *APP* que tendrá comunicación con el módulo bluetooth.

### **3.1 Diseño del hardware**

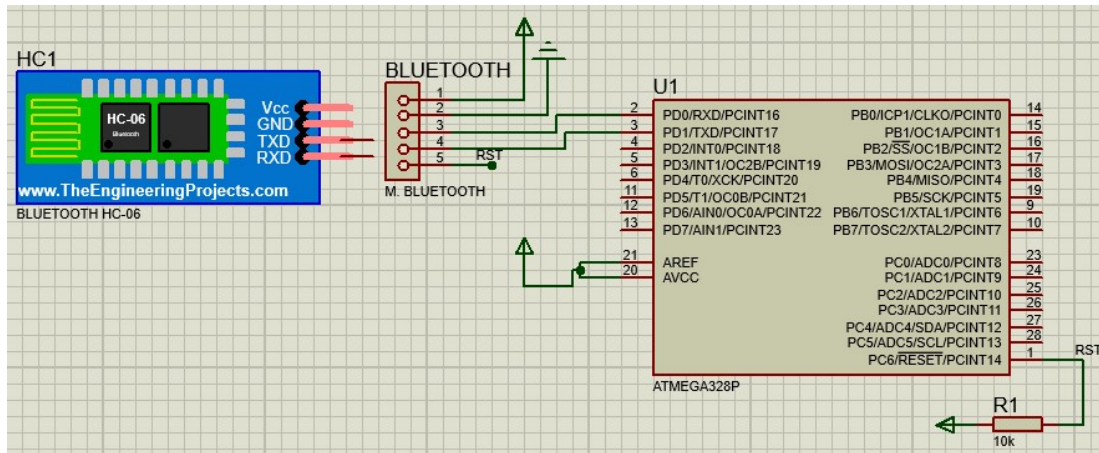
#### **3.1.1 Etapa de entrada**

El ingreso de la información en la etapa de entrada está encabezado por cuatro dispositivos, los cuales son el aplicativo en el *smartphone*, el *bluetooth*, el GPRS y el GPS.

El módulo *bluetooth* HC-06 es el encargado de recibir los comandos que el aplicativo envíe, una vez recibidos, los envía al microcontrolador y realizará la respectiva gestión que se le programó. Esta conexión va a ser local debido a que el módulo *bluetooth* tiene un alcance de 10 metros, por lo que hace la función de llave inteligente.

Mientras el aplicativo esté conectado el vehículo podrá arrancar y circular, pero en el caso de no estarlo se abrirá el relé asignado e impedirá el bombeo de la gasolina al motor a través de la bomba de combustible.

En la Figura 3.27, se aprecia el diagrama esquemático del microcontrolador con el módulo *bluetooth* HC-06.



**Figura. 3.27. Diseño etapa de entrada, módulo bluetooth.**  
**Fuente: Elaborado por el Autor.**

El módulo GPRS se encarga de realizar la comunicación mediante la red celular, es decir, se puede enviar comandos al dispositivo desde cualquier celular convencional o *smartphone*. Los comandos varían dependiendo de lo que se desee que realice el microcontrolador.

La comunicación entre el usuario y el SIM800 es mediante mensajes de texto o SMS, se utiliza este módulo ya que la red celular es de gran cobertura por lo que tenemos un amplio rango de acción remoto en caso de robo del vehículo.

En la Figura 3.28, se aprecia el diagrama esquemático del microcontrolador con el módulo SIM800.



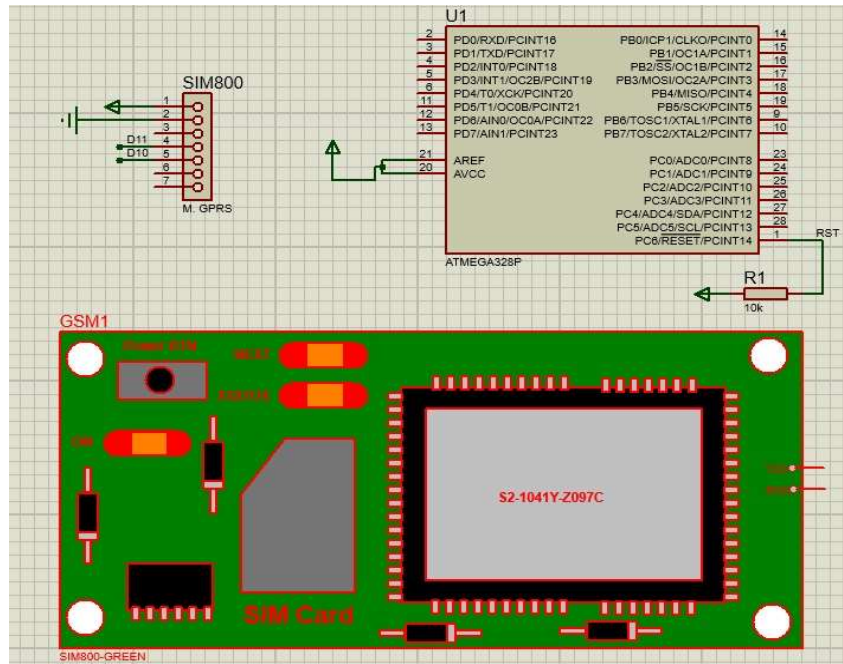


Figura. 3.28. Diseño etapa de entrada, módulo GPRS.  
Fuente: Elaborado por el Autor.

La ubicación del vehículo se lo realiza mediante un módulo GPS, el módulo NEO-6, brinda la utilidad de entregar las coordenadas en tiempo real al microcontrolador, con lo que el dispositivo de seguridad del vehículo tiene la capacidad de mostrar al usuario la ubicación geográfica del mismo.

En la Figura 3.29, se aprecia el diagrama esquemático del microcontrolador con el módulo GPS NOE6.

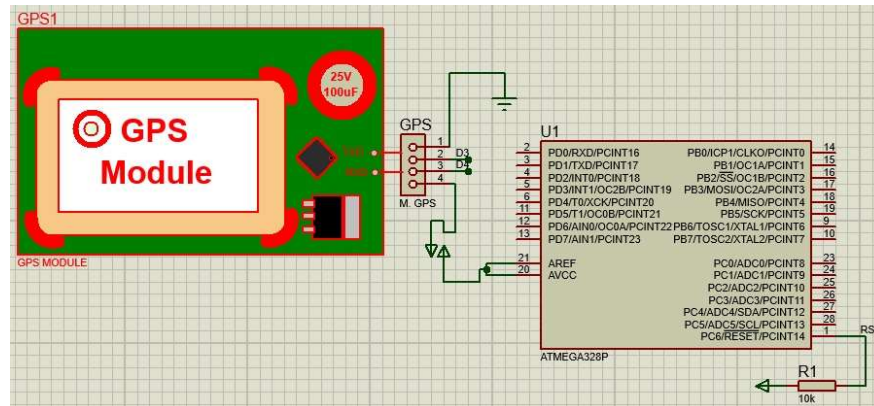


Figura. 3.29. Diseño etapa entrada, módulo GPS.  
Fuente: Elaborado por el Autor.

Los sensores de ruptura de vidrio indicarán al usuario cuando haya un posible robo del vehículo, estos enviarán la señal al microcontrolador, el cual la procesa y la envía al usuario por medio de mensaje de texto.

En la Figura 3.30, se observa el diagrama esquemático de conexión de los pines de los sensores de ruptura de vidrio con el microcontrolador.

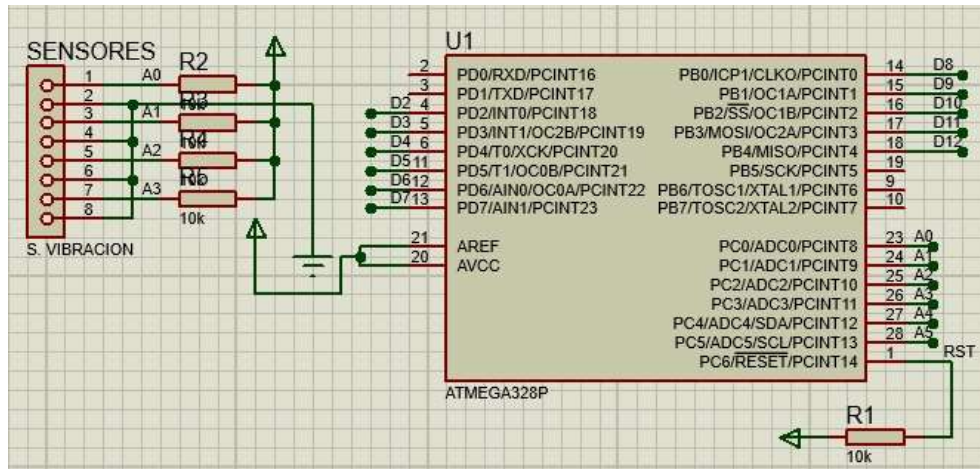


Figura. 3.30. Diagrama esquemático de conexión de sensores de ruptura con el microcontrolador.  
Fuente: Elaborado por el Autor.

### 3.1.2 Etapa de proceso y control

La etapa de proceso y control es la más fundamental, esta etapa es la encargada de recibir los datos de los módulos de la etapa de entrada para procesarla y posteriormente transferirlos a la etapa de salida.

Esta etapa central es manejada por el microcontrolador Atmega 328P el cual se observa en la Figura 3.31, el cual tiene el número suficiente de entradas y salidas necesarias para el manejo de todo el conjunto de etapas que se desea controlar.

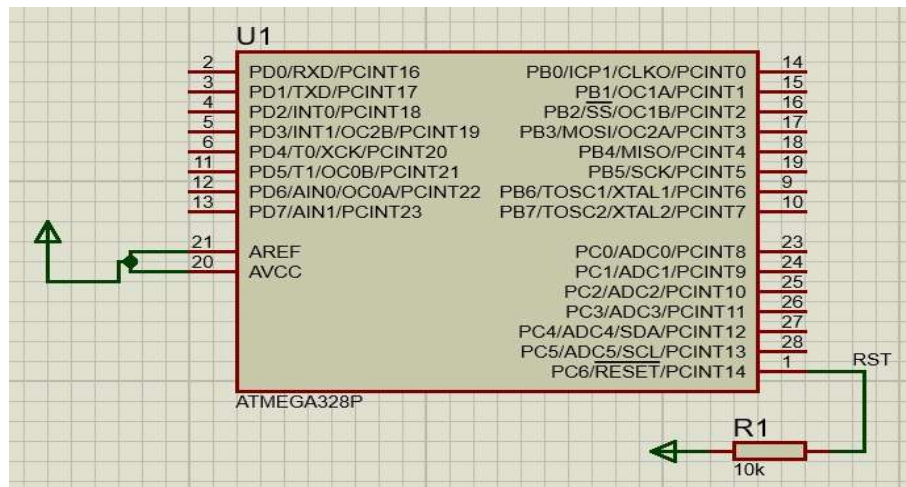


Figura. 3.31. Diseño de la etapa de control, microcontrolador Atmega 328P.  
Fuente: Elaborado por el Autor.

