

Universidad Acción Pro-Educación y Cultura
(UNAPEC)



Decanato de Ingeniería e Informática
Escuela de Ingeniería

Tesis de Grado para Optar por el Título de:
Ingeniero Electrónico, Mención Comunicaciones.

**“PROPUESTA DE DISEÑO DE UN SISTEMA DE ALARMA
INTELIGENTE PARA PREVENIR ROBOS DE VEHICULOS
UTILIZANDO EL SISTEMA GLOBAL DE LAS
COMUNICACIONES MÓVILES Y GEOLOCALIZACIÓN EN LA
REPUBLICA DOMINICANA
(2018)”**

Sustentantes:

Robert Antonio Pérez Mata	2013-0794
Luis Manuel Soto Pujols	2011-0581

Asesor:

Ing. Luis Pérez Méndez

*“Los conceptos expuestos en esta
investigación son de exclusiva
responsabilidad de sus autores”.*

Distrito Nacional
República Dominicana
Marzo 2018.

RESUMEN

Existe una gran variedad de marcas y modelos de vehículos que transitan por las calles de República Dominicana, tomando en cuenta que, estos en algún momento determinado, serán estacionados en zonas públicas o privadas de este país; es primordial la protección de estas inversiones por parte de los propietarios. Estos automóviles traen instalado de fábrica un sistema de alarma antirrobo muy convencional, cuya simplicidad hace que no le entorpezca el trabajo a los delincuentes que se ganan la vida despojando a los ciudadanos de sus vehículos. Este trabajo de grado presenta un conjunto de información, donde se evidencia datos estadísticos porcentuales de los robos de automóviles que ocurren en las calles de la República Dominicana, incluyendo el bajo porcentaje de recuperación de los mismos. El objetivo es presentar una propuesta de diseño con una gran variedad de mejoras enfocadas a los sistemas de alarmas convencionales que vienen pre instalados en los vehículos comercializados en la República Dominicana, buscando que con la implementación de nuestra propuesta de diseño, se beneficien los ciudadanos propietarios de vehículos sintiéndose menos inseguros a la hora de estacionarse en cualquier sector de R.D, a la vez ayudando al estado, bajando la tasa de robos de automóviles y mejorar los porcentajes de recuperación de estos activos. Los resultados presentados fueron logrados gracias a las investigaciones que se realizaron, durante las cuales fueron utilizados diferentes medios para obtener informaciones tales como: páginas web, libros, foros especializados en electrónica, base datos, artículos científicos y publicaciones de tesis de universidades extranjeras relacionadas al tema. Con la información recopilada determinamos los componentes más viables que puedan lograr el objetivo planteado de la forma más eficiente y al menor costo posible que se ajuste a las necesidades del mercado nacional.

DEDICATORIAS

Luis Manuel Soto Pujols

*El siguiente trabajo de grado se lo dedico a mi bella madre **Marilyn Pujols Castillo**, le agradezco a Dios por tenerte como mi madre y para mi eres la mejor madre del mundo, siempre estás presente en mi corazón sin importar la distancia que haya entre nosotros, brindándome tus mejores consejos como madre, tanto en los momentos buenos como en los malos, buscando la manera en que me sienta seguro a la hora de tomar algunas decisiones importantes en mi vida. Te agradezco por pasarme ese gran corazón que tienes y el carisma de cómo tratar con las personas que te rodean gracias. Sé que te he decepcionado en un sin número de ocasiones, dejándome llevar de la ambición y tomando decisiones que en algún momento de mi vida lamentaría, pero, aun así, sentía tu apoyo me hacías entender que en el mundo todo llega a su debido momento, que no me desesperara y que mi momento llegaría. Te amo con todo mi corazón y aquí esta una de las metas cumplidas Dedicated to you.*

*Este trabajo de grado es dedicado a mi padre **Luis Manuel Soto Mejía**, el mejor padre que un hijo puede tener, me has enseñado mucho, principalmente en como un hombre debe comportarse en cualquier situación que se le presente en la vida, eres el padre que muchos desearían tener y le agradezco a Dios por tenerte. Puedo decir de forma abierta que tomaste una de las mejores decisiones que marcaron mi vida y fue sacarme de San José de Ocoa e inscribirme en el Instituto Politécnico Loyola, buscando una mejor preparación educativa para mí. Debo agradecerte muchas cosas, pero las más importante son; que con las decisiones que tomaste para mi formación académica, tus buenos consejos como padre y tu mano dura, lograron formar a un hombre de bien, de buen corazón y eso te lo agradeceré por toda la vida. Para mi eres un ejemplo a seguir, sin importar las malas decisiones que hayas tomando y siempre comprenderé, ya que, me lo repetías muchas veces, que las oportunidades siempre les llegan a las personas que están preparados. Te amo mucho padre y este trabajo va dedicado a usted todólogo.*

Robert Antonio Pérez Mata

*Quiero dedicar este gran logro a todos mis familiares, de manera especial, a mis padres: **Roberto Pérez de la Rosa** y **Maribel Mata de Pérez**, por apoyarme durante todo mi trayecto como estudiante de preparatoria y, por supuesto, en mi carrera como universitario. Gracias por todos los sacrificios, los desvelos y los días extras de trabajo, cuyo propósito fundamental es y seguirá siendo darnos lo mejor de lo mejor, no solamente a mí, sino también a mis hermanas. Estoy infinitamente agradecido con ustedes por siempre mantenerme con actitud positiva ante todos los desafíos de la vida y metas que me proponía cumplir. Ahora me toca demostrar que todos los sacrificios por parte de ustedes en realidad valieron la pena. LOS AMO.*

*A mis abuelos **Roberto Mata Vargas** y **Clara Cruz de Mata**, por siempre mantenerme motivado con sus buenos y valiosos consejos. Gracias por siempre compartir conmigo las lecturas bíblicas y libros de texto, compartidos en mi hogar mediante sus visitas. Les agradezco por todos aquellos detalles que siempre tienen presente para mí, y aunque estos parezcan pequeños, me llenan de mucha alegría. Finalmente, gracias por ser parte de mi vida. Este gran logro es también dedicado a ustedes.*

*A mis hermanas **Paula Rosmary Perez** y **Clara Wilmary Perez**, por estar siempre ahí apoyándome en todo momento. Lucharé siempre por darles lo mejor.*

AGRADECIMIENTOS

Luis Manuel Soto Pujols

Primeramente, Le agradezco a Dios por darme la salud y la fortaleza para lograr unas de mis metas que es la entrega de este trabajo de grado. Fueron muchas oraciones realizadas pidiéndole a Dios que todo saliera bien y que nos ayudara tanto a mí, como a mi compañero de tesis Robert Pérez poder elaborar este trabajo de grado.

Le agradezco a mi primo Henry Gómez, Gracias por ayudarme en la elaboración de este trabajo de grado y brindarme tu tiempo sabiendo que podías priorizarlo en otras cosas. Te puede decir que quedo en deuda contigo y por siempre agradecido.

Le agradezco a mi madre: Marilyn castillo, a mi padre: Luis Soto, a mis tíos/as: Francis Soto, Elizabeth Soto, Niove Soto, Virginia Soto, Deisy Soto, Nelson Soto y Jorge Soto. A mis primas: Denise Matos, Yadira Matos, Anny Matos y Nelsy Soto. A mis primos: Santiago Brito, Eddy Gómez y Otto Gómez, mi hermana: Margerie Soto, a mi madrastra: Isailis Pujols y finalmente a mi querida abuela Lidia Soto, se les quiere mucho, gracias por su apoyo y por siempre agradecido.

Le agradezco a mi novia Pamela Tavares Sosa, por brindarme todo su apoyo en el desarrollo de este trabajo de grado, desarrollaste un papel importante, te amo mucho y por siempre agradecido. Le doy las gracias a Dios por darme una segunda familia a través de ti que está formado por: mis suegra:s Leyda Sosa, Mercedes Sosa, La cuña: Paola Tavares, tus tíos: Barcilio Ruiz, Héctor Sosa y a tus primos que se les quiere como si fueran hermanos: Junior Ruiz y Rosemary Ruiz. Gracias por aceptarme como si fuera parte de su familia y por su apoyo.

Robert Antonio Pérez Mata

Quiero agradecer primero a Dios por brindarme las fuerzas de poder llevar a cabo el desarrollo de este trabajo de grado junto a mi compañero, Luis Manuel Soto. También, por haber hecho posible la finalización de mi carrera universitaria, la cual era una de las tantas metas que me proponía cumplir.

*Le agradezco a mi asesor de tesis, el **Ing. Luis Pérez Méndez**, por habernos brindado su apoyo en todo el transcurso de la elaboración de este trabajo de grado.*

*Al profesor y decano, el **Ing. Emín Rivera**, por guiarnos por el buen camino y por su gran contribución en la formalización de nuestra idea de proyecto. Agradezco también por su disposición de siempre ayudarnos. Gracias por todos los consejos y enseñanzas impartidos a lo largo de cada una de las materias cursadas con usted.*

*A mi gran amigo **Joan Heiliguer** (el alemán), porque gracias a su experiencia de programación, de forma desinteresada nos brindó su apoyo para hacer posible la demostración del funcionamiento de nuestro proyecto. Gracias por ayudarnos a hacer que este proyecto fuera más que simples palabras en un papel.*

*A la **Ing. Tracey Pérez Paulino**, por siempre estar dispuesta a darme una mano en todo lo que necesité. Por siempre estar atenta a las fechas importantes de entrega para que no se me pasara ninguna. Gracias por toda tu ayuda.*

*Por último, agradezco a tod@s mis amig@s y colegas: **Rolando Mata, Isaías Gómez, Iván Gerónimo, Michelle Fernández, Natividad Ortíz, Wascar García, Francisco Hernández, Raymer Feliz, Miguel Medina, Andrickson Vicente, Omielant M., Karla Pérez** y a todos los demás, que de alguna u otra manera aportaron en el desarrollo de mi carrera.*

TABLA DE CONTENIDO

RESUMEN	i
DEDICATORIAS.....	ii
AGRADECIMIENTOS	iv
LISTA DE TABLAS.....	12
LISTA DE FIGURAS	13
INTRODUCCIÓN	16
1. INTRODUCCIÓN A LOS SISTEMAS DE ALARMAS VEHICULARES. FUNCIONAMIENTO E IMPORTANCIA SOBRE LA IMPLEMENTACIÓN DEL USO DE LAS ALARMAS PARA AUTOMÓVILES.	
1.1 Referencias sobre las cantidades de ingresos y robos de vehículos en la República Dominicana para el año 2017.....	18
1.1.1 Datos estadísticos acerca de la cantidad de registro y robos de vehículos en la República Dominicana según la Oficina Nacional de Estadística (ONE) y la Policía Nacional (P.N.) para el año 2017.....	18
1.1.2 Provincias de la República Dominicana donde son más populares los robos de vehículos de motor de cuatro ruedas.....	20
1.1.3 Modalidades de protección contra robos de vehículos	22
1.1.4 Bastón:	22
1.1.5 Tranca Palancas:.....	22
1.1.6 Bloqueador del volante-pedal:	22
1.1.7 Bloqueador de pedales:	23
1.1.8 Inmovilizador Electrónico:.....	23
1.1.8 Inmovilizador por Comandos Remotos Infrarrojos:	23
1.1.9 Inmovilizador con Teclado Numérico:	23
1.1.10 Inmovilizador con Llave Transpondedor:	24
1.2 Los sistemas de alarmas contra robo de vehículos.....	24
1.3 Invención y evolución de los sistemas de alarma contra robos de vehículos .	25
1.4 Partes Complementarias de los Sistemas de Alarma de vehículos.	26
1.4.1 Módulo central.....	27
1.4.2 Control transmisor.....	27
1.4.3 Armado.....	27
1.4.4 Desarmado	28
1.4.5 Armado/Desarmado Silencioso	28
1.4.6 Apertura de baúl o cajuela.....	28
1.4.7 Luz indicadora.....	28

1.4.8 Sensor de golpe	28
1.4.9 Interruptor de valet.....	29
1.5 Funcionamiento de los sistemas de alarma.....	29
1.5.1 Alimentación, activación y sensores de puerta.	29
1.6 Introducción a las tecnologías inalámbricas.....	30
1.6.1 Conceptos básicos sobre redes inalámbricas.....	30
1.6.2 Clasificación de las redes inalámbricas.....	31
1.6.3 Extensiones de Estándares Inalámbricos como el 802.11 son:	31
1.6.3 Breve Historia del GPS	32
1.6.3 Conceptos básicos del GPS.....	33
1.6.4 Funcionamiento de la tecnología del GPS	34
1.6.5 Fuentes de errores en los sistemas GPS	35
1.7 Sistema global de las comunicaciones móviles, GSM	37
1.7.1 Breve historia sobre el GSM.....	37
1.7.2 Operatividad del GSM	39
1.7.3 Características de la comunicación mediante tecnología GSM	40
1.7.4 Funciones Básicas del NSS.....	42
1.7.5 Banda de frecuencia GSM	44
1.7.6 Tarjeta SIM (Modulo de identificación de suscripción).	45
1.7.7 Mensajería de texto en Redes GSM.	45
1.7.8 Centro de Servicios de Mensajes de texto cortos (SMS-C)	46
1.8 Sistema general de paquetes de datos, GPRS.....	47
1.8.1 Mejora del servicio GSM (generación 2.0 a 2.5).....	47
1.8.2 Conceptos básicos sobre el GPRS.....	48
1.8.3 Arquitectura del sistema GPRS.....	48
1.9 Tecnología Bluetooth.	49
1.9.1 Breve historia sobre el Bluetooth.....	49
1.9.2 Utilidad del sistema Bluetooth	50
1.9.3 Tipos de enlace Bluetooth.....	51
1.9.4 Versiones de Bluetooth	51
1.9.5 Clases de Bluetooth.....	52
1.9.6 Modos de Comunicación del dispositivo Bluetooth	54
1.9.7 Seguridad en el sistema Bluetooth.....	54
1.9.8 Modos de seguridad básicos de Bluetooth	56
2. DISEÑO DE SISTEMA DE ALARMA INTELIGENTE FUNDAMENTADO EN RADIOFRECUENCIA (SAIRF)	58

2.1 Diagramas Generales del Sistema de Alarma Inteligente antirrobo de vehículos.	58
2.1.1 Hardware	58
2.1.2 Software	60
2.2 Hardware seleccionado para el diseño del sistema antirrobo de vehículos. .	61
2.2.1 Microcontrolador ATMEGA	61
2.2.2 Arduino UNO.	62
Tabla 3: Características generales del Arduino UNO	64
2.2.3 Módulo de comunicación GSM y GPS	64
2.2.4 Módulo SIM808	64
2.2.5 Módulo de Bluetooth HC-06.	68
2.2.5.1 Conectores del módulo Bluetooth HC-06.	69
2.2.6 Sensor de golpe AUDIOVOX AS-9492	70
2.2.7 Batería de litio	72
2.3 Tecnología de comunicación interna para el sistema antirrobo de vehículos fundamentado en radio frecuencia (SAIRF).	73
2.3.1 Protocolo de comunicación UART	73
2.3.2 Comandos AT	74
2.4 Descripción del funcionamiento del sistema de alarma antirrobo de vehículos.	76
2.4.1 Representación del funcionamiento del sistema de alarma antirrobo de vehículos. .	76
2.4.2 Representación rutinas de operación entre el control de mando y el Módulo de Bluetooth HC-06.	77
2.4.3 Representación pictórica de las conexiones del prototipo del sistema SAIRF. .	78
2.5 Programas fundamentales para el funcionamiento del SAIRF.	81
2.5.1 Códigos para la fase de accesibilidad y control.	81
2.5.2 Códigos para la fase de asistencia GSM-GPRS.	83
2.5.3 Realización de llamada telefónica.	83
2.5.4 Lectura de mensaje y envío de coordenadas.	84
3. CONTRASTE Y VERIFICACION DEL DISEÑO.	87
3.1 Resultados	87
3.1.1 Alimentación del sistema para pruebas de funcionamiento.	87
3.1.2 Prueba funcional del sistema.	88
3.2 Aplicación móvil.	89
3.2.1 Diseño de la interfaz APK.	89
3.2.2 Diseño interno de la aplicación APK.	91

3.3 Recepción de ubicación geográfica.....	92
3.4 Factibilidad de la propuesta de diseño	94
CONCLUSIONES.....	96
RECOMENDACIONES.....	97
REFERENCIAS BIBLIOGRAFICAS.....	98
GLOSARIO.....	108
ANEXOS.....	109
APÉNDICE A: Programas del sistema.....	109
A1. Accesibilidad y control.....	109
A2. Assistance GPS-GPRS	111
APÉNDICE B: Datos estadísticos.....	116
B1. Datos estadísticos de la Oficina Nacional de Estadísticas (ONE).....	116
B2. Datos estadísticos de la Policía Nacional Dominicana (PN).....	116
APÉNDICE C: Presupuesto del SAIRF	118
C1: Costos de dispositivos, materiales e instalación para elaboración de prototipo del sistema de alarma contra robos de vehículos.	118
C2: Cotización de planes para vehículo ofrecido por el Banco BHD y sus deducibles. ...	118
C3: Cotizaciones de los planes ofrecidos por el banco BHD para un vehículo Toyota corolla del año 2015.....	119
APÉNDICE D: Contenido del CD.....	120

LISTA DE TABLAS

Tabla 1: Rango de tipos de Bluetooth.....	53
Tabla 2: Características principales del microcontrolador ATMEGA. Extraído de ATmega328/P: Data Sheet Complete ATMEL. (2016).....	62
Tabla 3: Características generales del Arduino UNO	64
Tabla 4: Características de hardware del módulo SIM808. Extraída de: Diseño de un sistema electrónico para localizar personas con Alzheimer. Ortiz N., Vicente A. y Muñoz O. (2016). República Dominicana.....	65
Tabla 5: Características técnicas del chip SIM80. Extraída de: Diseño de un sistema electrónico para localizar personas con Alzheimer. Ortiz N., Vicente A. y Muñoz O. (2016). República Dominicana.....	67
Tabla 6: Características técnicas del módulo Bluetooth HC-06. Extraída de Módulo Bluetooth HC-06 Serial Rs232 (TTL) Electronilab (2018).....	68
Tabla 7: Características fundamentales del sensor de golpe AS-9492.....	71
Tabla 8: Comandos AT utilizados para establecer comunicación con el SIM 808. Obtenido del manual: Instructivo de comandos AT.....	75
Tabla 9. Cantidad de vehículos registrados por mes. Obtenido de: Oficina Nacional de Estadísticas. (2018).....	116
Tabla 10: Cantidad de robo de vehículos. Primer semestre 2017. Obtenido de: Policía Nacional. (2018).....	116
Tabla 11. Cantidad de robo de vehículos. Primer semestre 2017. Obtenido de: Policía Nacional. (2018).....	117
Tabla 12: costo de los materiales utilizados para la elaboración de la propuesta.....	118
Tabla 13: Cotización de planes para vehículo Toyota Corolla del año 2015.....	118

LISTA DE FIGURAS

Figura 1: Comparación de las cantidades de robos de vehículos durante el primer y el segundo semestre del 2017 en República Dominicana. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.	19
Figura 2: Representación de los tipos de vehículos que presentan una mayor probabilidad de robos. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.	20
Figura 3: Cantidades de robos de vehículos en las provincias de República Dominicana más afectadas en el año 2017. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.	21
Figura 4: Cantidades en porcentaje de robos de vehículos en las provincias de República Dominicana más afectadas en el año 2017. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.	21
Figura 5: Bandas de Frecuencia GSM. Extraídas de Communication Systems for the Mobile Information Society (Martin Sauter, 2006).	44
Figura 6: Representación de las conexiones existentes entre el módulo procesador de datos, módulos y sensores del SAIRF. Herramienta de diseño: Lucidchart.	59
Figura 7: Representación de la estructura comunicacional entre el control de mando y el SAIRF. Herramienta de diseño: Lucidchart.	59
Figura 8: Representación de la estructura interna del módulo procesador de datos del SAIRF. Herramienta de diseño: Lucidchart.	60
Figura 9: Estructura interna del Control de mando del SAIRF. Herramienta de diseño: Lucidchart.	60
Figura 10: Apariencia física del microcontrolador ATMEGA328P. Extraída de ATmega328P: Data Sheet Complete ATMEL. (2016).	61
Figura 11: Parte superior (izquierda) e inferior (derecha) de la placa Arduino UNO con el microcontrolador ATMEGA como cerebro de la plataforma.	62

Figura 12: Descripción de entradas, salidas y componentes del Arduino UNO. Extraída de Arduino. Pinterest. Lasuvas, Q. (2018).....	63
Figura 13: Parte superior del módulo SIM808, GPS-GSM, con sus respectivas antenas.....	65
Figura 14: Parte inferior del módulo808 con tarjeta SIM instalada.....	66
Figura 15: Chip SIM808. Extraída de: SIMCOM. GSM/GPRS+GPS Module.....	67
Figura 16: Vista frontal (izquierda) y vista trasera (derecha) del módulo de Bluetooth HC-06.	69
Figura 17: Ilustración del sensor de golpe AUDIOVOX, AS-9492. Plástico protector (izquierda) y estructura interna (derecha).	71
Figura 18: Batería de Ion de litio.	73
Figura 19: Conexión entre dos dispositivos UART extraída de Geeky Theory (2017).....	74
Figura 20: Representación del funcionamiento del sistema de alarma en general mediante un diagrama de flujo. Herramienta de diseño: Lucidchart.	76
Figura 21: Representación del funcionamiento entre el control de mando y el módulo de Bluetooth para el acceso, a través de una aplicación APK para teléfonos inteligentes. Herramienta de diseño: Lucidchart.	77
Figura 22. Diagrama pictórico sobre la fase de accesibilidad y control. Imágenes de los dispositivos obtenidas de google.com.do. Herramienta de diseño: Paint	78
Figura 23. Representación pictórica de la etapa de asistencia GPS-GPRS. Imágenes de los dispositivos obtenidas de google.com.do. Herramienta de diseño: Paint.	80
Figura 24. Conexiones correspondientes para la comunicación con la fase de accesibilidad y control del SAIRF.	88
Figura 25. Conexiones correspondientes para la comunicación con la fase de asistencia GPS-GPRS.....	88
Figura 26. Conexión completa del SAIRF.....	89
Figura 27. Ilustración de la interfaz de la aplicación para teléfonos inteligentes.	90
Figura 28. Apariencia del ícono de la aplicación instalada en un teléfono inteligente.	90
Figura 29. Representación del diseño interno de la aplicación.	91
Figura 30. Ubicación en el mapa de google de las coordenadas enviadas por el sistema.	93

Figura 31. Datos obtenidos en el monitor serial del software Arduino.....	93
Figura 32: Cotización de los Planes ofrecidos por el banco BHD.....	119

INTRODUCCIÓN

En los últimos años, el espacio público en este país ha presenciado un aumento destacable en el tránsito de vehículos, siendo evidente que las necesidades de sus propietarios van a la vanguardia con los últimos modelos de distintos fabricantes. Sin embargo, a pesar de que se adhieren a un paradigma de modernidad, estos vehículos vienen preinstalados con sistemas de seguridad antirrobo convencionales que suplen las necesidades básicas de advertencia, dejando muchos aspectos insatisfechos.

La realidad en la que nos vemos sumergidos en este país es de inseguridad. Diariamente la tasa de crímenes ha aumentado con reportes en diferentes sectores de atracos y hurta de vehículos, datos estadísticos que presentaremos en este trabajo. Esto hace imperante la protección de nuestras inversiones y al enfocarse en los automóviles que transitan en nuestras calles, es necesario un sistema avanzado contra el robo de automóviles.

Para proteger la integridad de las inversiones de los dominicanos en materia de transporte, hay que emplear diferentes mecanismos y métodos, que al complementarse de forma holística brindara seguridad y satisfacción a los sujetos beneficiarios de este proyecto, porque hay que tomar en cuenta que la tecnología posee un aspecto ambivalente, más cuando se refiere a aspectos de criminalidad; por lo que se considera que sin importar lo avanzado que sea un sistema de seguridad establecido, aquellos que ilegalmente quieran sacar provecho, encontrarán la forma de hacerlo vulnerable. Es por esta razón que decidimos abordar diferentes tecnologías y métodos para proveer protección utilizando radiofrecuencia y geolocalización (GSM, GPRS, Bluetooth y GPS), que en conjunto dificultara las acciones delictivas y mermar la tasa de robo de vehículos y aumentar la tasa de recuperación de los mismos en la República Dominicana.

Para dilucidar los elementos que necesitaríamos para lograr el objetivo de elaborar un sistema de alarma inteligente antirrobo de vehículos, nos planteamos organizar las informaciones referentes al caso de manera estructurada, yendo de lo más simple a lo más complejo y dividiendo el problema en sus constituyentes más básicos. De esta forma abordamos el problema según sus particularidades y finalmente como un todo; tomando en cuenta que los componentes físicos deben regirse por su funcionabilidad, sean adaptables o flexibles, permitiendo que los mismos puedan ser constantemente actualizados y mejorados y finalmente que sean una opción de bajo costo y fácil de implementar.

En el cuerpo de este trabajo, los capítulos fueron divididos según las tecnologías que consideramos emplear en la propuesta de diseño. Plasmamos todos los datos relevantes de los diferentes componentes a utilizar, para conocer a plenitud su funcionamiento y sus debilidades, así poder complementarlos con las fortalezas de otras tecnologías, como sería el caso del aspecto de comunicación a través de módulos Bluetooth y GSM/GPRS. Luego se puso en marcha la evaluación entre la sinergia de los diferentes módulos incluyendo el GPS, que nos ofrecerá datos de geolocalización que permita al usuario la ubicación de su vehículo constantemente. Finalmente diseñamos diagramas de flujo que nos guíen a obtener una idea, para desarrollar la programación del controlador (Arduino) que pondrá en funcionamiento y procesara la información de los diferentes componentes.

1. INTRODUCCIÓN A LOS SISTEMAS DE ALARMAS VEHICULARES. FUNCIONAMIENTO E IMPORTANCIA SOBRE LA IMPLEMENTACIÓN DEL USO DE LAS ALARMAS PARA AUTOMÓVILES.