### 3.1.3 Etapa de salida

La etapa de salida es la que se puede verificar visualmente, cuando todo el dispositivo de control electrónico para el encendido/bloqueo y seguridad del vehículo esté instalado, se puede verificar que cada una de las etapas funcionan de acuerdo con diagrama de la Figura 3.26. La apertura local y remota de los seguros del vehículo, la activación de la bocina para buscarlo en caso de haber dejado el vehículo en espacios grandes, el símil de llave electrónica, la ubicación en tiempo real.

Las etapas de salida son:

- Control de Bocina: La bocina sonará por 5 segundos cuando el usuario envíe un mensaje de texto con la palabra PITO800.
- Control de Vidrio: El vidrio del conductor bajará por 3 segundos cuando el usuario envíe un mensaje de texto con la palabra VENTANA800.
- Control de puerta: La puerta del conductor se abrirá cuando el usuario envíe un mensaje de texto con la palabra ABRIR800
- Control bomba de gasolina: La bomba de gasolina dejará de bombear combustible cuando el usuario envíe la palabra ROBO800.
- Luces: El usuario será notificado de que dejó las luces encendidas al número preestablecido en el microcontrolador cuando el vehicule este apagado y se haya dejado las luces bajas encendidas.

### 3.1.4 APP

El aplicativo tiene las funciones de que cuando se haya conectado al módulo *bluetooth*, podrá dar paso al encendido del vehículo cerrando de manera automática el relé que va conectado a la bomba de gasolina y posteriormente acceder a las funciones de abrir y cerrar los seguros de las puertas, bajar la ventana del conductor.

### 3.2 Diseño del software

Para entender todas las funciones del programa a diseñar para el dispositivo de control electrónico para el encendido/bloqueo y seguridad del vehículo se utilizó el diagrama de flujo de la Figura 3.32.

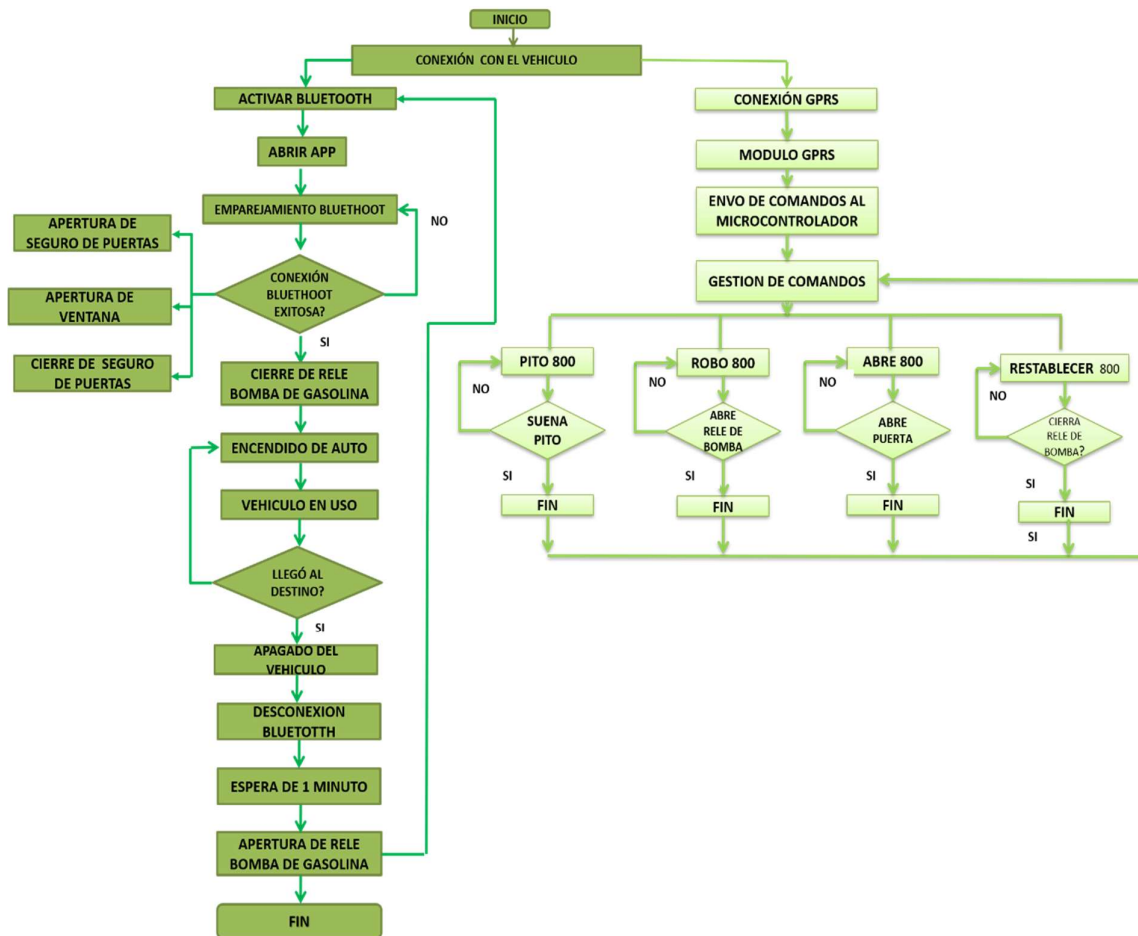


Figura. 3.32. Flujograma del funcionamiento del dispositivo de seguridad.  
Fuente: Elaborado por el Autor.

El flujograma comienza por la conexión del vehículo, para esto es necesario activar el *bluetooth* del *smartphone*, abrir el aplicativo y emparejarlo al *bluetooth* del dispositivo electrónico de control.

Si la vinculación no es exitosa se tiene que repetir los pasos antes mencionados, caso contrario, el relé de la bomba de gasolina se cierra y se puede encender el auto.

Cuando se establece la vinculación entre los dispositivos *bluetooth*, el aplicativo permite abrir y cerrar las puertas del vehículo y también la apertura de la ventana del conductor.

Cuando se haya llegado al destino y el usuario apague el vehículo y se aleje, se va a perder la conexión entre ambos dispositivos *bluetooth*, en ese momento el dispositivo electrónico de control espera un minuto para abrir nuevamente el relé de la bomba de gasolina y también para cerrar los seguros de las puertas. En el caso de que se quiera encender nuevamente el vehículo se debe realizar todo el proceso desde activar el *bluetooth*.

Cuando no exista una comunicación local por medio del *bluetooth*, el dispositivo electrónico de control toma conexión con el vehículo mediante la conexión GPRS, a través de mensajes de texto, los mismo que pueden hacer sonar la bocina a través del mensaje de texto PITO800, bloquear la bomba de gasolina a través del mensaje de texto ROBO800, abrir los seguros de las puertas con el mensaje de texto ABRIR800 y cerrar nuevamente el relé de la bomba de gasolina a través del mensaje de texto RESTABLECER800.

Los comandos recibidos son receptados por el microcontrolador y se ejecutan cada vez que el usuario envíe un mensaje de texto.

### **3.3 Presupuesto y materiales**

A continuación, se describe los elementos electrónicos que conforman el dispositivo de control y seguridad del vehículo. Todos ellos se los consigue localmente y a un costo bajo.

Tabla. 3.6. Tabla de materiales y costos de los elementos electrónicos.

No.	DESCRIPCIÓN	CANT.	V. UNIT.	V. TOTAL
1	Microcontrolador Atmega 328P	1	\$ 5	\$ 5
2	Módulo Bluetooth HC-06	1	\$ 9	\$ 9
3	Módulo GPRS SIM800	1	\$ 25	\$ 25
4	Módulo GPS NEO-06	1	\$24	\$ 24
5	Módulo Step Down LM2596	1	\$ 8	\$ 8
6	Resistencias	4	\$ 0,10	\$ 0,40
7	Condensador electrolítico	1	\$ 0,80	\$ 0,80
8	Condensador cerámico	1	\$ 0,40	\$ 0,40
9	Cristal	1	\$ 1	\$ 1
10	Led	1	\$ 0,25	\$ 0,25
11	Transistor	2	\$ 1	\$ 2
12	Regleta hembra	1	\$ 1	\$ 1
13	Regleta macho	1	\$ 1	\$ 1
14	Bornera	1	\$ 1	\$ 1
15	Cables	1	\$ 1	\$ 1
16	Chip GSM	1	\$ 5	\$ 5
17	Saldo del Chip GSM	1	\$10	\$ 10
18	Horas de trabajo	150	\$ 3,5	\$ 375
19	Enclosure impreso en 3D	1	\$ 70	\$ 70
20	Imprevistos y varios	1	\$ 100	\$ 100
TOTAL				\$ 641,85

Fuente: Elaborado por el Autor.

### 3.4 Ventajas del control electrónico para encendido/bloqueo y seguridad de un vehículo

- En un mismo dispositivo se tiene integrado un sistema GPS, sistema de prevención de robo y también comunicación por la red celular.
- No necesita estar ligado a un plan mensual de rastreo satelital para saber la ubicación en tiempo real.
- Funciona como llave inteligente de los autos modernos que implementan este tipo de seguridad, con la adición de que al alejar el *smartphone* del dispositivo de seguridad este reacciona apagando el vehículo.
- En el caso de dejar las llaves dentro del vehículo, se puede abrir el seguro de la puerta, así como también bajar el vidrio de la puerta del conductor, sea local o remotamente.
- Localiza al vehículo mediante la bocina cuando se lo haya dejado en sitios grandes ya sean áreas abiertas o cerradas.

## CAPITULO 4

### IMPLEMENTACIÓN

En este capítulo se lleva a cabo la implementación del dispositivo de control electrónico para el encendido/bloqueo y seguridad de un vehículo de acuerdo a la propuesta presentada.

#### 4.1 Desarrollo

Para la implementación del dispositivo de control de seguridad fue necesario elaborar la programación para el microcontrolador, así como también diseñar el aplicativo del smartphone. El presente desarrollo permite realizar pruebas de funcionamiento del dispositivo y corregir posibles errores.

##### 4.1.1 Desarrollo del aplicativo

El aplicativo fue diseñado con el *App Inventor*, siendo este un entorno de desarrollo de *software* orientado a la elaboración de aplicaciones orientadas al sistema operativo Android. Tiene una interfaz de programación por bloques siendo muy sencilla de utilizar. (Riego, 2019)

Mediante el aplicativo se puede ejecutar tres acciones como abrir seguro, cerrar seguro y bajar ventana.

Primero, se configuró un botón en el aplicativo para que se pueda seleccionar el *bluetooth* a conectarse directamente de la interfaz, esto se realiza mediante una lista llamada *ListPicker* y no es más que una lista de cadena de texto.

Luego, se indica que el *ListPicker* muestre todos los dispositivos bluetooth que se encuentren dentro del rango de cobertura del smartphone, como se observa en la Figura 4.33.

```
when ListPicker1 . BeforePicking
do set ListPicker1 . Elements to BluetoothClient1 . AddressesAndNames
```

Figura. 4.33. Muestra los dispositivos bluetooth cercanos al smartphone  
Fuente: Elaborada por el Autor.

Una vez que se haya visualizado el *bluetooth* se lo selecciona y procede a conectarse con el *smartphone* como se observa en la Figura 4.34.

```
when ListPicker1 . AfterPicking
do set ListPicker1 . Selection to call BluetoothClient1 . Connect
address ListPicker1 . Selection
```

Figura. 4.34. Conexión con el bluetooth seleccionado.  
Fuente: Elaborada por el Autor.