1.1 Referencias sobre las cantidades de ingresos y robos de vehículos en la República Dominicana para el año 2017.

1.1.1 Datos estadísticos acerca de la cantidad de registro y robos de vehículos en la República Dominicana según la Oficina Nacional de Estadística (ONE) y la Policía Nacional (P.N.) para el año 2017.

Con mucha frecuencia en la República Dominicana, al igual que en muchas otras partes del mundo, ocurren un sin número de hurtos de diversos tipos de propiedades, lo cual hace que la seguridad de dichos bienes sea cada vez más exigente para así disminuir o evitar de forma definitiva este tipo de incidentes. Uno de los casos más destacados en este país es el robo de vehículos de motor o automóviles.

Es importante destacar que a medida en que la adquisición de vehículos siga aumentando, las cantidades de robo de los mismos también seguirán yendo en ascenso. Según la Dirección General de Impuestos Internos (DGII), para finales del año 2016 el parque vehicular sumó unas 3,854,038 unidades, creciendo un 6.7% equivalente a unas 241,074 unidades con relación al año 2015, informa un anuncio del periódico HOY, publicado el 10 de febrero del 2017 [1].

Según la Oficina Nacional de Estadística (ONE), de enero a noviembre del año 2017, en la República Dominicana se registró una cantidad alrededor de 165,446 vehículos de motor de cuatro ruedas que ingresaron al país, entre ellos un 23.57% automóviles, el 51.98% autobuses y 15.43% para los jeeps o yipetas [2].

Para el mismo año 2017, la Policía Nacional de la República Dominicana (P.N) registró 573 robos de vehículos de distintos tipos alrededor de todo el territorio dominicano. Entre estos se encuentran 389 robos de carros, equivalente a un 67.88%, 95 robos de camionetas, con un 16.57%, 61 robos yipetas (10.64%), 25 robos de camiones (4.3%) y 3 robos de minibuses (0.52%). La figura 2 representa estas cifras en un gráfico en un orden de menor a mayor [3].

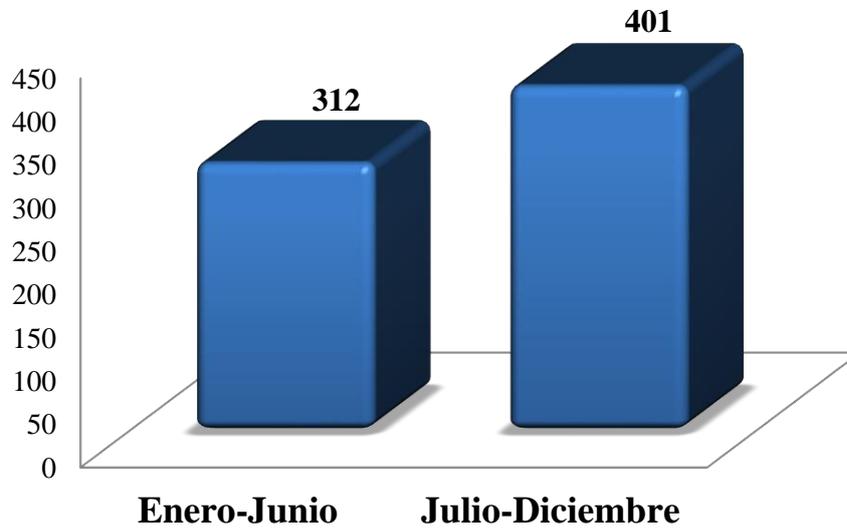


Figura 1: Comparación de las cantidades de robos de vehículos durante el primer y el segundo semestre del 2017 en República Dominicana. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.

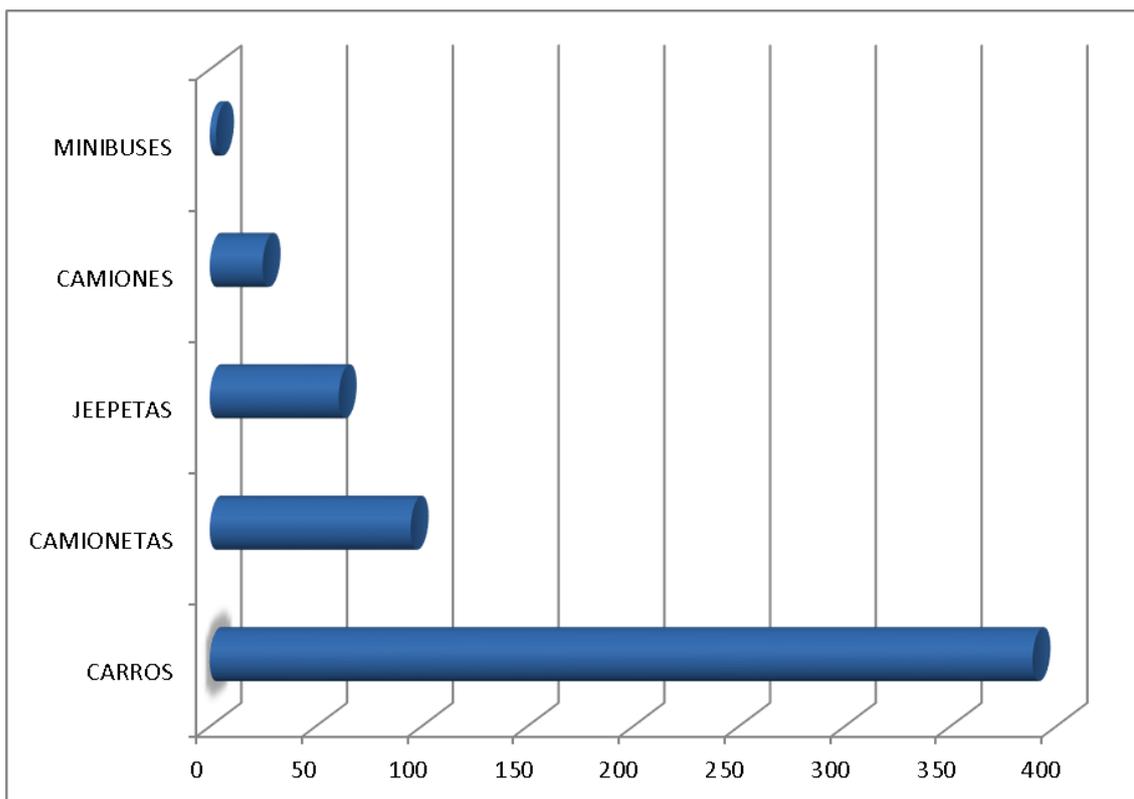


Figura 2: Representación de los tipos de vehículos que presentan una mayor probabilidad de robos. Obtenido de: Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.

1.1.2 Provincias de la República Dominicana donde son más populares los robos de vehículos de motor de cuatro ruedas.

Los robos de vehículos son muy populares en toda la República Dominicana, aunque en algunos lugares estos sean más populares que en otros. En el 2017, lugares como la Vega, Santiago, San Cristóbal, Puerto Plata, el Distrito Nacional y el gran Santo Domingo, fueron los más populares en cuanto a hurtos de autos nos referimos [4]. La provincia más afectada de las anteriormente mencionadas fue Santo Domingo con 244 robos, cuyo promedio sería de un 34.22% de robos. Luego le siguió el Distrito Nacional con algunos 135, con promedio de 18.93%. En este mismo orden le siguieron Santiago con 109, con un 15.28%, San Cristóbal con 33 robos de vehículos, con un 4.6%, La Vega con 109, con un 15.28%, San Cristóbal con 33 robos de vehículos, con un 4.6%, La Vega con 30, con un 4.2% y Puerto Plata con 19 robos, equivalente a un 2.66 % [5].

Representación de robos por provincias en el año 2017, República Dominicana.

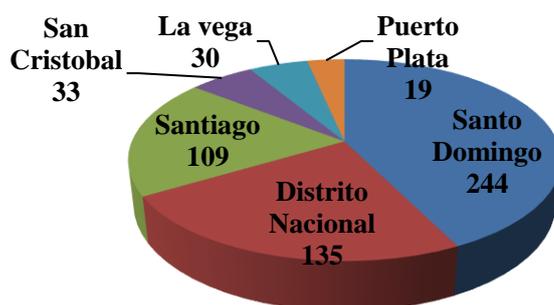


Figura 3: Cantidades de robos de vehículos en las provincias de República Dominicana más afectadas en el año 2017. Obtenido de: *Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.*

Representación en porcentajes de robos de vehículos por provincias en el año 2017, República Dominicana.

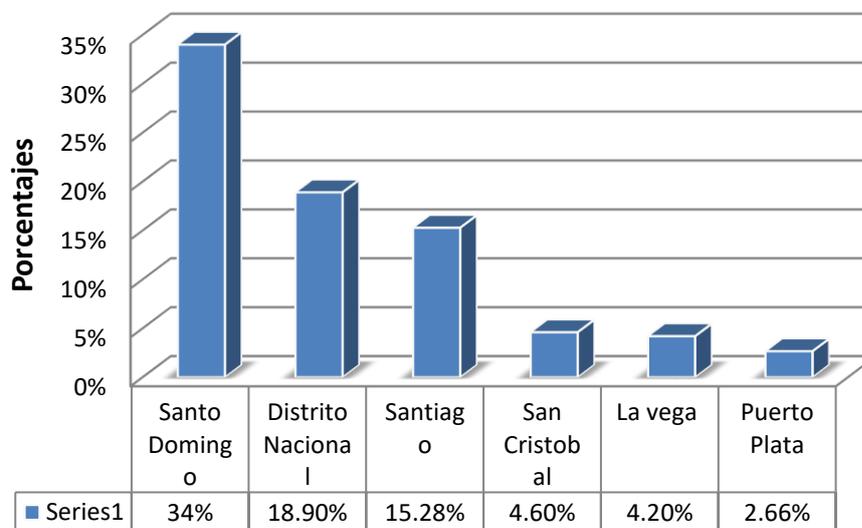


Figura 4: Cantidades en porcentaje de robos de vehículos en las provincias de República Dominicana más afectadas en el año 2017. Obtenido de: *Departamento de Información y Estadísticas. (2017). Vehículos Robados Por Provincias 2017. Policía Nacional.*

1.1.3 Modalidades de protección contra robos de vehículos

Las necesidades que de forma frecuente se les presentan a los individuos son las que hacen posible los cambios novedosos que asiduamente se ven en todas partes del mundo. Siempre que alguien adquiera algún producto tecnológico, novedoso y considerado de valor, existirán personas que estarán interesadas profundamente en adueñarse de aquello que les pertenece a otros. Es por esto que, para el caso de los vehículos de motor existen un sinnúmero de modalidades de protección antirrobo, para evitar así la pérdida parcial o total de sus propiedades. Estos métodos serán descritos a continuación, desde el más básico, hasta el más complejo actualmente utilizado.

1.1.4 Bastón:

Esta es una de las modalidades más comunes y de bajo costo. Este artefacto generalmente está elaborado a base de metal y posee una especie de cerradura en la parte superior, lo cual permite que se pueda sujetar el guía en una posición fija para que una vez activado el bastón, el timón no pueda moverse [6].

1.1.5 Tranca Palancas:

Como su nombre lo indica, este instrumento consiste en la instalación de una pieza de metal que mantiene la palanca de cambios del vehículo inmovilizada. Este lleva instalado una cerradura para llaves que solo el propietario posee y es el único capaz de desactivar la misma [7].

1.1.6 Bloqueador del volante-pedal:

Este mecanismo es también otra de las más populares y de bajo costo. Consiste en una barra de metal que se sujeta desde el pedal del freno del automóvil, hasta el volante,

impidiendo así que se pueda accionar el freno y que el guía pueda maniobrase en cualquier dirección [8].

1.1.7 Bloqueador de pedales:

Es una barra de acero que aprisiona los pedales para que estos queden totalmente fijos y no se puedan accionar en caso de que el vehículo sea encendido. De esta manera, el automóvil no puede ser puesto en marcha [9].

1.1.8 Inmovilizador Electrónico:

La función de este es imposibilitar el encendido del motor del vehículo, sin la llave, comando remoto u otro dispositivo programado en el equipo [10]. En general, este tipo de sistema consiste en la comunicación de un artefacto electrónico con otro, de manera que, cuando esta se efectúa, se activa el paso de la corriente a la ignición del motor del automóvil, haciendo posible el arranque del mismo. En caso contrario, si no surge un intercambio de información entre estos dispositivos, pues sería imposible poner el vehículo en marcha, al menos que esto suceda [11]. Los inmovilizadores electrónicos más comercialmente utilizados serán explicados a continuación.

1.1.8 Inmovilizador por Comandos Remotos Infrarrojos:

Este consiste en la instalación de un transmisor infrarrojo (IR) en el cabezal de la llave del vehículo, el cual envía un código único al dispositivo receptor que se encuentra en el conmutador de arranque del vehículo [12].

1.1.9 Inmovilizador con Teclado Numérico:

En este el conductor debe ingresar una pequeña contraseña de 4 dígitos en un teclado electrónico alfanumérico antes de intentar encender el vehículo. En este tipo de

inmovilizadores no hay receptores ni emisores de radiofrecuencia como en casos anteriores [13].

1.1.10 Inmovilizador con Llave Transpondedor:

Este sistema consiste en una llave convencional equipada con un dispositivo que permite ser identificado por señales de radio frecuencia una vez se encuentra dentro o cerca del vehículo. La palabra “transponder” viene del inglés "Transmitter & Responder", lo que significa que el mismo dispositivo transmite y responde [14].

1.2 Los sistemas de alarmas contra robo de vehículos.

De forma general, un sistema de alarma es conocido como un conjunto de dispositivos electrónicos, capaces de producir una señal de aviso, la cual advierte a las personas acerca de la proximidad de un peligro [15]. Estos equipos con inteligencia programada fueron creados para evitar el robo total o parcial de los automóviles, así como también, de pertenencias colocadas en el interior del mismo [16]. Estos son artefactos electrónicos diseñados como elemento notificador de alguna anomalía en el vehículo.

Esta modalidad es la más utilizada en la actualidad, ya que, es una de las más conocidas, seguras y completas del mercado. Este sistema consiste en un conjunto de dispositivos que permiten el acceso al vehículo mediante la transmisión de información por ondas electromagnéticas, que son emitidas por el módulo de acceso (control de mando) al sistema de recepción instalado en el vehículo.

Este sistema puede ser activado o desactivado a distancia, mediante el control inalámbrico que posee el propietario. Se debe agregar que, también tiene la capacidad de bloquear el sistema de ignición del vehículo, haciendo que el motor no pueda ser

encendido en caso de que se ingrese al automóvil sin antes desactivar el sistema mediante el control de mando.

Lo que diferencia este tipo de modalidad contra robo de vehículos de los demás, es la capacidad que tiene de enviar una señal alterna, permitiendo la activación de la corneta y las luces del automóvil, advirtiéndole así al propietario que el perímetro del vehículo ha sido violado, ya sea en caso de intento de apertura de alguna de las puertas mientras el sistema está activo, o en caso de que el automóvil sea golpeado. Esto es posible ya que la computadora central controla los sensores instalados en el auto, y en el momento que se detecta un movimiento se activan estas señales visuales y sonoras. Este sistema posee también un sensor llamado “sensor de golpe”, el cual se describe detalladamente en la sección 1.2.4 “Partes Complementarias de los Sistemas de Alarma”.

1.3 Invención y evolución de los sistemas de alarma contra robos de vehículos

La creación de todo artículo de valor que tiene fácil salida y que es de interés para todo tipo de persona, ha hecho que algunos individuos vean como necesario el hurto de los mismos. Desde la invención del primer automóvil surgieron los denominados ladrones de vehículos, los cuales realizan este tipo de acciones. Esto ha hecho que con el tiempo se lanzaran al mercado los actualmente conocidos sistemas de alarmas para vehículos, para evitar o disminuir este tipo de robo. Según la empresa alemana ABUS, fabricante de productos de seguridad desde el 1924, la primera alarma electromagnética del mundo la patentó el 21 de junio de 1853 un hombre llamado Augustus Russel Pope, nacido en somerville, Boston [17].

Pope ideó un dispositivo a base de pilas que, a pesar de que ahora nos pueda parecer simple, demostró ser un sistema efectivo contra los ladrones. Este reaccionaba al

cerrar un circuito eléctrico, en el cual las puertas y ventanas estaban conectadas como unidad independiente a una conexión en paralelo. Así, si se abría la puerta o una de las ventanas, y con ello el circuito eléctrico conectado a ellas, la corriente eléctrica repentinamente creada dentro de los imanes del sistema producía una vibración [18].

Las oscilaciones electromagnéticas producidas se transmitían a un martillo, el cual golpeaba una campanilla de latón [19]. Lo especial del invento de Pope era que la alarma no se podía desconectar simplemente cerrando la puerta o ventana, ya que, por encima de la puerta iba montado una especie de muelle que mantenía el circuito eléctrico en continuo funcionamiento y hacía que la campana siguiera sonando [20].

A pesar de que Pope fue el pionero, es a otra persona a la que se suele considerar el padre de las modernas instalaciones de alarma. Su nombre es Edwin Holmes, comerciante y fundador de la primera empresa de instalaciones de alarmas eléctricas, que curiosamente compró en 1857 los derechos del invento al propio Pope [21]. Fue él quien puso en marcha la técnica de alarmas electromagnéticas con su empresa "Holmes Electric Protection Company" y quien marcaría los derroteros que seguiría la industria [22].

Cabe destacar que a través de los años la tecnología ha ido avanzando y los sistemas de seguridad son más seguros y cada vez más exigentes. En principio eran sistemas sencillos, ahora son estructuras más complejas y robustas que brindan mayor seguridad, tranquilidad y satisfacción al usuario. En la actualidad, se implementan las comunicaciones inalámbricas para brindar más comodidad.

1.4 Partes Complementarias de los Sistemas de Alarma de vehículos.

Todo sistema debe su funcionamiento a un conjunto de dispositivos que, interconectados entre sí, desarrollan una serie de funciones según sea el propósito o necesidad. Cabe destacar que esto ocurre en cualquier tipo de artefacto que dependa de

otros componentes para un correcto procesamiento de la información, incluso en el caso de las alarmas automotrices.

Para tener conocimiento del funcionamiento de este tipo de sistema tecnológico para la protección, previamente se deben dar a conocer las partes básicas que lo complementan, las cuales se describen a continuación.

1.4.1 Módulo central.

Esta es la parte más importante del sistema. Es un módulo encargado de controlar todas las funciones de la alarma y cuenta con interfaces de salida para la conexión de cada una de las funciones que desempeña en el vehículo. A este se interconectan los periféricos de entrada (pulsadores de cortesía de las puertas, el switch de encendido del vehículo y el receptor de RF) y los periféricos de salida (corneta del vehículo, luces y seguros de las puertas) [23].

1.4.2 Control transmisor

Los equipos de seguridad disponen de dos controles remotos para la comunicación del dispositivo. Existen cientos de marcas de controles remotos los cuales varían en diseño y alcance según las especificaciones del fabricante [24]. Este dispositivo es el que utiliza el usuario para comunicarse a distancia con la alarma del vehículo. Esto es posible gracias a los pulsadores que este posee, que en la mayoría de los casos son 4:

1.4.3 Armado

Este botón se presiona cuando el usuario desea activar el sistema de alarma. Al hacerlo, la bocina emite un solo sonido y las luces encienden y se apagan una sola vez. Si la bocina emite 3 sonidos en vez de uno solo, la alarma está indicando que una de las puertas todavía se encuentra abierta [25].

1.4.4 Desarmado

Este botón se pulsa cuando el usuario desea desactivar el sistema de alarma. Al hacerlo, la bocina emite el mismo sonido dos veces y las luces encienden y se apagan dos veces [26].

1.4.5 Armado/Desarmado Silencioso

Con este botón el usuario puede hacer que la alarma se active o desactive de forma silenciosa. Esto es posible presionando este botón con el ícono del asterisco (*) antes de presionar el botón de armado o desarmado [27].

1.4.6 Apertura de baúl o cajuela

Como su nombre lo indica, con este pulsador el propietario tiene la facilidad de abrir el baúl de su carro a distancia, dejando presionado el mismo por un periodo de tiempo muy corto, según indique el fabricante [28].

1.4.7 Luz indicadora

Esta luz indicadora inteligente muestra el estatus del sistema de seguridad con un determinado número de parpadeos, los cuales indican si la alarma se encuentra activada, desactivada, o en modo de valet, si fue activada o que zona de la alarma fue violada [29]. Esta luz es un LED (Diodo Emisor de Luz) que se coloca mayormente en la parte baja del cristal delantero del vehículo para la fácil visualización.

1.4.8 Sensor de golpe

Este sensor generalmente se incluye de manera externa en las alarmas y cuenta con un arnés de conexión directa con el módulo principal. El sensor envía una señal al módulo central cada vez que exista alguna vibración o golpe en el vehículo, la cual hace que la alarma se ponga en modo de disparo [30]. La mayoría de los sensores de impacto

que vienen con la alarma tienen la capacidad de poder regularlos de manera manual, gracias al potenciómetro que este trae instalado en su tarjeta. Con esto cada usuario puede poner la sensibilidad del sensor de golpe que desee según entienda prudente.

1.4.9 Interruptor de valet

En este modo la alarma deshabilita todas las funciones del sistema tales como sonido de claxon y/o sirena, activación de cortacorrientes, intermitencia de luces, etc. Esta función es utilizada cuando el usuario desea que el dispositivo de seguridad permanezca inactivo, por ejemplo, cuando el vehículo es llevado a un taller de servicio mecánico, taller de lavado o en un valet de estacionamiento [31].

También se utiliza como botón de emergencia, ya que se usa en caso de existir una pérdida o avería de control remoto el usuario tenga la posibilidad de desactivar el sistema de seguridad de manera manual. El procedimiento de desactivación de emergencia de las alarmas a través del valet no codificado, es poner el interruptor de ignición del vehículo en modo de arranque, presionar o mover el botón de valet hasta que el dispositivo deje de sonar el claxon y las luces dejen de parpadear, deshabilitando los cortacorrientes de la alarma y permitiendo que el vehículo pueda ser encendido [32].

1.5 Funcionamiento de los sistemas de alarma.

1.5.1 Alimentación, activación y sensores de puerta.

Una vez conocidos los componentes de un Sistema de Alarma, es preciso describir los principales modos de operación de la misma para poder tener una idea más amplia acerca de este tipo de sistemas de protección.

Los sistemas de alarma en general están interconectados a un conjunto de periféricos, los cuales, son utilizados para hacer posible su activación justo en el momento

necesario. Este es el caso de los pulsadores que traen de fábrica todos los automóviles en cada una de sus puertas. Estos sensores hacen posible la visualización de un ícono en el tablero del auto que indica cuando una de las puertas se encuentra abierta, además de que mantienen encendidas las luces interiores del coche mientras la puerta permanezca abierta.

Cuando las puertas están cerradas, estos sensores se mantienen abiertos, es decir, que no envían ninguna señal a las del interior del vehículo, y, por lo tanto, estas no encienden. En caso contrario, si una de las puertas es abierta, el pulsador de dicha puerta cierra el circuito y envía una señal a las luces del interior del auto, permitiendo que las mismas enciendan, lo que significa que una de las puertas no se encuentra cerrada.

Esta señal enviada a las luces del interior es la que se aprovecha para activar el sistema de alarma cuando una de las puertas se apertura. La misma llega al módulo central, cuya misión es comunicarse con el claxon, seguros eléctricos de las puertas y luces delanteras/ traseras. Esto ocurre cada vez que la alarma sea activada o desactivada. Una vez esto sucede, el sistema puede ser deshabilitado mediante el control que posee el propietario o dueño. De la misma manera, en caso de abrir o cerrar los seguros del vehículo, el usuario debe usar el mando inalámbrico.

1.6 Introducción a las tecnologías inalámbricas.

1.6.1 Conceptos básicos sobre redes inalámbricas.

Las comunicaciones inalámbricas, en sentido general, es todo aquello que permita transferir una información de un punto A hasta un punto B sin la necesidad de utilizar un canal que requiera la interconexión de cables. Se puede decir, que todo lo que está relacionado a la utilización del espectro radioeléctrico mediante artefactos como

dispositivos móviles, comunicaciones de dispositivos electrónicos vía Bluetooth, Infrarrojo, Radiodifusión o sencillamente una pequeña conversación entre un grupo de personas entra en la categoría de comunicaciones inalámbricas [33].

1.6.2 Clasificación de las redes inalámbricas.

Las comunicaciones inalámbricas se pueden clasificar de forma distinta dependiendo su alcance y la manera que se controla el acceso a la red. Este tipo de comunicación se clasifica de la siguiente manera [34]:

Redes de área personal inalámbrica (WPAN): Este tipo de red tiene una cobertura inferior a los 10 Metros y es más utilizada para las conexiones entre dispositivos tales como impresoras.

Redes de área local inalámbrica (WLAN): Esta red tiene una cobertura de cientos de metros y es utilizada mayormente en edificios o grupos de edificios para crear un entorno de red local para brindar el servicio de WI-FI.

1.6.3 Extensiones de Estándares Inalámbricos como el 802.11 son:

- **802.11d:** Constituye a una mejora al nivel de control de Acceso al Medio (MAC) en 802.11 permitiendo el uso, a escala mundial, de las redes WLAN del estándar 802.11, ayudando a los puntos de acceso transferir información sobre los canales de radio admisibles, con un nivel de potencia aceptables, para los dispositivos de los usuarios [35].
- **802.11e:** El objetivo de este estándar es proporcionar soporte de Q o S (Calidad de Servicio) para aplicaciones de redes LAN. Este servicio será aplicado a los estándares físicos a, b y g del estándar 802.11. Su finalidad es proporcionar claves de servicio con niveles gestionados de Q o S para aplicaciones de datos, voz y vídeo [36].