Para la visualización en la interfaz se utilizó la botonera que se muestra en la Figura 4.35, con lo cual se selecciona el dispositivo a conectar y realiza el vínculo con el dispositivo de seguridad.



Figura. 4.35. Botón para seleccionar bluetooth.  
Fuente: Elaborado por el Autor.

Cuando se abra la aplicación y se seleccione el *bluetooth* por medio de la botonera que se creó, se tendrá una lista de dispositivos como se muestra en la Figura 4.36. El siguiente paso es seleccionar el bluetooth con el cual se desea emparejar y se obtendrá la conexión entre ambos dispositivos.



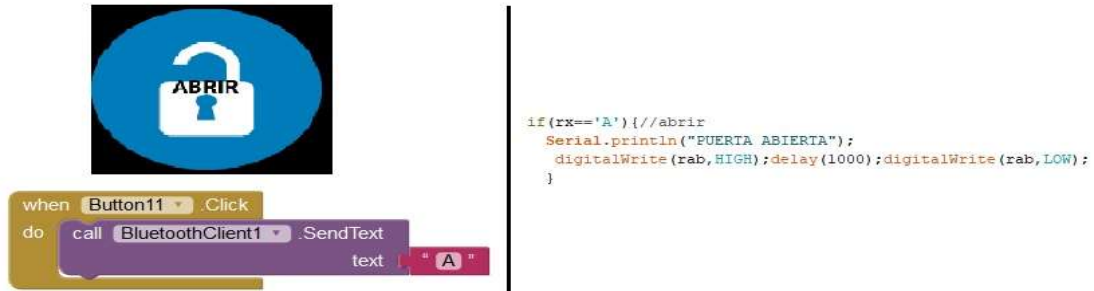


**Figura. 4.36. Lista de dispositivos bluetooth disponibles.**  
Fuente: Elaborado por el Autor.

Se debe asignar los botones que realizaran las acciones que anteriormente se describieron, para lo cual se creó los siguientes botones, abrir, cerrar y ventana, los que van ligados al microcontrolador para que este sepa la función que debe realizar.

Al botón de abrir los seguros de la puerta se le asignó el nombre de *button11*, el cual está programado para enviar la letra A cuando este sea seleccionado. La letra A es recibido por el microcontrolador y realiza la acción de activar una salida digital en el pin 5 del microcontrolador, el cual también accionará el relé que se encuentra conectado en esta salida.

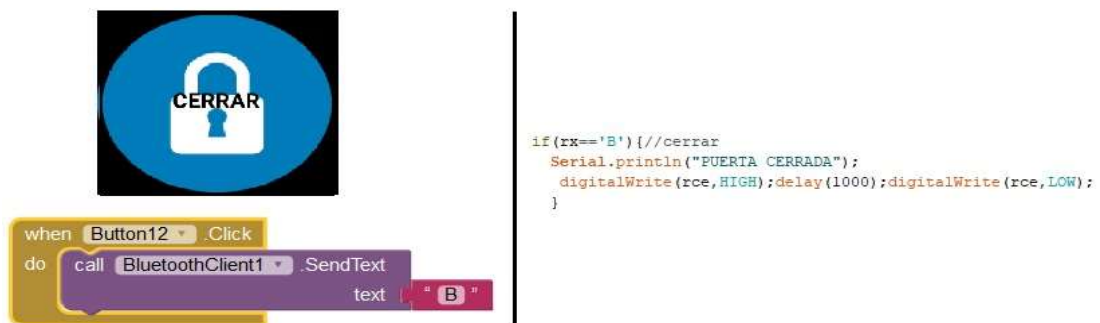
En la Figura 4.37, se observa al costado izquierdo la visualización del botón en el aplicativo, así como la programación en *App Inventor* y a la derecha la programación en el microcontrolador.



**Figura. 4.37. Programación botón abrir seguros del vehículo.**  
Fuente: Elaborado por el Autor.

Así mismo, se configuró el botón de cerrar seguros, el cual en la configuración del aplicativo es llamado *button12* y que envía la letra B al microcontrolador al ser accionado, el microcontrolador gestionará esta letra y lo buscará en su configuración para proceder con la acción correspondiente a realizar. Este botón activa el pin 6 del microcontrolador que tiene un relé conectado a esta salida.

En la Figura 4.38, se observa al costado izquierdo la visualización del botón en el aplicativo, así como la programación en *App Inventor* y a la derecha la programación en el microcontrolador.



**Figura. 4.38. Programación botón cerrar seguros del vehículo.**  
Fuente: Elaborado por el Autor.

El ultimo botón que se creó, es el de la ventana, el mismo que va a permitir bajar la ventana del conductor, en el desarrollo del aplicativo es llamado *button13*. De la misma manera, al presionar se enviará la letra C al microcontrolador el cual será comparado con la programación del microcontrolador y realizará la acción de abrir la ventana. El pin 8 del microcontrolador será el encargado de accionar el relé para el propósito descrito.

En la Figura 4.39, se observa al costado izquierdo la visualización del botón en el aplicativo, así como la programación en *App Inventor* y a la derecha la programación en el microcontrolador.

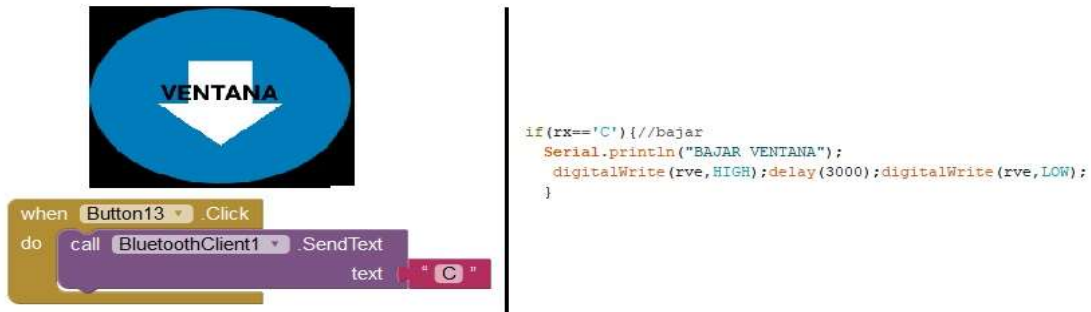


Figura. 4.39. Programación botón para bajar una ventana del vehículo.  
Fuente: Elaborado por el Autor.

Una vez definidos los botones de la interfaz del aplicativo, se desarrolló los botones de desconectar y cerrar aplicación.

El botón de desconectar permite terminar la comunicación entre el *smartphone* y el módulo *bluetooth HC-06*, es una opción necesaria si se desea establecer la comunicación con otro dispositivo. El botón de cerrar aplicación será etiquetado como *button6*.

En la Figura 4.40, se muestra el botón desconectar que se visualizará en el aplicativo cuando esté terminado, con su respectiva programación en *App Inventor*.



Figura. 4.40. Programación botón desconectar.  
Fuente: Elaborado por el Autor.

El botón de cerrar aplicación es fundamental ya que si no se cierra la aplicación esta va a estar corriendo en segundo plano y si no tiene conexión con el dispositivo de seguridad emitirá un pitido y también el *smartphone* vibrará. El botón de cerrar aplicación fue etiquetado como *button14*.

Esto se consideró como medida de seguridad para alertar al usuario que ha perdido comunicación con el dispositivo y que debe revisar la comunicación.

En la Figura 4.41, se muestra el botón de cerrar aplicación, que va a mostrar el aplicativo cuando esté instalado en el *smartphone*.



**Figura. 4.41. Programación botón cerrar aplicación.**  
Fuente: Elaborado por el Autor.

Es importante programar un tipo de alerta audible y vibratoria que indique que se ha perdido la conexión entre el *smartphone* y el dispositivo de seguridad, con esto se puede saber que el vehículo se apagará.

El usuario al tener esta notificación deberá detenerse y volver a realizar la conexión.

En la Figura 4.42, se muestra la programación para que el aplicativo emita una alerta audible en caso de desconexión con el dispositivo de control electrónico.

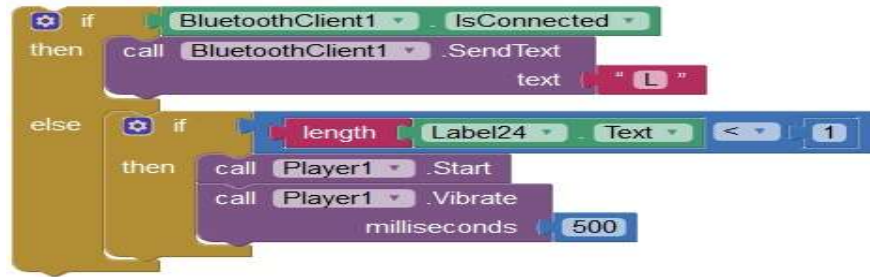


Figura. 4.42. Programación para alerta audible por desconexión entre el smartphone y el dispositivo de seguridad.

Fuente: Elaborado por el Autor.

Una vez realizadas estas configuraciones el aplicativo está listo para ser compilado y exportado por la misma plataforma a un formato .APK, el cual es un formato comprimido que el sistema operativo Android dará lectura y lo instalará.

La Figura 43. Muestra la interfaz que se me visualizará en el *smartphone*.



Figura. 4.43. Aplicativo instalado en smartphone.

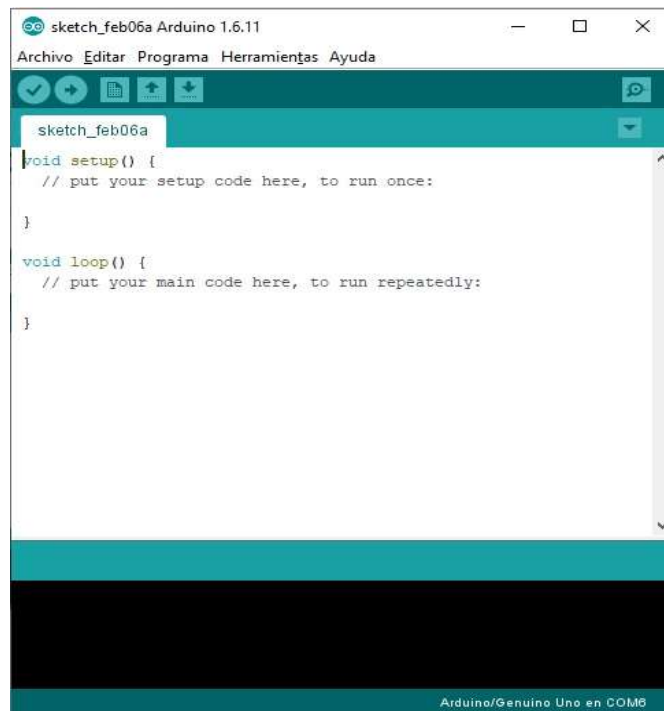
Fuente: Elaborado por el Autor.

#### 4.1.2 Desarrollo del software para microcontrolador 328P.

La programación del microcontrolador Atmega 328P se lo realiza a través del IDE de Arduino, debido a la sencillez de trabajo de la interfaz, además de tener la facilidad de ser descargable directamente de la página oficial de Arduino.

Se consideró trabajar con la versión portable 1.6.11, debido a que el IDE puede ser transportado y ejecutado desde cualquier dispositivo de almacenamiento USB, sin la necesidad de ser instalado en sistemas operativos como otras versiones.