- **802.11f:** Inter-Access Point Protocol (IAPP) tiene como objetivo lograr la interoperabilidad de Puntos de Acceso (AP) dentro de las redes WLAN multi-proveedor. Cuando un usuario se traslada desde un punto de acceso a otro, este estándar define el registro de Puntos de Acceso (AP) dentro de la red y permite el intercambio de información entre dichos Puntos de Acceso [37].
- **802.11h:** Dynamic Frequency Selection and Transmit Power Control mechanisms su objetivo es hacer cumplir los reglamentos europeos para las redes WLAN a 5 GHz. Las demandas de Europa para la banda de 5 GHz, es que los productos tengan control de la potencia de transmisión (TPC) esto limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano y selección de frecuencia dinámica (DFS); que es la que selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas, en particular el radar [38].
- **802.11i:** Se refiere a la seguridad. Se aplica a los estándares físicos a, b y g de 802.11. Dicho estándar Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) utilizando nuevos métodos de encriptación y nuevos procedimientos de autenticación. El IEEE 802.1x constituye una parte clave de 802.11i [39].

1.6.3 Breve Historia del GPS

En el año 1965 la Fuerza Aérea y la Marina de los Estados Unidos financio el proyecto TRANSIT. Este sistema de navegación basado en satélites era utilizado para localizar objetos sobre la superficie de la tierra. TRANSIT estaba constituido por seis satélites orbitando sobre la superficie terrestre a una altura de 1074 Km por encima del mar donde los datos transmitidos por este sistema eran dimensionales (2D) latitud y longitud. Dicho sistema nunca fue utilizado para la ubicación de vehículos móviles tales

como aviones, misiles, ya que, las mediciones que tomaba eran muy lentas y duraba mínimo 30 minutos en pasar por encima del objeto de estudio [40].

En 1973 el departamento de Defensa de los Estados Unidos unifico los proyectos TIMATION (Bidimensional, pero con mejor precisión temporal y financiado por la marina de los Estados Unidos) y el sistema 621B (Tridimensional en desiertos simulando diferentes comportamientos y financiado por la Fuerza Aérea de los Estados Unidos) dicha unión para el 17 de agosto de 1974 se llamó NAVSTAR (Global positioning System) incluía un total de 24 satélites donde 3 eran de reservas por recorte de presupuesto [41].

Para el año 1991 el Sistema NAVSTAR _GPS no estaba en su total funcionamiento; fue durante la guerra del golfo pérsico que el sistema demostró su potencialidad en los campos de pruebas inmejorables logrando provocar que el mundo quedara estupefacto con la alta precisión que tenía el sistema en dirigir los misiles a sus objetivos ocasionando una aceleración en el desarrollo de dicha tecnología [42].

1.6.3 Conceptos básicos del GPS

El Sistema global de posicionamiento (GPS en ingles Global Positioning System) es un sistema de navegación satelital conectado a una red de 24 satélites que han sido colocados en órbita por el Departamento de Defensa de los Estados Unidos. Este sistema fue originalmente creado para el uso militar, pero en los años 80's, el sistema ya estaba disponible para el uso general. Esta tecnología funciona bajo cualquier tipo de condiciones climáticas, en cualquier parte del mundo, las 24 horas del día, sin ninguna suscripción o cargos por la utilización del servicio [43].

Los satélites que forman parte de esta red circulan la órbita de la tierra dos veces al día a una velocidad de 1400km/h transmitiendo información hacia la tierra donde los receptores GPS reciben la información transmitida por el satélite y utilizando la triangulación calculan la ubicación exacta del satélite. Dichos receptores hacen comparaciones con el tiempo que el satélite transmite la señal y el tiempo en el que se recibió la señal y conociendo la diferencia de tiempo entre ambas señales el receptor calcula que tan lejos está el satélite de la tierra [44].

En el transcurso del tiempo la comunidad civil ha encontrado alternativas que les ha permitido obtener una excelente precisión en la localización utilizando las técnicas de diferenciación. Gracias a estas técnicas las aplicaciones de este sistema han experimentado un gran crecimiento y actualmente existen más de 70 fabricantes de receptores GPS [45].

1.6.4 Funcionamiento de la tecnología del GPS

El sistema GPS tiene por objetivo calcular la posición de un punto cualquiera en un espacio de coordenadas de 3 dimensiones (x,y,z), partiendo del cálculo de las distancias del punto a un mínimo de tres satélites cuya localización ya es conocida. Para la medición del tiempo de vuelo de la señal de radio tanto el reloj del receptor como el de satélite tienen que estar muy bien sincronizados entre sí, debido a que ambos deben generar simultáneamente el mismo código. Ahora bien, los relojes de los satélites son de muy alta precisión, no se puede decir lo mismo de los receptores ya que, los relojes son osciladores de cuarzo de muy baja calidad siendo menos imprecisos que los del satélite. Las distancias con errores debido al sincronismo se denominan pseudodistancias. La

desviación en los relojes de los receptores añade una incógnita más que hace necesario un mínimo de cuatro satélites para estimar correctamente las posiciones [46].

Existen 5 pasos principales, en los cuales se resume el funcionamiento del sistema GPS son [47]:

1. **Triangulación:** La base del GPS es la "triangulación" desde los satélites.
2. **Distancias:** Para "triangular", el receptor de GPS mide distancias utilizando el tiempo de viaje de señales de radio.
3. **Tiempo:** Para medir el tiempo de viaje de estas señales, el GPS necesita un control muy estricto del tiempo y lo logra con ciertos trucos.
4. **Posición:** Además de la distancia, el GPS necesita conocer exactamente donde se encuentran los satélites en el espacio. Orbitas de mucha altura y cuidadoso monitoreo, le permiten hacerlo.
5. **Corrección:** Finalmente, el GPS debe corregir cualquier demora en el tiempo de viaje de la señal que esta pueda sufrir mientras atraviesa la atmósfera.

1.6.5 Fuentes de errores en los sistemas GPS

A continuación, se describirán las fuentes de error que en la actualidad afectan de manera significativa a las medidas realizadas con el GPS [48]:

- **Perturbación ionosférica:** La capa inosférica está formada por una capa de partículas cargadas eléctricamente que cambian la velocidad de las señales de radio que la atraviesan.

- **Fenómenos meteorológicos:** En la troposfera el vapor de agua afecta a las señales electromagnéticas ocasionando la disminución de su velocidad. Los errores que son generados son muy similares en magnitud a los causados por la capa ionosferica, y su corrección es prácticamente imposible.
- **Imprecisión en los relojes:** Los relojes atómicos de estos satélites presentan una ligera desviación a pesar de su cuidadoso ajuste y control, esto mismo ocurre con los relojes de los receptores.
- **Interferencias eléctricas imprevistas.** Las interferencias eléctricas pueden ocasionar correlaciones erróneas de los códigos pseudo-aleatorios o un redondeo inapropiado en el cálculo de una órbita. Si este error es grande resulta fácil detectarlo, pero no ocurre lo mismo si las desviaciones son pequeñas y provocan errores de hasta un metro.
- **Error multisenda.** Las señales que son transmitidas desde los satélites pueden sufrir reflexiones antes de poder alcanzar el receptor. Los receptores modernos tienen la facilidad de emplear técnicas avanzadas de proceso de señal y contienen antenas con un diseño especial para ayudar a minimizar este error, que resulta ser muy difícil de modelar dependiendo del entorno donde se ubique la antena GPS.

1.7 Sistema global de las comunicaciones móviles, GSM

1.7.1 Breve historia sobre el GSM

El sistema **GSM** (*Sistema global de comunicaciones móviles*) se ha convertido en el estándar más usado en Europa y Latinoamérica desde comienzos del siglo XXI. Para Europa este sistema inicio su estandarización en el año 1982, por Groupe Special Mobile o grupo GSM en la CEPT (Conference Europeenne de Postes y Telecommunications), cuyo objetivo fue, definir un sistema de comunicaciones móviles en todo el continente europeo, que permitiera la utilización de un mismo terminal en todos los países que lo conforman.

Este junto a los sistemas de comunicaciones americano IS54 e IS95 constituyen la segunda generación de comunicaciones móviles que usan el sistema digital de forma exclusiva, con la capacidad de abarcar la mayor población posible a un costo disminuido. La parte técnica de estandarización del sistema GSM está bajo la autoridad de la ETSI (European Telecommunications Standards Institute), pero la CEPT estaría encargada de la regulación de frecuencias en este sistema [49].

En 1991 se convirtió en el estándar internacional llamado "Sistema Global de Comunicaciones Móviles". Convirtiéndose en la tecnología digital inalámbrica de segunda generación (2G) más ampliamente utilizada a nivel mundial, y está disponible en más de 210 países, contando con más del 75% del total de clientes inalámbricos, por lo que actualmente es la referencia mundial redes de radio móviles [50] [51].

Esta generación se caracteriza por pasar de sistemas análogos a sistemas digitales, usando circuitos digitales de datos conmutados por circuito y protocolos de codificación más sofisticados. La segunda generación de la telefonía celular redujo costos, siendo la tecnología más predominante el sistema GSM, donde los circuitos estaban dedicados exclusivamente a cada usuario [52].

Trabaja gama amplia del espectro de bandas, como las siguientes: 850, 900, 1800 y 1900 MHz. El estándar GSM, en Europa, usa las bandas de frecuencia 900MHz y 1800 MHz. Sin embargo, en los Estados Unidos y Suramérica se usa la banda de frecuencia de 1900 MHz. Por esta razón, los teléfonos móviles que funcionan en Europa y los Estados Unidos solían conocerse con el termino Tri-banda y los que funcionaban sólo en países europeos se denominaban Bi-banda [53].

El sistema GSM inicialmente se desarrolló para transmisión de voz, pero este también era capaz de transmitir datos hasta 9,6 kbit/s en el enlace descendente o Downlink y en el enlace ascendente o Uplink. Provisionalmente, con la solución técnica HSCSD se consiguió aumentar la velocidad de transmisión a 43,2 kbit/s en el Downlink y hasta 14,4 kbit/s en el Uplink [54]. Con el rendimiento máximo de 9,6 kbps del sistema GSM, es posible la transmisión de voz y datos digitales de volumen bajo, por ejemplo, mensajes de texto (SMS, *Servicio de mensajes cortos*) o mensajes multimedia (MMS, *Servicio de mensajes multimedia*).

El sistema global para las comunicaciones móviles, es un sistema estándar, mediante el cual se implementaron tecnologías como: Servicio General de Paquetes de Radio (GPRS), Tasa de Datos Mejorada para la Evolución de GSM (EDGE) y Acceso

Múltiple por División de Código (CDMA IS95, IS95B); lo que dio paso a la generación 2.5G, con la que se aumentó la velocidad de transferencia, apareciendo nuevos servicios como acceso a Internet desde el móvil mediante el Protocolo para Aplicaciones Inalámbricas (WAP), el Servicio de Mensajería Mejorada (EMS), el Servicio de Mensajería Multimedia, (MMS), entre otros [55].

1.7.2 Operatividad del GSM

En el estándar GSM se describe una red telefónica móvil terrestre (PLMN) completa, digital y de servicios integrados, que comprende:

- Radio acceso con estructura celular.
- Transmisión, conmutación y señalización específicas que soporta las funciones de movilidad.
- Mecanismos de seguridad para establecer llamadas y proteger la información transmitida durante éstas.

La Red del Sistema Global de Telefonía GSM fue definido según el Consejo Superior de Administración Electrónica (CSAE) como: Un servicio portador constituido por cualquier medio de transmisión y conmutación necesarios que permitan enlazar a voluntad dos terminales móviles mediante un canal digital establecido específicamente para la comunicación y que desaparece completado la misma [56].

La comunicación telefónica es posible debido a la conexión entre centrales móviles y públicas. Según las frecuencias en las que opera, el móvil podrá funcionar en diferentes partes del mundo. Por tal razón, la telefonía móvil consiste en una combinación

de una red de estaciones transmisoras y receptoras de radio; repetidores, estaciones base (BTS) y centrales telefónicas de conmutación (MSC y BSC respectivamente), que hacen posible la comunicación entre terminales portátiles (teléfonos móviles) o entre teléfonos móviles y la telefonía fija tradicional. La red GSM consiste en cuatro subsistemas: MS (Mobile Station), BSS (Base Station Subsystem), NSS (Network Switching Subsystem) y OSS (Operation and Service Subsystem). Dentro de dichos subsistemas pueden definirse diversas entidades funcionales [57].

Durante su operación el móvil establece comunicación con una estación base, y a medida que cambia de ubicación, los sistemas que administran la red van cambiando la llamada a la estación base siguiente de forma transparente para los usuarios. Por esto se dice que las estaciones base forman una red de celdas, similar a un panal de abeja, proveyendo cada estación base a los móviles encontrados en su celda [58].

1.7.3 Características de la comunicación mediante tecnología GSM

La telefonía móvil o telefonía celular, básicamente está formada por dos grandes partes: una red de comunicaciones (red de telefonía móvil) y los terminales (teléfonos móviles) que permitirán el acceso a dicha red. Las antenas de los móviles, poseen la capacidad de emitir y recibir ondas electromagnéticas, usando el espacio como medio no guiado para enviar información entre estaciones móviles y estaciones base [59].