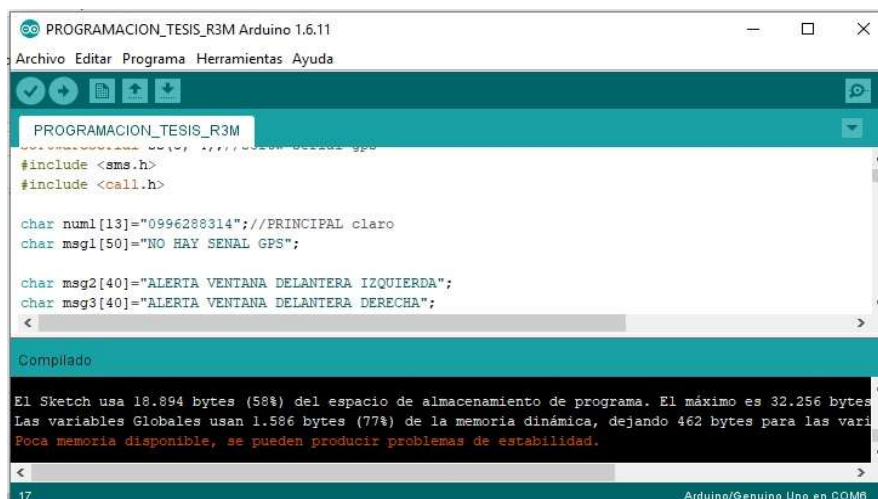
La Figura 4.44, muestra el entorno de programación de Arduino en la versión portable.



**Figura. 4.44. Interfaz de programación portable versión 1.6.11 de Arduino.**  
Fuente: Elaborado por el Autor.

Cuando se haya realizado la programación para el microcontrolador se la debe compilar para ver si no posee errores de programación, caso contrario se debe corregir el error.

Como se puede observar en la figura 4.45, en el área de mensajes indica compilado, quiere decir que el programa no tiene errores, así también en la consola se aprecia el porcentaje de espacio que ocupa la programación en el microcontrolador.

The image shows a screenshot of the Arduino IDE interface. The title bar reads "PROGRAMACION\_TESIS\_R3M Arduino 1.6.11". The menu bar includes "Archivo", "Editar", "Programa", "Herramientas", and "Ayuda". The toolbar contains icons for opening, saving, and running. The main editor window shows the following code:

```
PROGRAMACION_TESIS_R3M
//...
#include <ams.h>
#include <call.h>

char num1[13]="0996288314";//PRINCIPAL claro
char msg1[50]="NO HAY SENAL GPS";

char msg2[40]="ALERTA VENTANA DELANTERA IZQUIERDA";
char msg3[40]="ALERTA VENTANA DELANTERA DERECHA";
```

Below the code is the "Compilado" (Compiled) section, which displays the following message:

```
El Sketch usa 18.894 bytes (58%) del espacio de almacenamiento de programa. El máximo es 32.256 bytes
Las variables Globales usan 1.586 bytes (77%) de la memoria dinámica, dejando 462 bytes para las vari
Poca memoria disponible, se pueden producir problemas de estabilidad.
```

The status bar at the bottom indicates "17" and "Arduino/Genuino Uno en COM6".

**Figura. 4.45. Mensaje de compilación exitosa en el IDE de Arduino.**  
**Fuente: Elaborado por el Autor.**

Una vez que la programación está lista se debe cargarla al microcontrolador Atmega 328P, para esto se utilizó el Arduino Uno, debido a que el microcontrolador que éste trae embebido es el mismo microcontrolador con el que se trabaja en el presente proyecto.

Se debe insertar el microcontrolador en el sócalo y conectar vía USB al Arduino a la PC, ahí se procede a indicar al IDE que se está conectado el Arduino Uno para que realice la descarga de la programación.

Cuando se haya realizado la descarga se podrá extraer el microcontrolador de la placa Arduino y se la instalará en el sócalo de la PCB del dispositivo de seguridad.

En la Figura 4.46, se observa cómo es la conexión física entre la PC y el dispositivo Arduino uno para cargar el programa que se compilo previamente.



**Figura. 4.46. Carga de programación al Atmega 328P.**  
Fuente: Elaborado por el Autor.

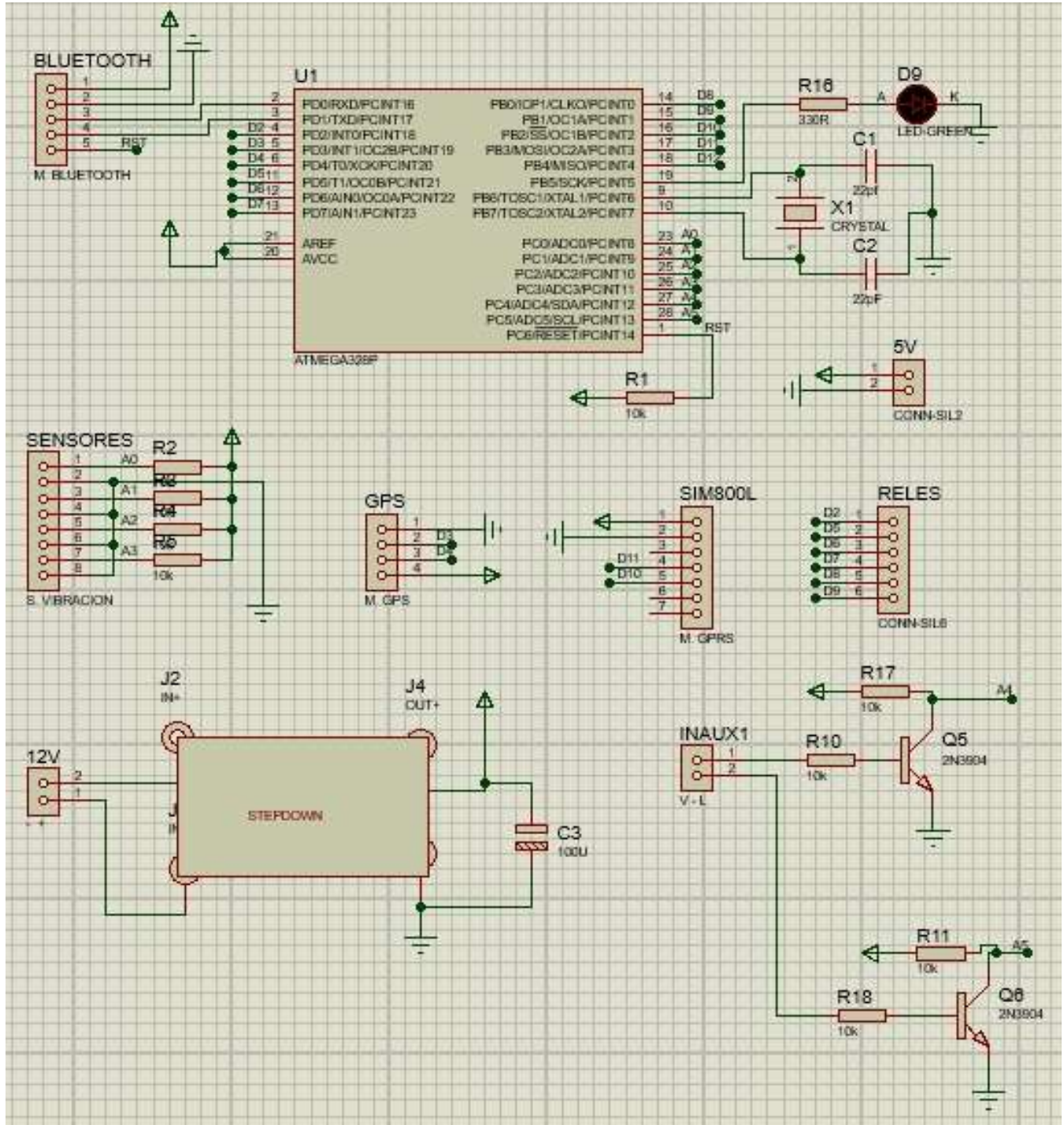
#### 4.1.3 Desarrollo del hardware.

Para el desarrollo del *hardware* se utilizó el *software* Proteus, el cual permite diseñar circuitos electrónicos y de placas PCB. Se utilizó la versión 8.7 que es una de las más actuales.


Cuando se ha reunido los elementos en el *software* y se ha realizado las conexiones necesarias de todos los elementos que van a intervenir en el dispositivo se obtendrá el diagrama esquemático electrónico.

A continuación, en el rotulado, se observa el diagrama esquemático del dispositivo de control electrónico encendido/bloqueo y seguridad de un vehículo.



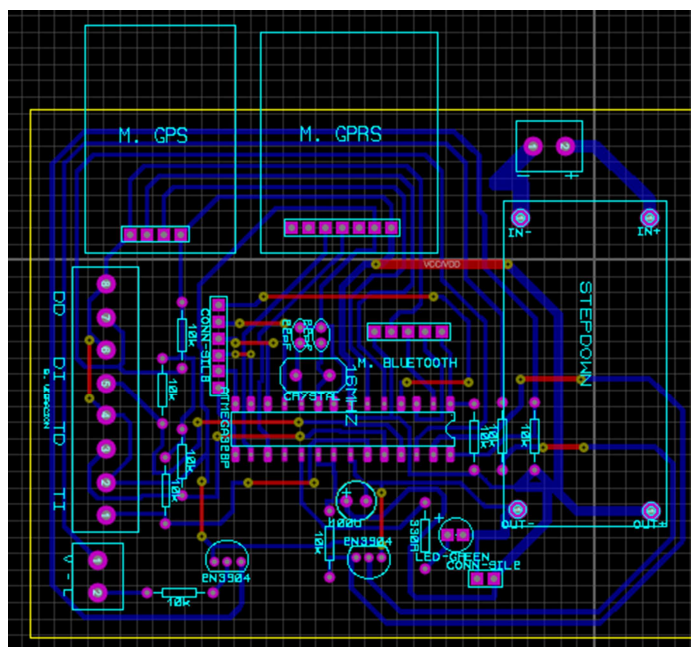


UNIVERSIDAD TECNOLÓGICA ISRAEL

Esc. 1:1	Observación: Diseñado en Proteus	Fecha: 25-02-2019	Cuadro de Referencia Diagrama Esquemático	
	Autor: Ricardo Ramos M.		Tutor: Ing. L. Montoya	Calificación:
	DIAGRAMA ESQUEMÁTICO DEL DISPOSITIVO DE CONTROL ELECTRÓNICO PARA ENCENDIDO/BLOQUEO Y SEGURIDAD DE UN VEHÍCULO.			

El *software* Proteus también permite realizar la placa PCB, se debe hacer el ruteo de las pistas que previamente fueron diseñadas en el diagrama esquemático para posteriormente quemar la placa de baquelita.

En la Figura 4.47, se muestra el diseño de la placa PCB realizada en el programa Proteus.



**Figura. 4.47. Diseño de placa PCB.**  
Fuente: Elaborado por el Autor.

Adicionalmente se puede obtener del *software* Proteus una imagen en tres dimensiones de cuál va a ser el resultado final de la placa del dispositivo de seguridad.

En la figura 4.48, se observa una simulación en 3D del trabajo realizado en el *software* Proteus, respecto al dispositivo de control electrónico encendido/bloqueo y seguridad de un vehículo.

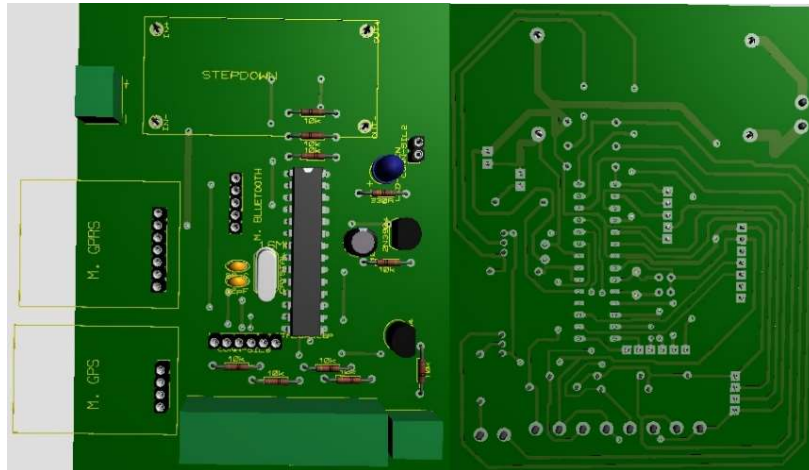


Figura. 4.48. Simulación 3D de la placa del dispositivo de seguridad.  
Fuente: Elaborado por el Autor.

## 4.2 Implementación

La implementación del dispositivo de seguridad inicia con la placa PCB y la soldadura de los diferentes elementos que conforman todo el circuito.

En la Figura 4.49, se aprecia la placa de baquelita con algunos elementos ya soldados a ella.

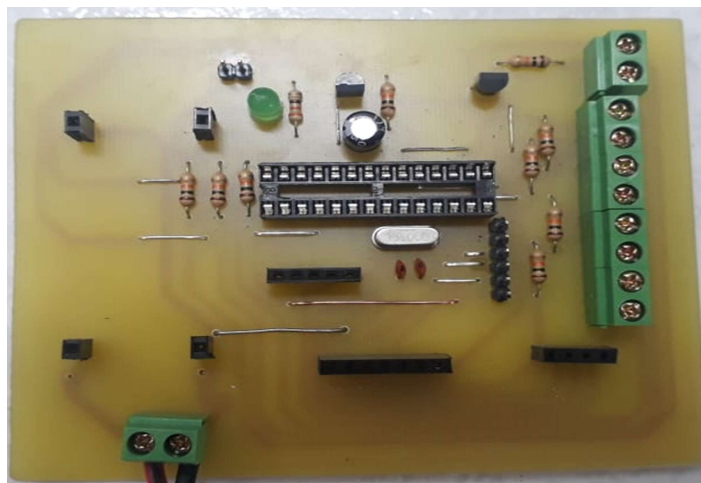
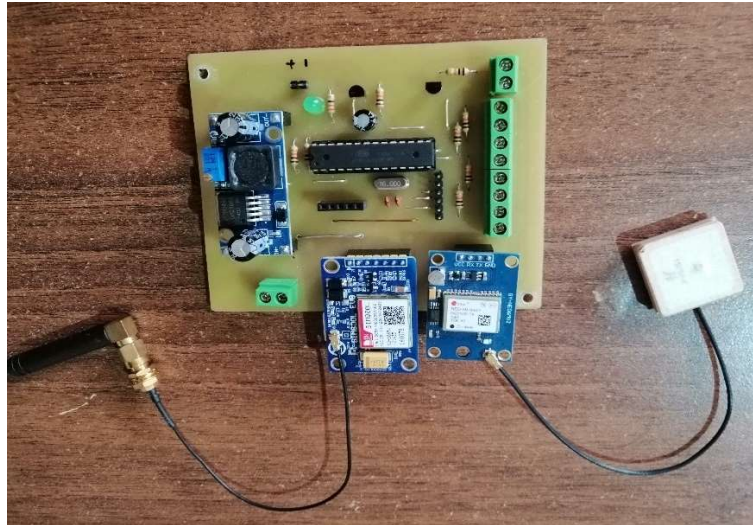


Figura. 4.49. Soldadura de los elementos del dispositivo de seguridad.  
Fuente: Elaborado por el Autor.

Una vez soldado todos los elementos en la placa PCB se inserta en los sócalos los diferentes módulos como el *bluetooth*, GPS, GPRS, *Step Down*.

En la Figura 4.50, se observa el montaje de los módulos GPS y GPRS en el dispositivo de seguridad electrónica encendido/bloqueo y seguridad de un vehículo.



**Figura. 4.50. Montaje de módulos en placa PCB.**  
Fuente: Elaborado por el Autor.

Se debe tener en cuenta que hay que insertar la *Sim Card* en el módulo SIM800 para poder establecer comunicación mediante la operadora elegida. Para el dispositivo electrónico se utilizó una *Sim Card* de la operadora CNT la cual tiene el numero celular 096 057 9419.

En la Figura 4.51, se observa la inserción de la *Sim Card* de la operadora CNT en el módulo Sim800.

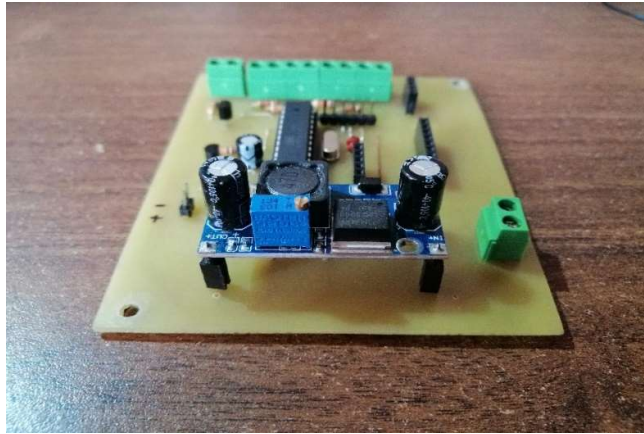


**Figura. 4.51. Módulo Sim800 con *Sim Card*.**

**Fuente: Elaborado por el Autor.**

Para el óptimo funcionamiento de todos los módulos que conforman el dispositivo de seguridad se agrega un *Step Down*, su función es brindar a todos los elementos de la paca un voltaje fijo de trabajo y con la característica de que puede entregar hasta 3A de corriente, con lo que se garantiza que cada dispositivo recibe un voltaje fijo y abastecerá para el consumo de corriente.

En la Figura 4.52, se observa el módulo *Step Down*, mismo que es el encargado de entregar el voltaje necesario a todos los elementos del dispositivo de seguridad electrónica encendido/bloqueo y seguridad de un vehículo.



**Figura. 4.52. Módulo *Step Down* LM2596.  
Fuente: Elaborado por el Autor.**

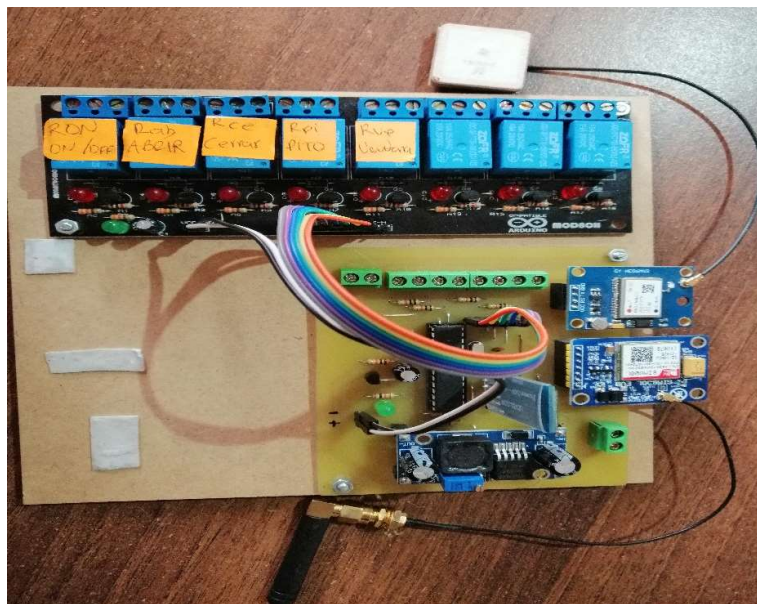
Adicionalmente se incorporó un módulo relé de 8 canales, como se aprecia en la Figura 4.53, de los cuales se utilizó uno para la bomba de gasolina, otro para la apertura de seguros de las puertas, otro para cerrar los seguros de las puertas, otro para la bocina y el último para la ventana del conductor. Se dejan tres relés adicionales para cualquier implementación a futuro.



**Figura. 4.53. Módulo de relés de 8 canales.**  
Fuente: Elaborado por el Autor.

Para realizar las pruebas de funcionamiento se coloca la PCB en una superficie plana que sirva de base, previamente a insertarla en el *enclosure* que será instalado en el vehículo.

En la Figura 4.54, se observa la colocación de una superficie plana para contener a todo el dispositivo de seguridad electrónico encendido/bloqueo y seguridad de un vehículo a fin de realizar las pruebas respectivas.



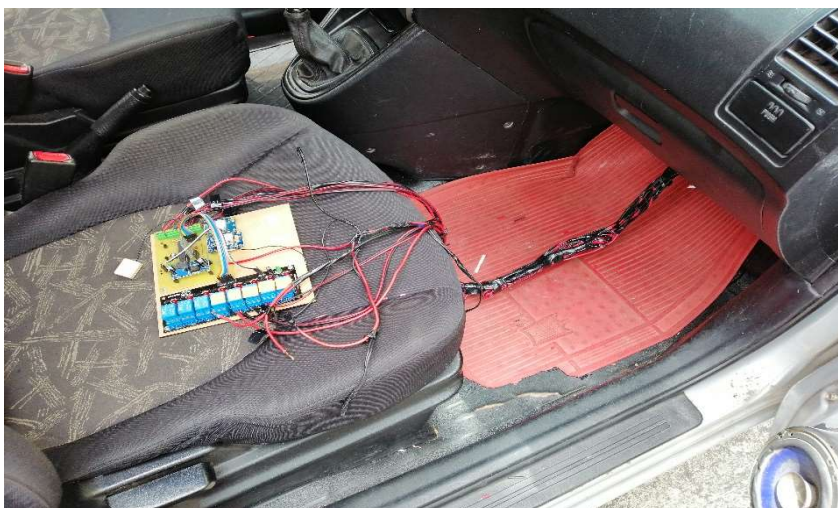
**Figura. 4.54. Placa PCB montada en superficie plana para pruebas.**  
Fuente: Elaborado por el Autor.

Se instaló el dispositivo de seguridad en un vehículo tipo *hatchback*, marca Hyundai modelo matriz del año 2003 como se observa en la Figura 4.55, en este se realizaron todas las pruebas de funcionamiento.