Estación de telefonía móvil (SM): El teléfono celular representa una estación móvil, en su interior contiene: un sistema para transducción de voz y comunicación de información, una unidad de radio y una antena emisora/receptora, para que la estación móvil se conecte a la estación base. El teléfono móvil es el dispositivo inalámbrico que

permite tener acceso a la red. Se conoce como celular en la mayoría de países latinoamericanos, porque el servicio funciona mediante una red de celdas, donde cada antena repetidora es una célula, aunque también existen redes telefónicas satelitales. La principal característica de esta tecnología es su portabilidad, permitiendo a la vez, comunicarse desde casi cualquier lugar. Sin embargo, su principal función es la comunicación de voz, como el teléfono convencional.

Estación Base Transceptora (BTS) o Subsistema de Estación Base (BSS): Se instala en una posición óptima dentro del área de cobertura o celda y sus elementos básicos son: antenas emisoras/receptoras, unidades de radio, unidad de energía para alimentar las antenas y otros sistemas necesarios para enlazar las unidades móviles entre si y unidades móviles con la telefonía convencional fija [60]. Esta contiene todos los nodos y funcionalidades necesarias para conectar de manera inalámbrica a los subscriptores móviles, a través de la interfaz de radio hasta la red.

El subsistema de Conmutación de Red (NSS): Es el núcleo de la red, contiene los nodos y funcionalidades necesarias para hacer los intercambios e interconexiones mediante Switch de las llamadas, para manejar subscriptores y la movilidad [61].

También es conocido como SMSS (Switching and Management Subsystems), se encarga de gestionar todas las funciones relacionadas con la señalización para realizar el establecimiento, el mantenimiento, y la posterior liberación de recursos en una llamada en el entorno de una comunicación móvil.

1.7.4 Funciones Básicas del NSS

- Localizar y registrar al subscriptor, posterior a la autenticación del usuario en la red.
- Encaminar llamadas.
- Considera los aspectos que afectan la movilidad del usuario.
- Intercambiar señalización entre entidades funcionales de GSM con redes Externas.

MSC (Mobile Switching Center). Es la entidad base para el funcionamiento de la red, encargada de las labores de conmutación internas de la red y posibilita la comunicación con otras redes. Sus funciones más relevantes son:

- Autenticación de llamadas. Confirma que el usuario que llame tiene disponible o está habilitado para el servicio solicitado.
- Asegura la confidencialidad de los datos de los usuarios. El número IMSI nunca se envía. En lugar de este, se utiliza el número temporal TMSI, generado por la MSC.
- Handover: En la red se pueden dar dos casos: El MS permanece en una BTS perteneciente al mismo MSC o que el MS se desplace en otra área perteneciente a una segunda MSC. En estos casos será misión de la MSC permitir la continuidad de la llamada.

AuC (Authentication Center): Se encarga de verificar si el usuario que solicita el servicio tiene derecho a éste. El mecanismo de autenticación funciona verificando la legitimidad de la SIM, sin transmitir sobre el canal de radio, información personal del

subscriber como (IMSI, Ki). Los códigos de autenticación y la clave son generados por cada subscriber en particular mediante algoritmos establecidos por el estándar. Dichos algoritmos son conocidos por el AuC y la SIM. La función del AuC puede estar integrado como otra aplicación en el mismo HLR, el cual es el único elemento del sistema con el que interactúa. Por razones de seguridad no es posible acceder a él remotamente.

HLR (Home Location Register): Es un registro que se utiliza para almacenar y gestionar la información de usuarios en la red. Pueden ser varios o solamente uno, y es la base de datos más importante en la red dado que guarda datos de los usuarios permanentemente, como el perfil de servicios contratados, información de su localización, o su estatus en la red. En el HLR los usuarios son identificados con el MSISDN (Mobile Station ISDN Number): contiene el CC (Country Code o prefijo internacional del país), NDC (National Destination Code o prefijo nacional) y SN (Subscriber Number or numero de subscriber) [62].

La sociedad occidental actual, vive un fenómeno de exposición y creciente uso de tecnología celular en todas las áreas del quehacer humano. En su mayor parte, se debe a la disminución del costo de los equipos de telefonía móvil y al aumento de sus capacidades tecnológicas. Especialmente, la confluencia de dos tecnologías: la telefonía móvil y el cómputo ubicuo, han propiciado el desarrollo de un dispositivo portátil diminuto; al que se conocen como Smartphones, los cuales han adquirido funcionalidades que van más allá de limitarse a llamar o enviar mensajes de texto, actualmente poseen capacidades técnicas que han propiciado su aceptación, entre las cuales están: su tamaño reducido, carácter personal y una gran conectividad que permite acceder en cualquier momento y lugar, a información y a redes sociales [63].

1.7.5 Banda de frecuencia GSM

El interfaz de radio del sistema GSM se ha implementado en diferentes bandas de frecuencia mencionadas anteriormente, sin embargo, existen más bandas de frecuencias, siendo un total de 14 bandas de frecuencias establecidas por el estándar diseñado por la ETSI [64]. Inicialmente en Europa, el sistema GSM solo especificaba la banda 900 MHz para su operación. Con las frecuencias de 890-915 MHz en el Uplink o subida y entre 935-960 MHz en el Downlink o bajada. El Uplink, se refiere a la transmisión de la estación móvil a la red y el Downlink, a la transmisión de la red a la estación móvil. El ancho de banda de 25 Mhz está separado en 125 canales, con un ancho de banda de 200kHz cada uno.

Con el tiempo los canales disponibles no eran suficiente para cubrir la demanda creciente de esta tecnología en los países europeos, por lo que los diferentes organismos regulatorios, decidieron agregar nuevas bandas de frecuencias como: 1800 MHz, con un ancho de banda de 75 MHz y 375 canales. Esta tecnología y estándares se comenzaron a utilizar en todo el mundo. En el caso de los Estados Unidos, debido a que ya estaban usadas estas frecuencias, se aplicaron para GSM las bandas de 1900 MHz y luego de 850 MHz [65].

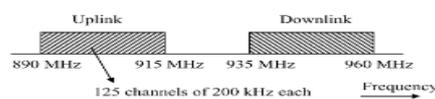


Figure 1.17 GSM uplink and downlink in the 900 MHz frequency band

Table 1.5 GSM frequency bands

Band	ARFCN	Uplink (MHz)	Downlink (MHz)
GSM 900 (Primary)	0-124	890-915	935-960
GSM 900 (Extended)	975-1023, 0-124	880-915	925-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900 (North America)	512-810	1850-1910	1930-1990
GSM 850 (North America)	128-251	824-849	869-894
GSM-R	0-124, 955-1023	876-915	921-960

Figura 5: Bandas de Frecuencia GSM. Extraídas de Communication Systems for the Mobile Information Society (Martin Sauter, 2006).

1.7.6 Tarjeta SIM (Modulo de identificación de suscripción).

Una tarjeta SIM (Subscriber Identity Module) es un componente que representa una de las ventajas del sistema GSM. Un SIM es una tarjeta inteligente desmontable que contiene un chip y memoria no volátil, el cual es insertado en una ranura ubicada usualmente en los lados o la base de los dispositivos móviles. La memoria de esta tarjeta contiene información acerca del suscriptor que permite a una red inalámbrica proveer servicios. Esta tarjeta puede ser movida de un dispositivo a otro, el nuevo dispositivo lee la información contenida en la SIM y la envía a la red para procesar, identificarla y autenticarla. Esta información incluye [66]:

- Numero de identidad del suscriptor.
- Número del teléfono.
- La red original a la que el suscriptor está registrado.

El uso de la tarjeta SIM es de carácter obligatorio en las redes GSM. Su equivalente en las redes UMTS se denomina USIM o UICC (Universal Integrated CircuitCard) y el RUIM (Removable User Identify Module) en los teléfonos CDMA.

1.7.7 Mensajería de texto en Redes GSM.

El servicio de mensajes cortos o SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que como su nombre indica permite el envío de mensajes cortos entre teléfonos móviles, teléfonos fijos y otros dispositivos. SMS fue diseñado originalmente como parte del estándar de telefonía móvil digital GSM, pero en la actualidad está disponible diferentes redes, incluyendo las redes 3G. Un mensaje SMS

es una cadena alfanumérica de un máximo de 140 caracteres o de 160 caracteres de 7 bits, cuyo encapsulado incluye una serie de parámetros [67].

1.7.8 Centro de Servicios de Mensajes de texto cortos (SMS-C)

Es un elemento importante de la red GSM, usado para almacenar y redirigir los mensajes de texto. Los SMS solamente fueron introducidos 4 años luego de la puesta en operación de la primera red GSM, como una utilidad extra y ha sido especificado y estandarizado mediante el artículo de 3GPP TS 23.040. En la actualidad, el uso masivo de los SMS en la mayoría de los proveedores de comunicación, representa un margen de ganancias de alrededor de 15% del total. Los SMS pueden ser usados como mensajería entre persona a persona, para recibir notificaciones de la llegada de un correo electrónico, o que una llamada ha sido redirigida al sistema de correo de voz. Siendo el método de transferencia para estos casos el mismo.

Quien origina el SMS, lo redacta y lo envía desde su dispositivo, este comienza su trayecto a través de los canales de señalización de la red GSM hacia el MSC. Este canal de señalización usado es el mismo que usan los mensajes de actualización de la ubicación del móvil, o mensajes de mantenimiento y servicio del proveedor como los que originan la inicialización para ejecutar una llamada de voz.

En los mensajes de textos solo envían a través de estos canales, el contenido del mensaje, el MSISDN del destinatario y la dirección del SMSC, la cual fue extraída por el dispositivo móvil de la tarjeta SIM. Cuando el MSC recibe un SMS del suscriptor, este lo reenvía directamente al SMSC. Como el mensaje contiene la dirección del SMSC del suscriptor, se hace posible el roaming internacional y el MSC foráneo puede enviar el

SMS a SMSC origen sin la necesidad de una base de datos internacional para todos los SMSC existentes.

Para entregar el mensaje este equipo toma los datos incluidos en el mensaje con la dirección del recipiente y su respectivo MSC. El MSC destino intenta contactar al dispositivo móvil del destinatario, si recibe respuesta el SMS se reenvía. Una vez que se confirma en el dispositivo la recepción del mensaje, el MSC notifica al SMSC para que el mensaje pueda ser borrado de su memoria. En caso contrario que el destinatario no pueda confirmar la recepción, ya sea porque se descargó la batería, está fuera de cobertura o el dispositivo está apagado. En estos casos el flag o bandera de señalización de mensaje en espera se activa, notificando al SMSC que debe mantener almacenado el mensaje, hasta que el dispositivo del destinatario se comuniquen nuevamente con el MSC [68].

1.8 Sistema general de paquetes de datos, GPRS

1.8.1 Mejora del servicio GSM (generación 2.0 a 2.5)

La generación 2.5 es una mejora de la generación 2.0, la cual solo permitía el envío de MMS. La evolución de esta generación les ha permitido a las empresas de telecomunicación brindar un mejor servicio a sus usuarios. Esta mejora contiene 4 estándares principales que son [69]:

- Sistema GPRS (Servicio general de radio por paquetes).
- Sistema HSCSD (Datos de alta velocidad con conmutación de circuitos).
- Sistema EDGE (Tasas de datos mejorados para la Evolución mundial).
- Sistema GERAN (GSM EDGE Radio Access Network).

1.8.2 Conceptos básicos sobre el GPRS

El Sistema General de Paquetes de Datos, mejor conocido por sus siglas en inglés GPRS (General Packet Radio Service), pero antes de tratar sobre las particularidades del mismo, se debe definir esta tecnología y los conceptos relacionados con la misma de tal forma que se desarrolle una idea general sobre lo que consiste dicho sistema, los aspectos que lo caracterizan y el enfoque que lo hace esencial para el desarrollo de nuestra propuesta.

El sistema GPRS consiste en “un estándar para el transporte de paquetes de datos que comparte con GSM su rango de frecuencias. Pensado para facilitar la compatibilidad entre operadores, se implementa sobre la red GSM añadiendo las entidades funcionales que la doten de esta nueva capacidad, y que a su vez posibiliten el inter-funcionamiento con redes externas basadas en paquetes de datos como Internet⁶⁵.” Es decir, la creación del sistema GPRS les facilita a las empresas de telecomunicaciones transferir voz y datos como el internet simultáneamente permitiendo la explotación máxima del ancho de banda que ocupa el sistema GSM del espectro radio eléctrico.

1.8.3 Arquitectura del sistema GPRS

Para que sea posible ajustar el sistema GPRS sobre una red GSM es necesario, implementar un conjunto de modificaciones tanto a la red de acceso como al núcleo de la red, para permitirle al sistema GSM transferir voz y data al mismo tiempo [70].

De todas las modificaciones hechas al sistema GSM, el núcleo de la red será el más afectada y requerirá de actualizaciones más profunda para poder lograr la unión de

ambos métodos y así obtener la mayor eficiencia posible tanto del GSM como del espectro radio eléctrico. Los nuevos elementos que GPRS aporta a la red GSM serán [71]:

- **SGSN**: Serving GPRS Support Node/Nodo de Soporte del Servicio GPRS.
- **GGSN**: Gateway GPRS Support Node/Pasarela del Nodo de Soporte GPRS.
- **CG**: Charging Gateway/Pasarela de Cargo
- **BG**: Border Gateway/Pasarela de Frontera
- **DNS**: Domain Name Sistema/Sistema Nombre de Dominio
- **PCU**: Packet Control Unit/Unidad de Control de Paquete.