**Figura. 4.55.** Vehículo de pruebas e implementación.  
**Fuente:** Elaborado por el Autor.

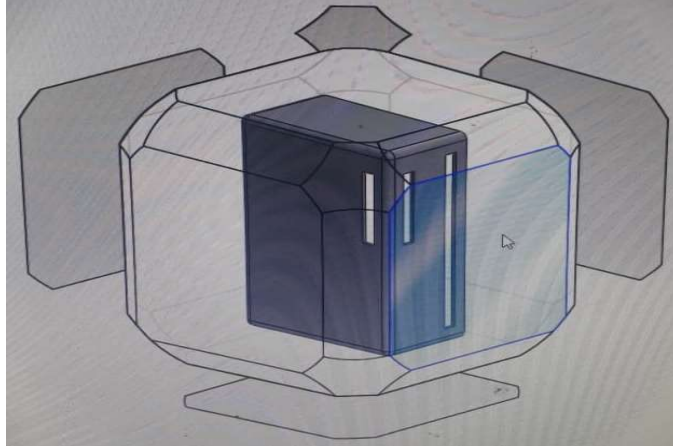
Se realizaron las pruebas de funcionamiento con el vehículo como se observa en la Figura 4.56, con una instalación provisional, esto indica que errores se pueden presentar tanto en conexiones físicas como de programación. De esta manera se podrán evidenciar las diferentes posibilidades de corrección de los errores que surjan.



**Figura. 4.56.** Instalación provisional para verificar funcionamiento del dispositivo.  
**Fuente:** Elaborado por el Autor.

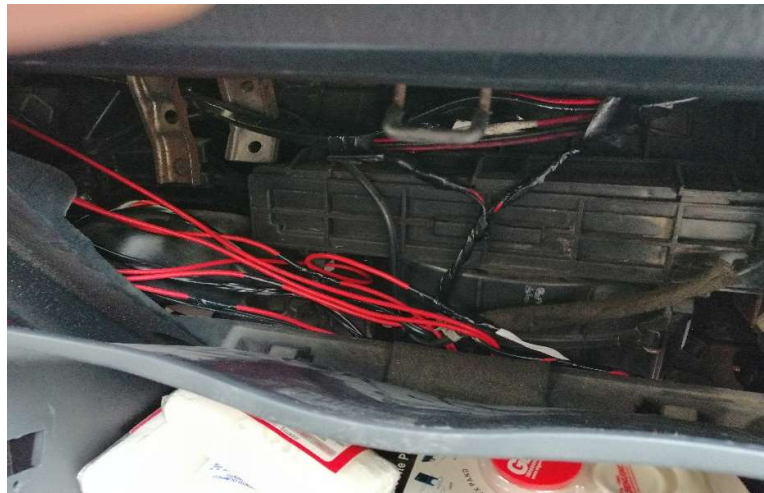
El *enclosure* que va a contener a la placa PCB, se lo construyó en una impresora 3D. Visualmente la presentación del contenedor será apropiada ya que es de plástico ABS resistente a golpes y será almacenado detrás de la guantera del vehículo.

En la Figura 4.57, se observa el diseño en 3D del *enclosure* del sistema de control electrónico encendido/bloqueo y seguridad de un vehículo antes de ser impreso.



**Figura. 4.57. Diseño del *enclosure* para placa ABS.**  
Fuente: Elaborado por el Autor.

Para la implementación en el vehículo, se consideró instalar el *enclosure* detrás de la guantera como se aprecia en la Figura 4.58, por lo que las conexiones que se van a realizar en las diferentes partes del vehículo deberán llegar hasta dicho compartimento.



**Figura. 4.58. Parte posterior de la guantera.**  
Fuente: Elaborado por el Autor.

Los detectores de ruptura de vidrio se colocaron en cada ventana, tomando en cuenta que al bajar y subir las ventanas no tenga inconvenientes por rozamiento o estancamiento



con los mecanismos que tiene el eleva vidrios eléctricos entre otros componentes internos que pueden tener las puertas tal como se aprecia en la Figura 4.59.



**Figura. 4.59. Instalación sensor de vibración.**  
Fuente: Elaborado por el Autor.

Para la apertura de las puertas se debe localizar el módulo del bloqueo central para realizar la conexión hacia el dispositivo de seguridad. Todos los fabricantes de bloqueos centrales proveen de dos cables que sirven para la apertura y cierre de los seguros de las puertas, siempre se deberá verificar cuales son los pines para ese propósito como se muestran en la Figura 4.60.



**Figura. 4.60. Conexión a módulo de bloqueo central.**  
Fuente: Elaborado por el Autor.

Se debe verificar cual es el circuito que lleva la corriente hacia la bocina y hacia la ventana del conductor con la finalidad de abrir los circuitos e insertarlos en serie al relé que controlan estos dispositivos.

En la figura 4. 61, se observa la circuitería del vehículo debajo del volante que es donde se localizan los circuitos de la bocina y la ventana del conductor.



**Figura. 4.61. Circuitos de bocina y ventana del conductor.**  
**Fuente: Elaborado por el Autor.**

Por último, se revisó cuáles son los cables que proporcionan voltaje a la bomba de gasolina para abrirlo e insertarlo al relé, de esta manera se tiene el control sobre el bombeo de gasolina hacia el motor.

En la Figura 4.62, se muestra la bomba de gasolina, donde se abrirá el circuito para conectarlo al relé del dispositivo electrónico de control encendido/bloqueo y seguridad de un vehículo.



**Figura. 4.62. Bomba de gasolina del vehículo.**  
Fuente: Elaborado por el Autor.

### 4.3 Pruebas de funcionamiento.

Las pruebas de funcionamiento se las dividió en tres partes: la local que funciona mediante el módulo *bluetooth* y la remota que funciona mediante el módulo GPRS.

#### 4.3.1 Pruebas Locales por bluetooth.

Las pruebas locales se realizaron de la siguiente manera:

1. Se realizó la conexión inalámbrica entre el *smartphone* y el módulo *bluetooth* del dispositivo de control electrónico. Cabe mencionar que mientras no exista conexión o ésta se pierda, se genera una alerta audible en el *smartphone*.
2. Una vez conectado se verificó que el vehículo se pueda encender normalmente. Si el vehículo enciende es indicativo de que la función llave inteligente está operativa.
3. Se probó el funcionamiento del botón abrir, el cual al seleccionarlo debe abrir el seguro de las puertas que estén dentro del bloqueo central, en este caso abre las puertas del conductor y el copiloto.
4. Se probó el funcionamiento del botón cerrar, el cual también al seleccionarlo debe cerrar el seguro de las puertas.
5. Se probó el funcionamiento del botón ventana, el cual al ser seleccionado debe bajar la ventana del conductor del vehículo por tres segundos.

6. Se probó el funcionamiento del botón desconectar, el cual al ser seleccionado debe desconectar la actual comunicación existente entre el *smartphone* y el módulo *bluetooth* del dispositivo electrónico de control. Adicionalmente el *smartphone* debe emitir la señal sonora ya que se desvincularon ambos dispositivos.
7. Se probó el funcionamiento del botón cerrar aplicación, el cual al ser seleccionado debe cerrar el aplicativo en el *smartphone* y la alerta audible se detiene.

También se realizaron pruebas de desconexión por distancia, esto debido a que el usuario puede alejarse por un rango de diez metros que indica el fabricante del módulo HC-06, con lo cual si se da esta premisa el auto se apagará y cerrará el seguro de las puertas una vez haya pasado un minuto.

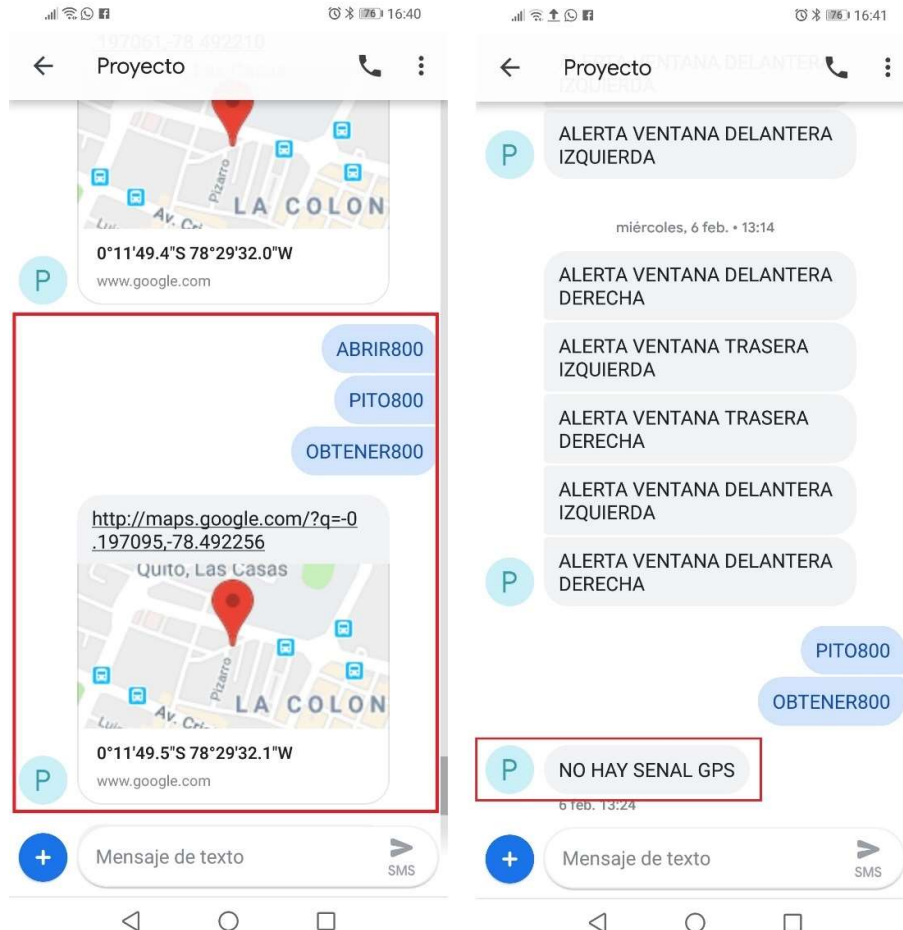
#### 4.3.2 Pruebas remotas por GSM/GPRS

Se enviaron los mensajes de texto con cada acción a ejecutar, teniendo en cuenta que no existe conexión *bluetooth*. La respuesta positiva a la prueba es que el dispositivo electrónico de control haga que se ejecuten las diferentes acciones sobre el vehículo.

1. Apertura de seguros de puertas: Se envió el texto ABRIR800 al dispositivo electrónico de control y se verifica que los seguros de las puertas se abren.
2. Bocina del vehículo: Se envió el texto PITO800 al dispositivo electrónico de control y se verifica que la bocina suene por 5 segundos.
3. Ubicación geográfica del vehículo: Se envió el texto OBTENER800 al dispositivo electrónico de control y se debe recibir de vuelta vía mensaje de texto un *link* para poderlo abrir y verificar mediante *Google Maps* la ubicación del vehículo. En el caso de no tener cobertura GPS, el NE0-6 informará al microcontrolador este particular y hará que el GPRS envíe al usuario un mensaje de texto indicando “NO HAY SEÑAL GPS”.

En la Figura 4.63 se muestra las pruebas remotas que se enviaron al dispositivo de control electrónico para las funciones de apertura de seguros de las puertas, bocina y GPS,

adicionalmente se aprecia que cuando no existe señal GPS, el módulo GSM nos envía la notificación.



**Figura. 4.63. Pruebas remotas o GSM/GPRS**  
Fuente: Elaborado por el Autor.

Para la prueba de robo fue necesario simular la acción. Si el usuario sufre un atraco cuando esté circulando o esté parqueado con el vehículo encendido, el atracador puede llevarse sin ningún problema el vehículo siempre y cuando el *smartphone* haya quedado dentro del automotor, ya que realiza la función de llave inteligente.

Para solventar esta eventualidad se programó al microcontrolador para que enviando el mensaje de texto ROBO800, desde cualquier *smartphone* al número celular del dispositivo de control electrónico el dispositivo electrónico de control abra el relé de la bomba de

gasolina sin importar que exista la conexión local mediante *bluetooth*, con lo cual garantiza que el vehículo va a dejar de continuar movilizándose.

Una vez que se haya recuperado el vehículo debido a que no pudo movilizarse, el usuario envía el mensaje de texto RESTABLECER800, con lo cual el dispositivo electrónico de control regresa el control del vehículo al smartphone que actúa como llave inteligente.

Adicionalmente se realizó la prueba con los sensores de ruptura de vidrio, la prueba consistió en simular una eventual ruptura de los vidrios del conductor, copiloto y de las dos ventanas posteriores.

Se dejó caer al sensor desde la altura donde va a estar adherido al vidrio hasta la parte interna de la puerta. La altura prevista es la suficiente para activar al sensor y que envíe la señal al microcontrolador para que éste, envíe un mensaje de texto a través del módulo GPRS al usuario. Dependiendo de la ventana que se rompa, el texto del mensaje será, “ALERTA VENTANA DELANTERA DERECHA”, “ALERTA VENTANA DELANTERA IZQUIERDA”, “ALERTA VENTANA TRASERA DERECHA” ó “ALERTA VENTANA TRASERA IZQUIERDA”, con lo cual se sabe que existe una intrusión por ruptura de vidrio hacia el vehículo.

Otra prueba adicional, fue verificar el funcionamiento del dispositivo electrónico de control con *sim cards* de las tres operadoras telefónicas como se observa en la Figura 4.64.

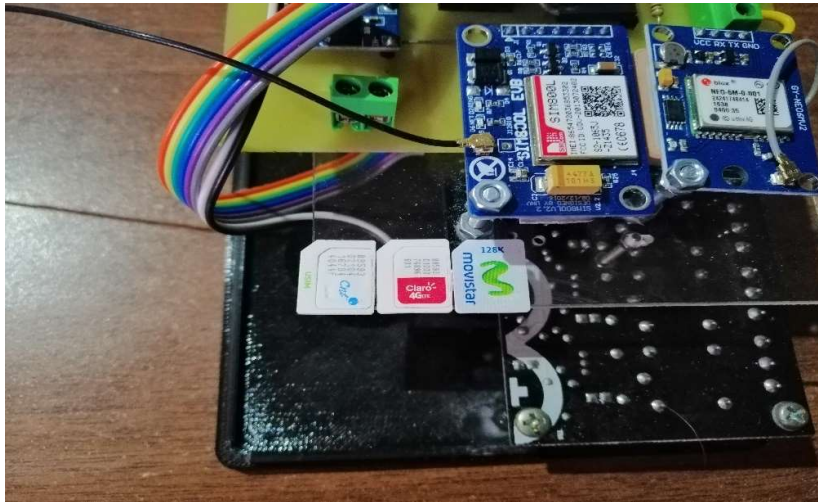


Figura. 4.64. Pruebas GSM/GPRS con las tres operadoras celulares.  
Fuente: Elaborado por el Autor.

#### 4.4 Análisis de resultados

##### 4.4.1 Análisis de resultados locales por bluetooth.

Para las pruebas locales mediante *bluetooth*, se ubicó el smartphone cada tres metros y a partir de los 10 metros se prueba cada metro adicional como se observa en la Figura 4.65.



Figura. 4.65. Pruebas de alcance de conexión módulo bluetooth.  
Fuente: Elaborado por el Autor.

En la Tabla 4.7, se observa hasta cuantos metros existe comunicación *bluetooth* y cuando se pierde.

**Tabla. 4.7. Pruebas de distancia módulo Bluetooth HC-06**

Bluetooth vinculado en cada posición	3m	6m	9m	10m	11m	12m	13m
Conexión	x	x	x	x	x		
Desconexión						x	x

**Fuente: Elaborado por el Autor.**

Se concluye que el rango de funcionamiento localmente mediante el módulo *bluetooth* es de 11m de radio, con lo que en esta distancia los botones de el aplicativo funcionan correctamente.

#### 4.4.2 Análisis de resultados remotos o por GPRS

Como se observa en la Tabla 4.8, se verificó el funcionamiento remoto del dispositivo electrónico de control con las tres *sim cards* de las operadoras que brindan el servicio de telefonía celular en el país, validando el correcto funcionamiento con cada una de ellas.

**Tabla. 4.8. Verificación de funcionamiento remoto del dispositivo de control electrónico.**

COMANDO	OPERADORA 1	OPERADORA 2	OPERADORA 3
ABRIR800	x	x	x
PITO800	x	x	x
OBTENER800	x	x	x
RESPUESTA CON COORDENADAS DEL GPS	x	x	x
RESPUESTAS DE NO HABER SEÑAL GPS	x	x	x
ROBO800	x	x	x
RESTABLECER800	x	x	x

**Fuente: Elaborado por el Autor.**



Se concluye que el dispositivo electrónico de control funciona con cualquier operadora telefónica de red celular y que en todos los casos los comandos enviados por mensaje de texto se ejecutaron con normalidad.

También se realizó pruebas de cobertura en subsuelos, se va a verificar el número de subsuelos en el cual el módulo SIM800 puede tener cobertura de señal celular.

**Tabla. 4.9. Señal celular en subsuelos.**

<b>No. SUBSUELO</b>	<b>SEÑAL CELULAR EN DISPOSITIVO ELECTRÓNICO</b>
SUBSUELO 1	SI
SUBSUELO 2	NO
SUBSUELO 3	NO

**Fuente: Elaborado por el Autor.**

En la Tabla 4.9, se observa que la señal celular tubo cobertura hasta el primer subsuelo, a partir del subsuelo 2 y 3 no se tenía respuesta del dispositivo electrónico.

#### **4.4.3 Análisis de resultados remotos por GPS**

Como se observa en la Tabla 4.10, se realizaron pruebas de cobertura de la señal GPS, con los subsuelos donde se realizaron las pruebas de cobertura celular, este propósito es para conocer hasta dónde el módulo NEO-6 va a brindar cobertura.

La señal GPS del módulo NEO-6, se pierde por completo en el primer subsuelo, por lo que, cuando el dispositivo se encuentre bajo un solo subsuelo no existirá cobertura.

**Tabla. 4.10. Pruebas de cobertura GPS.**

<b>No. SUBSUELO</b>	<b>SEÑAL GPS EN DISPOSITIVO ELECTRÓNICO</b>
SUBSUELO 1	NO
SUBSUELO 2	NO
SUBSUELO 3	NO

**Fuente: Elaborado por el Autor.**

## CONCLUSIONES

Se definieron los parámetros y dispositivos a ser utilizados para la ejecución del dispositivo de control electrónico, todos ellos son de fácil accesibilidad en el mercado local y con costos bajos.

La tarjeta de control fue diseñada para ser gobernada por el microcontrolador AVR328P, el cual maneja todos los dispositivos que están asociados al diseño, el microcontrolador cuenta con el número suficiente de entradas y salidas para el proyecto.

Se desarrolló todas las etapas de comunicación, la etapa de comunicación del dispositivo bluetooth hacia el aplicativo, así como la etapa de comunicación GSM hacia el *smartphone*. Esto es de mucha importancia debido a que ninguna de ellas puede fallar en el proceso caso contrario no cumpliría con las expectativas previstas.

El aplicativo se programó para la ejecución de comandos locales, el mismo trabaja también en segundo plano para no interrumpir con la llamada de entradas u otras acciones que el *smartphone* puede realizar. Así también el microcontrolador fue programado para la recepción de mensajes de texto a través del módulo GPRS, el mensaje de texto consta de una palabra y un número como medida de seguridad para que no cualquiera pueda enviar comandos al dispositivo.

Se realizaron pruebas de funcionamiento del dispositivo en el vehículo, todas las funcionalidades que se integraron en el dispositivo de control electrónico fueron validadas, por lo que el dispositivo funciona correctamente.

## RECOMENDACIONES

Para lograr la apertura y cierre de las puertas del vehículo es necesario que el auto cuente con un sistema de bloqueo central ya instalado, de esta manera el dispositivo de seguridad electrónica se acopla y está en la capacidad de abrir y cerrar los seguros de las puertas.

Se debe verificar que la bocina del vehículo esté funcionando para que al integrarlo al dispositivo de seguridad cumpla con realizar el aviso sonoro.

Se debe hacer una recarga de saldo a la *sim card* de al menos \$1 al mes o a su vez \$12 por año, esto va a depender del uso de SMS que se ocupe en el dispositivo. Se debe revisar cual es el costo por cada SMS enviado en la operadora con la que se desea trabajar.

Es necesario no dejar al vehículo sin actividad por un periodo prolongado de tiempo debido a la descarga de la batería, si ese es el caso el dispositivo no tendrá alimentación y dejará de funcionar.

No se debe juntar la antena del módulo GSM/GPRS con la antena del módulo GPS, debido a que causa interferencias una con otra y ninguna puede desempeñar la función que realiza.

## REFERENCIAS BIBLIOGRÁFICAS

Meganeboy, D. (2016). *Inmovilizador electrónico*. Aficionados a la mecánica. Recuperado de <http://www.aficionadosalamecanica.com/inmovilizador.htm>

Digital, A. (2019). *Métodos de recolección de datos*. Venezuela: Centro de Estudios de Estrategias Digitales Universidad Monteávila. Recuperado de <http://www.uma.edu.ve/audiencia/wordpress/metodos-de-recoleccion-de-datos-en-una-investigacion-cualitativa/>

Duplirapid. (2019). *Duplicado de llaves electrónicas de coche*. España: Duplirapid. Recuperado de <https://duplirapid.com/duplicado-de-llaves-electronicas-de-coche/>

Electronics, G. (2019). *Piezoelectricidad*. Sensor de vibración piezoeléctrico. Recuperado de <http://www.geekbotelectronics.com/producto/sensor-de-vibracion-piezo-electrico/>

INFOOTEC. (2018). *Sensor de vibración SW-18015P*. Infootec. Recuperado de <https://www.infootec.net/sensor-vibracion-sw-18015p/>

Iza, C. (2018). *Diseño e implementación de un Biométrico Inteligente que envíe SMS de alerta a los empleados antes de su hora de entrada* (Tesis de pregrado). Universidad Tecnológica Israel, Quito, Ecuador.