1.9 Tecnología Bluetooth.

1.9.1 Breve historia sobre el Bluetooth

El nombre de esta tecnología se estableció en honor al rey Vikingo Harald Blatand que vivo durante el siglo X. este pudo controlar y unificar Dinamarca y Noruega, a partir de esto llego la inspiración del nombre y la creación de esta conexión. Harald le gustaba comer moras y por eso tenía el Tinte azul en los dientes de ahí proviene el nombre (Bluetooth significa: diente azul).

En 1994 se inició la elaboración de una tecnología inalámbrica de corto alcance por el fabricante sueco creador de los teléfonos móviles Ericsson. En 1998 un grupo de compañías formado por Nokia, IBM, Toshiba, Intel y Ericsson llamados SIG (Special Interest Group hicieron posible la creación de esta tecnología que permite la transferencia de información inalámbricamente entre dispositivos [72].

Desde entonces una alta variedad de compañías están utilizando esta tecnología de baja potencia y de corto alcance que se ha convertido en un elemento necesario para

un sin número de dispositivos tecnológicos. El concepto detrás del Bluetooth es proveer una conexión inalámbrica de 2.4 GHz esto quiere decir, que los dispositivos que utilizan Bluetooth para transferencia de datos que estén a una distancia de 10m entre ellos, podrán compartir una capacidad de transferencia de 720Kbps. La tecnología Bluetooth provee múltiples utilidades, apreciables por los usuarios en los diversos artefactos o dispositivos que la emplean. Entre ellas están [73]:

- Hacer llamadas desde un auricular inalámbrico conectado remotamente al móvil.
- Eliminación de cables que interconectan impresoras, teclados, y el mouse de una computadora.
- Llamar a la casa para encender y apagar electrodomésticos, configurar la alarma y monitoreo de actividad etc.

1.9.2 Utilidad del sistema Bluetooth

El Bluetooth tiene una cobertura o alcance alrededor de unos 10m y opcionalmente un alcance medio de 10m. Esta conexión inalámbrica permite que unas variedades de dispositivos se conecten de manera instantánea sin necesidad de utilizar un cableado entre ellos teniendo como objetivo la transferencia de datos entre diferentes dispositivos sin interferencia. Este enlace de radio corto trabaja en un rango de frecuencia de 2.402GHz a 2.480 GHz [74].

El Bluetooth es utilizado para transferir información de forma inalámbrica entre un dispositivo y otro. Para poder lograr un enlace confiable entre ambos dispositivos el Bluetooth establece un intercambio de códigos secretos compartidos denotados PINs. A la hora de establecer la conexión entre los dispositivos que poseen esta tecnología y dependiendo la cantidad de personas que se irán a conectar a la red, el Bluetooth puede

ser tipo maestro o tipo esclavo. El esclavo permite el emparejamiento entre 7 dispositivos esclavos conocidos como como Piconet [75].

1.9.3 Tipos de enlace Bluetooth.

La tecnología banda base Bluetooth soporta dos tipos de enlaces que son: conexión sincrónica orientada (SOC) en inglés synchronous connection oriented, utilizada mayormente para la transferencia de voz y conexión asíncrona sin conexión (ACL) en inglés asynchronous connectionless, utilizada para la transferencia de dato [76].

1.9.4 Versiones de Bluetooth

La tecnología Bluetooth es usada principalmente para establecer redes de área personal inalámbricas (WPAN), también conocidas como redes Peer to Peer (P2P). Esta tecnología actualmente está integrada a muchos tipos de dispositivos dirigidos a negocios y al consumidor, incluyendo telefonía celular, asistentes digitales personales, computadoras portátiles, automóviles, audífonos, etc...permitiendo conectarlos a una amplia gama de otros dispositivos para transferir voz y data [77].

Con el tiempo se ha modificado la tecnología Bluetooth pasando progresivamente a diferentes versiones, denotando mejorías en cada una de ellas. La versión 1.1 y 1.2 especifica velocidades de transmisión que alcanzan hasta 1 Mbps, alcanzando una transmisión de salida de datos de aproximadamente 720 Kbps. Mientras que la versión 2.0+ EDR (Tasa de Datos Mejorada) y 2.1 + EDR, especifican una tasa de intercambio de hasta 3 Mbps y transmisión de datos de salida de aproximadamente 2.1 Mbps [78].

Las recientes versiones de Bluetooth 2.0 + Enhanced Data Rate (EDR) y 2.1 + EDR, fueron publicadas en noviembre del año 2004 y Julio 2007 respectivamente. Mientras que la versión 2.0 + EDR provee mejores tasas de transmisión que versiones anteriores; la versión 2.1 + EDR provee una mejoría significativa en la seguridad utilizando la generación de una llave vincula o Link key, y mejoras en el control y manejo en la forma del protocolo SSP (Secure Simple Pairing) [79].

Otras diferencias entre las distintas versiones de Bluetooth son: la versión 1.2 permite que un equipo tenga conexión Bluetooth y Wi-Fi simultáneamente, a diferencia de la 1.1. Tiene mayor seguridad en su arquitectura y ofrece una calidad de audio mejorada. En cuanto a la versión 2.0, esta incorpora la tecnología Enhanced Data Rate (EDR), que triplica la velocidad de transmisión de los datos. La última edición de esta tecnología, la versión 2.1, mejora y facilita la conexión entre equipos y logra un ahorro de energía cinco veces mayor a las versiones anteriores [76].

1.9.5 Clases de Bluetooth

Al tomar en cuenta las características de los canales de transmisión de datos de los equipos Bluetooth, pueden clasificarse según su clase en: Clase 1, Clase 2 y Clase 3. Estas clases hacen referencia a la potencia de transmisión del dispositivo sin alterar la compatibilidad entre un dispositivo de una clase y otra. Los distintos rangos de cada clase se pueden observar en la siguiente tabla [77]:

Clase	Potencia Máxima Permitida (mW)	Potencia Máxima Permitida (dBm)	Rango Aproximado
Clase 1	100 mW	20 dBm	~100 Metros
Clase 2	2.5 mW	4 dBm	~20 Metros
Clase 3	1 mW	0 dBm	~1 Metros (~10 Cm).

Tabla 1: Rango de tipos de Bluetooth

Una particularidad de estos dispositivos y la interacción entre las distintas clases ocurre en ciertos casos, como en los dispositivos de la clase 2 cuya cobertura efectiva se extiende cuando se conecta a otro dispositivo Bluetooth de clase 1. Esto se debe a la mayor sensibilidad y potencia de transmisión del dispositivo de clase 1. En otras palabras, como estos dispositivos cuentan con una mayor potencia de transmisión, permite que la señal llegue con mayor energía a los de clase 2. Como el dispositivo de clase 1 tiene una mayor sensibilidad, es capaz de recibir señales más débiles [78].

Debido a las diferencias en el alcance en la comunicación inalámbrica de los equipos Bluetooth de clase 1, 2 y 3. Como los dispositivos de clase 1 poseen una cobertura de alrededor de 100m son los más usados, siendo los de clase 2 a 20m y los de clase 3 los menos usados por la cobertura disminuida que ofrecen a 1m aproximadamente. A pesar de que no existen problemas de intercomunicación entre equipos de diferentes clases, es pertinente que se ubiquen dentro de la distancia de aquel cuya clase ofrezca el menor alcance. Por lo que, si un dispositivo clase 1 se conectara a uno clase 2 deben ser instalados a una distancia entre ellos menor de 20 metros. Debido a que la tecnología Bluetooth transmite en forma omnidireccional, es innecesario enfrentarlos de tal forma en que tengan una línea de vista ininterrumpida como era el caso con la tecnología de infrarrojos [79].

Los rangos en los dispositivos Bluetooth se caracterizan por tres clases que definen el manejo de la energía que disponen. La mayoría de los dispositivos pequeños, que son alimentadas por baterías son de la clase 2, mientras que los dispositivos clase 1 son típicamente encontrados en llaves o dispositivos USB para computadoras, así como puntos de acceso y otros dispositivos alimentados con energía AC (residencial).

1.9.6 Modos de Comunicación del dispositivo Bluetooth

Los dispositivos Bluetooth, para poder establecer una comunicación entre ellos se debe especificar el modo de comunicación, que son dos: Descubrible y Conectable. El dispositivo en modo descubrible escucha de forma periódica, peticiones de búsqueda de canales físicos, basado en un conjunto de frecuencias específicas y responderá a la petición en el mismo canal, comunicando las siguientes informaciones: su dirección de dispositivo, reloj local y otras características necesarias para sincronizarse y conectarse subsecuentemente al otro equipo. Un dispositivo en modo conectable periódicamente escucha en el canal de búsqueda física y responderá en la página de su canal para iniciar una conexión de red. Las frecuencias asociadas con la página de búsqueda física del canal para un dispositivo están basadas en su dirección de dispositivo Bluetooth. Por lo tanto, conocer esta dirección y el reloj es importante para la conexión entre dos dispositivos con esta tecnología [80].

1.9.7 Seguridad en el sistema Bluetooth

De acuerdo con la más amplia categorización de amenazas a los sistemas de computadoras, las amenazas generalmente se dividen en 3 tipos: Amenazas de revelación, Amenazas de integridad y Amenazas de denegación de servicios. Las amenazas de

revelación se refieren, a la fuga de información desde el sistema a un grupo externo que no debería haber obtenido dicha información, representando una amenaza en contra de la confidencialidad de la información. Las amenazas de integridad involucran cambios no autorizados de la información en cuestión. Las amenazas de denegación de servicios, se refiere al acceso a los recursos de un Sistema y su bloqueo por un agresor malicioso; es una amenaza en contra de la disponibilidad del sistema [81].

Las amenazas que afectan más frecuente a la tecnología Bluetooth y dispositivos asociados son susceptibles a las mismas amenazas generales que intervienen en las redes inalámbricas; como: Denegación de servicios, escuchas a escondidas (eavesdropping), ataques de hombre en el medio, modificación del mensaje, y desapropiación de recursos. Estos también son afectados por ataques, más específicos, en el renglón de la tecnología Bluetooth que se enfocan en vulnerabilidades conocidas en la implementación y especificaciones de esta tecnología. Los ataques en contra de la seguridad Bluetooth mal implementada puede proveer a los agresores con acceso no autorizado a información importante, al igual que les permitiría uso inadecuado de los dispositivos Bluetooth y otros sistemas, o redes a los cuales dicho equipo esté conectado. La combinación de esquemas de saltos de frecuencia y control de energía de la conexión de radio, proveen de forma limitada protección adicional en contra de las escuchas a escondidas y acceso malicioso.

El esquema de saltos de frecuencias es primordialmente una técnica que Evita interferencias, logrando que sea un poco más difícil, que algún atacante capture y localice transmisiones Bluetooth, evitando que sea capaz de diferenciarla de transmisiones de tecnologías de secuencia directa en amplio espectro, como las usadas en los protocolos

IEEE 802.11a/b/g. Cuando la capacidad de control de energía del Bluetooth es usada adecuadamente, cualquier agresor potencial estaría forzada a estar a una distancia relativamente cercana para que pueda representar un riesgo a la conexión Bluetooth, especialmente cuando los dispositivos están muy cercanos uno del otro [82].

1.9.8 Modos de seguridad básicos de Bluetooth

Diversas aplicaciones Bluetooth son descritas como perfiles. Algunos están dedicados a una aplicación específica, mientras que otros son perfiles generales para tareas genéricas.

- **Perfil de Acceso GAP:** define los procedimientos genéricos para descubrir los dispositivos Bluetooth y los aspectos relacionados con el manejo del vínculo o conexión. Este perfil también define los procedimientos de seguridad básico. Un dispositivo conectable opera en tres modos de seguridad diferente:
- **Seguridad Modo 1:** En este modo de seguridad, una unidad Bluetooth, nunca inicia ningún procedimiento de seguridad. Nunca demanda autenticación o encriptación de la conexión Bluetooth.
- **Seguridad Modo 2:** En este modo de seguridad, una unidad Bluetooth no debería iniciar ningún procedimiento de seguridad, como demandar autenticación o encriptación de la conexión de Bluetooth en el momento del establecimiento de dicha conexión. En vez de esto, la seguridad se aplica al canal o al establecimiento de la conexión.

- **Seguridad Modo 3:** En este modo de seguridad, una unidad Bluetooth debería iniciar los procedimientos de seguridad antes de que el proceso de conexión se complete. Dos políticas de seguridad son posibles: Siempre demandar autenticación o siempre demandar autenticación y encriptación a la vez.

Servicios de control para los niveles de acceso pueden ser provistos usando el modo de seguridad 2 y 3. El modo de seguridad que brinda mayor flexibilidad es el modo 2, ya que ninguna seguridad es aplicada a las peticiones de conexión o el canal. Por tal razón, es posible permitir acceso a algunos servicios sin ninguna autenticación o encriptación y una unidad puede estar completamente abierta a otros servicios, mientras se mantiene restricción acceso a otros servicios [83].