Maldonado, P. (2018). *El mundo utiliza las 'Apps' para todo o casi todo*. Quito, Ecuador. Revista Líderes. Recuperado de <https://www.revistalideres.ec/lideres/mundo-utiliza-apps.html>

Pérez, J. (2017). *Definición de Android*. Definición.de. Recuperado de <https://definicion.de/android/>

Premo. (2019). *Antenas RFID Premo*. Málaga, España. Premo. Recuperado de <https://www.grupopremo.com/610-kgea-af-and-kgea-afc-long-range-flexible-antenna-lf-for-smart-entry-system>

Riego, A. R. (2019). *Primeros pasos con APP Inventor I*. APP Inventor en Español. Recuperado de <https://sites.google.com/site/appinventormegusta/primeros-pasos>

## ANEXOS

### PROGRAMACIÓN

```
#include <SoftwareSerial.h>
#include <TinyGPS.h>
TinyGPS gps;
SoftwareSerial ss(3, 4);//softw serial gps
#include <sms.h>
#include <call.h>

char num1[13]="0996288314";//PRINCIPAL claro
char msg1[50]="NO HAY SENAL GPS";
char msg2[40]="ALERTA VENTANA DELANTERA IZQUIERDA";
char msg3[40]="ALERTA VENTANA DELANTERA DERECHA";
char msg4[40]="ALERTA VENTANA TRASERA IZQUIERDA";
char msg5[40]="ALERTA VENTANA TRASERA DERECHA";
char msg6[40]="LAS LUCES SE ENCUENTRA ENCENDIDAS";
String txt;
//String txt2;
byte state;
char number[15];
SMSGSM sms;
CallGSM call;
int st=0; //estado desarmado
int numdata;
boolean started=false;
char smsbuffer[160];
char n[20];

char sms_position;
char phone_number[20];
char sms_text[100];
int i;
String txt3;
int ron=2;//rele on off
int rab=5;
int rce=6;
int rpi=7;
int rve=8;
int rax=9;
int led=13;
```

```

int vdi=A0;//ventana delantera izq
int vdd=A1;
int vti=A2;
int vtd=A3;//ventana trasera derecha
int von=A4;
int lon=A5;

int cont=0;
int stlon=0;
char rx;
int r=0;
void setup()
{
  pinMode(von,INPUT);
  pinMode(lon,INPUT);
  pinMode(vdi,INPUT);
  pinMode(vdd,INPUT);
  pinMode(vti,INPUT);
  pinMode(vtd,INPUT);

  pinMode(led,OUTPUT);
  pinMode(ron,OUTPUT);
  pinMode(rab,OUTPUT);
  pinMode(rce,OUTPUT);
  pinMode(rpi,OUTPUT);
  pinMode(rve,OUTPUT);
  pinMode(rax,OUTPUT);

  digitalWrite(ron,LOW);
  digitalWrite(rab,LOW);
  digitalWrite(rce,LOW);
  digitalWrite(rpi,LOW);
  digitalWrite(rve,LOW);
  digitalWrite(rax,LOW);

  Serial.begin(9600);//bluet

  Serial.println("INICIO");

  if (gsm.begin(9600))
  {
    Serial.println("\nstatus=READY");
    started=true;
  }
  else
    Serial.println("\nstatus=IDLE");

  if(started)
  {int i;
    /*for(i=1;i<=15;i++)

```

```

    {
        sms.DeleteSMS(i);
    }*/
    //sendm1();//alarma desarmada
}
//ss.begin(9600);//GPS
}
void loop()
{
    //gpsst();
    //Serial.println("loop");
    if(started)
    {
        recunread();//LEER NO LEIDOS
    }
    if(r==0){//no hay robo
        if(digitalRead(von)==HIGH){//SI EL VEHICULO ESTA APAGADO CONTROLA
        SENSORES
            Serial.println("VEHICULO APAGADO");
            //el sensor normal LOW
            if(digitalRead(vdi)==HIGH){Serial.println("enviando sms2()");sms2();}//alerta ventana
            sms
            if(digitalRead(vdd)==HIGH){Serial.println("enviando sms3()");sms3();}//alerta ventana
            sms
            if(digitalRead(vti)==HIGH){Serial.println("enviando sms4()");sms4();}//alerta ventana
            sms
            if(digitalRead(vtd)==HIGH){Serial.println("enviando sms5()");sms5();}//alerta ventana
            sms
            if(digitalRead(lon)==LOW){if(stlon==0){stlon=1;Serial.println("enviando sms6()");
            sms6();}}//
        }//endif von
    else{
        stlon=0;
        }
        rx='z';
    while(Serial.available(>0){//LEE EL BLUETOOTH
        rx=Serial.read();

        if(rx=='A'){//abrir
            Serial.println("PUERTA ABIERTA");
            digitalWrite(rab,HIGH);delay(1000);digitalWrite(rab,LOW);
            }
        if(rx=='B'){//cerrar
            Serial.println("PUERTA CERRADA");
            digitalWrite(rce,HIGH);delay(1000);digitalWrite(rce,LOW);
            }
        if(rx=='C'){//bajar
            Serial.println("BAJAR VENTANA");
            digitalWrite(rve,HIGH);delay(3000);digitalWrite(rve,LOW);
            }
        }

```

```

} //whileserialread

if(rx=='L'){// HAY COMUNICACION
  digitalWrite(ron,HIGH);//activo el rele
  cont=0;
}else{//NO HAY COMUNICA BLUETOOTH
  cont++;//INCREMENTO EL CONT
  Serial.print("DESCONEXION:");Serial.println(cont);
  if(cont==30){//CONTROLO EL TIMPO
    digitalWrite(ron,LOW);//apago el rele
    digitalWrite(rce,HIGH);delay(1000);digitalWrite(rce,LOW);
  }
}

}else{//SI HAY ROBO
  digitalWrite(ron,LOW);
}

} //FINVOIDLOOP

void gpsst(){
  ss.begin(9600);// REINICIO EL GPS
  ss.listen();// FUNCION DE ATENCION
  bool newData = false;
  unsigned long chars;
  unsigned short sentences, failed;

  for (unsigned long start = millis(); millis() - start < 2000;)// ESPERA 2 SEGUNDOS Y
  LEE EL GPS
  {
    while (ss.available())// MIENTRAS HAYA DATOS DEL GPS
    {
      char c = ss.read(); //LEA LOS DATOS DEL GPS
      // Serial.write(c); // uncomment this line if you want to see the GPS data flowing
      if (gps.encode(c)) // BUSCA EL INICIO DE LA TRAMA QUE ENTREGA EL GPS
        newData = true;// SI ENCONTRO EL INICIO DE LA TRAMA CAMBIE A TRUE
    }
  }
  EL ESTADO DE LA VARIABLE NEWDATA

  if (newData)// SI HAY INICIO DE LA TRAMA
  {
    float flat, flon;
    unsigned long age;
    gps.f_get_position(&flat, &flon, &age); //LEA LAS VARIABLES LATITUD
    LONGITUD

    //Serial.print("LAT=");
    //Serial.print(flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6);
    //Serial.print(" LON=");

```



```

//Serial.print(flon == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6);
//Serial.print(" SAT=");
//Serial.print(gps.satellites() == TinyGPS::GPS_INVALID_SATELLITES ? 0 :
gps.satellites());
//Serial.print(" PREC=");
// Serial.print(gps.hdop() == TinyGPS::GPS_INVALID_HDOP ? 0 : gps.hdop());
char cadena[50]="http://maps.google.com/?q
char lat [15];
char lon [15];
dtostrf(lat,3,6,lat);//TRANSFORMA DE FLOAT A CHARACTER
dtostrf(lon,3,6,lon);

char buf2 [10];//lat
int t=analogRead(A1)/2;
sprintf (buf2, "%s", lat);
strcat(cadena,buf2);
sprintf (buf2, "%s", lon);
strcat(cadena,buf2);
//sprintf (buf2, "T%d", t);
//strcat(cadena,buf2);

Serial.println(cadena);
for (int x=0;x<50;x++){
msg1[x]=cadena[x];
}
}
Serial.println(msg1);
gps.stats(&chars, &sentences, &failed);

if (chars == 0)
Serial.println("***No characters from GPS***");

} //FIN GPSST

void compara() { // COMPARA EL TEXTO RECIBIDO POR SMS
Serial.println("comparando");
Serial.print("txt:");
Serial.println(txt);
if(txt.substring(0)=="OBTENER800"){ // EL TEXTO RECIBIDO ES "OBTENER800"
st=1;
gpsst();//OBTIENE LA POSICION DEL GPS
gsm.begin(9600);
digitalWrite(led, HIGH);
sendm1();//ENVIA EL MENSAJE ESCRITO
digitalWrite(led, LOW);
}
if(txt.substring(0)=="PITO800"){
digitalWrite(rpi, HIGH);//RELE PITO
delay(5000);
}
}

```

```

    digitalWrite(rpi, LOW);
  }
  if(txt.substring(0)=="ABRIR800"){
    digitalWrite(rab, HIGH);//RELE ABRIR SEGUROS
    delay(2000);
    digitalWrite(rab, LOW);
  }
  if(txt.substring(0)=="ROBO800"){
    r=1; //CAMBIO A ESTADO 1= EXISTE UN ROBO O PERDIDA
    digitalWrite(ron, LOW);//RELE ENCENDIDO DE VEHICULO
  }
  if(txt.substring(0)=="RESTABLECE800"){
    r=0; //RESTABLE LA VARIABLE A 0 FUNCIONAMIENTO NORMAL
  }
} //FIN COMPARA

void recunread(){
  txt="";

  Serial.println("recunread");
  sms_position=sms.IsSMSPresent(SMS_UNREAD);//LEA EL BUZON DE MENSAJE
  NUEVOS Y DEVUEVA LA PISCION DEL MISMO SI ES 0 NO HAY MENSAJES
  NUEVOS
  if (sms_position) //SI ES DIFERENTE DE 0 LEA EL SMS
  {
    Serial.print("SMS position:");
    Serial.println(sms_position,DEC);
    sms.GetSMS(sms_position, phone_number, sms_text, 100); //LEE EL SMS Y
  DEVUELVE POSICION, NUMERO Y CONTENIDO DEL MENSAJE
    Serial.println(phone_number);
    int x;

    txt="";
    for(x=0;x<20;x++){
      txt=txt+sms_text[x]; //GUARDO EL CONTENIDO DEL MENSAJE EN LA VARIABLE
  TXT, CAACTER POR CARACTER
    }
    txt=String(sms_text);
    txt.trim(); //BORRA ESPACIOS

    Serial.println(sms_text);
    Serial.println(txt);

    compara(); //FUNCION COMPARA EL CONTENIDO DEL SMS
  }
  delay(2000);
} //FIN RECUNREAD

void sendm1(){

```

```

gsm.begin(9600);
Serial.println("ENVIANDO");
delay(1000);
if (sms.SendSMS(num1, msg1))//ENVIE UN SMS AL NUMERO1 CON EL CONTENIDO
DE LA VARIABLE MSG1
{
  Serial.println(msg1);Serial.println("ENVIADO***");
  }else{
  //Serial.println("\nError sending SMS.");
}
}

void sms2(){
  digitalWrite(led, HIGH);
if (sms.SendSMS(num1, msg2))//
{Serial.println(msg2);}

//if (sms.SendSMS(num2, msg2))//
//{Serial.println(msg2);}
digitalWrite(led, LOW);

}

void sms3(){
if (sms.SendSMS(num1, msg3))//
{Serial.println(msg3);}
}

void sms4(){
if (sms.SendSMS(num1, msg4))//
{Serial.println(msg4);}
}

void sms5(){
if (sms.SendSMS(num1, msg5))//
{Serial.println(msg5);}
}

void sms6(){
if (sms.SendSMS(num1, msg6))//
{Serial.println(msg6);}
}

```