2. DISEÑO DE SISTEMA DE ALARMA INTELIGENTE FUNDAMENTADO EN RADIOFRECUENCIA (SAIRF)

Para poder llevar a cabo la selección de los módulos electrónico más convenientes, hemos utilizado el método de la observación y deducción, tomando en consideración las mejores tarjetas electrónicas que puedan ser compatibles con el módulo principal, el Arduino Uno.

Ambas metodologías nos ayudaron a seleccionar un conjunto de dispositivos que serán mostrados en el transcurso de este capítulo, los cuales nos permitirán alcanzar todos los objetivos, tanto el general como los específicos, ilustrados al inicio del anteproyecto. A continuación, se presentan los diagramas en bloques del hardware y software, los instrumentos de forma física, y la interconexión entre ellos, lo que, de manera general, ayudó a darle vida a esta propuesta de diseño.

2.1 Diagramas Generales del Sistema de Alarma Inteligente antirrobo de vehículos.

2.1.1 Hardware

En estos diagramas presentados a continuación, se muestra la forma en la que el cerebro del sistema está interconectado con cada uno de los módulos, sensores y de algunos accesorios del automóvil, los cuales complementan este sistema inteligente de protección contra robo de vehículos. Además, se presenta también la manera en la que se comunica el control de mando con cada uno de los módulos, de forma inalámbrica. En las (figuras 6 y 7) se describen estas características de conexión y diseño.

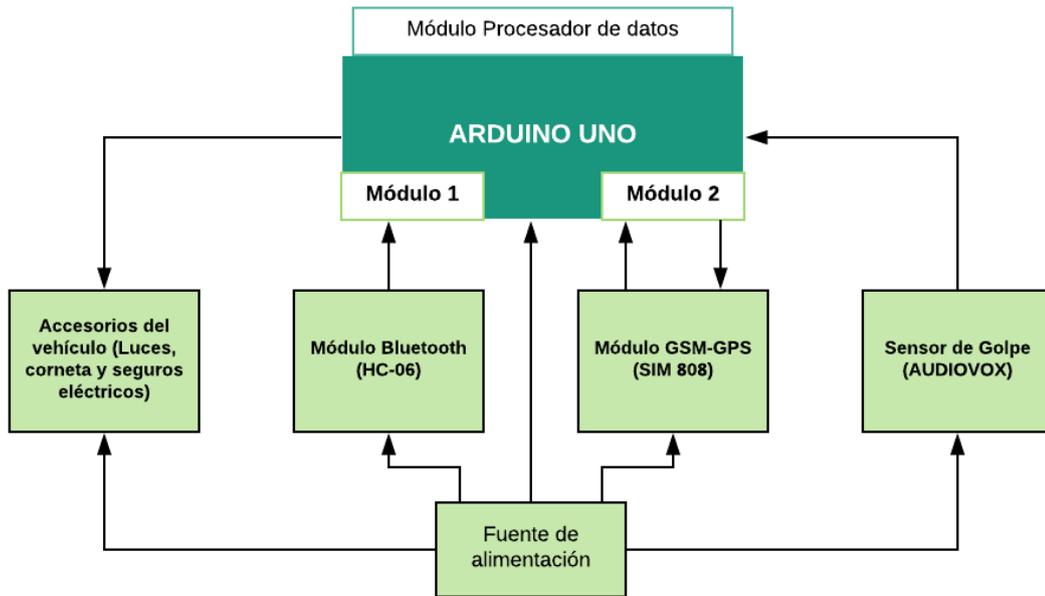


Figura 6: Representación de las conexiones existentes entre el módulo procesador de datos, módulos y sensores del SAIRF. Herramienta de diseño: Lucidchart.

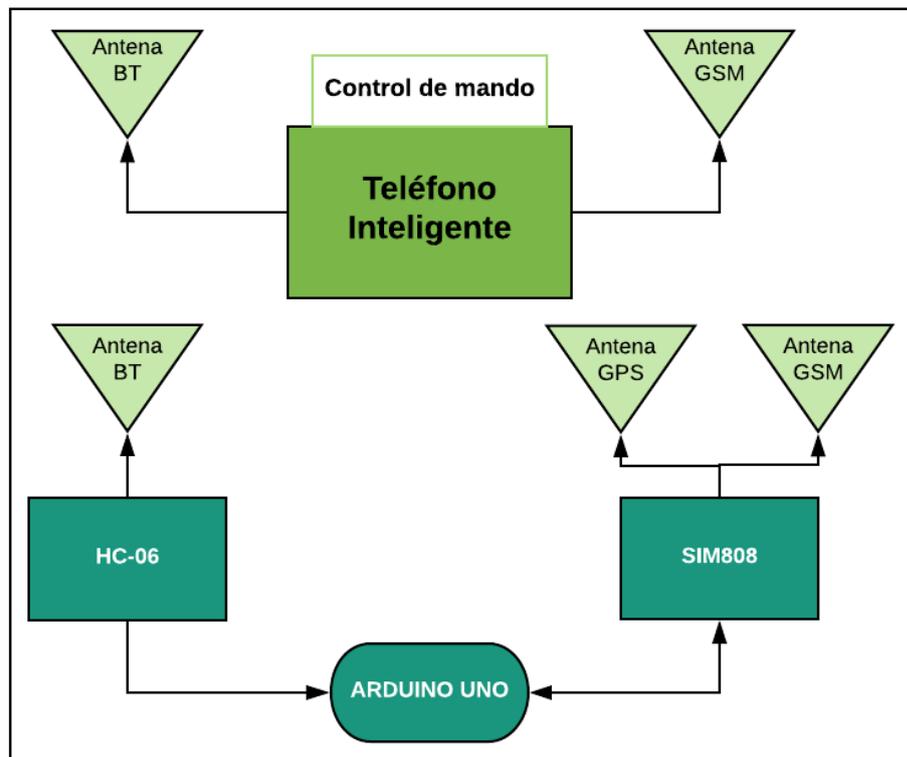


Figura 7: Representación de la estructura comunicacional entre el control de mando y el SAIRF. Herramienta de diseño: Lucidchart.

2.1.2 Software

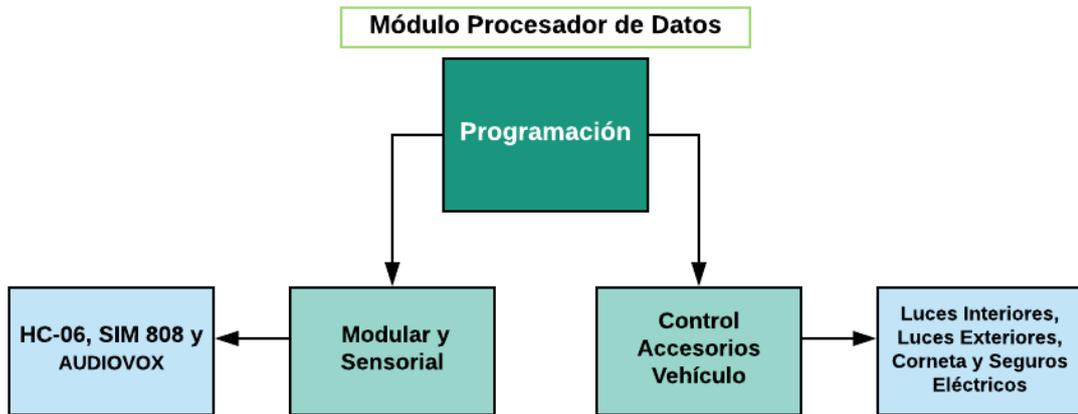


Figura 8: Representación de la estructura interna del módulo procesador de datos del SAIRF. *Herramienta de diseño: Lucidchart.*

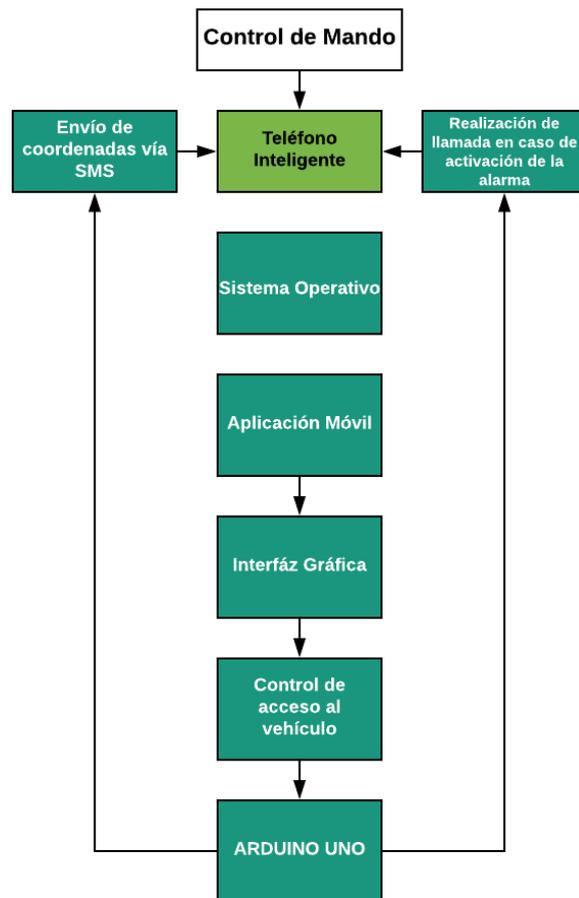


Figura 9: Estructura interna del Control de mando del SAIRF. *Herramienta de diseño: Lucidchart.*

2.2 Hardware seleccionado para el diseño del sistema antirrobo de vehículos.

El diseño del sistema supone el estudio de dispositivos, que mediante sus variaciones o cambios serán analizados para dar una respuesta de alerta en caso necesario. En este sentido, cada uno de los módulos y sensores serán interconectados de manera que los mismos tengan una comunicación estable y efectiva con el microcontrolador, y que este pueda procesar sus solicitudes en cualquier momento para mantener en funcionamiento continuo este sistema de seguridad.

2.2.1 Microcontrolador ATMEGA

Dentro de la lista de dispositivos elegidos para elaborar el sistema de alarma antirrobo de vehículos, se ha considerado el uso de un microcontrolador, el cual es usado como unidad de control en el mismo. El módulo seleccionado hace uso del ATMEGA 328P, un microcontrolador de la familia ATMEL que cumple con las características necesarias para controlar el módulo de comunicación GSM-GPS [84].

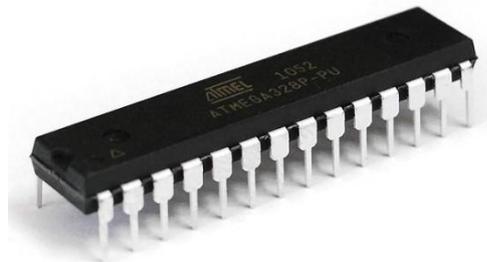


Figura 10: Apariencia física del microcontrolador ATMEGA328P. Extraída de ATmega328P: Data Sheet Complete ATMEL. (2016).

Este microcontrolador es el componente principal en la plataforma “Arduino” es muy utilizado y a la vez recomendado en la realización de pruebas, elaboraciones de proyectos y prototipos en el área de la electrónica y comunicaciones. Las características de este circuito integrado se ilustran en la (Tabla 2).

MCU ATMEGA328P
Características
Arquitectura de 8 bits
Comunicación Serial: UART (Software y Hardware)
Rango de voltaje de funcionamiento: 1.8V - 5.5V
Frecuencia de operación máxima: 20 MHZ
Memoria Flash de 32KB

Tabla 2: Características principales del microcontrolador ATMEGA. Extraído de ATmega328/P: Data Sheet Complete ATMEL. (2016).

2.2.2 Arduino UNO.

Consiste en una plataforma electrónica abierta de software libre, flexible, de grandes recursos y muy fácil de usar. Toda la información que recolecta este dispositivo (figura 11), lo hace a través de los pines de entrada en los cuales pueden conectarse una extensa variedad de sensores, llegando a tener control de una variedad de artefactos electrónicos [85].



Figura 11: Parte superior (izquierda) e inferior (derecha) de la placa Arduino UNO con el microcontrolador ATMEGA como cerebro de la plataforma.

Características generales del Arduino UNO	
Microcontrolador Atmega328P.	Corriente continua por pin IO 40mA
Voltaje de operación 5V.	6 pines pueden usar como OP de PWM.
Voltaje de entrada 7 – 12V.	6 pines de entrada analógica.
Voltaje de entrada (Límite) 6–20V.	14 pines de entradas-salidas digitales.
EEPROM 1 KB.	SRAM 2 KB.

Tabla 3: Características generales del Arduino UNO

2.2.3 Módulo de comunicación GSM y GPS

La localización es un procedimiento llevado a cabo por el módulo GPS, el cual es el encargado de recibir las señales satelitales para calcular las coordenadas geográficas de la posición del mismo. En adición, los módulos GSM corresponden a la etapa responsable de establecer comunicación con otros dispositivos de la red móvil [87]

El automóvil (dispositivo localizable), dispone del módulo SIM808 que conlleva tanto la etapa de localización para obtener la posición en latitud y longitud (GPS), como la de comunicación (GSM), ambas integradas en una misma tarjeta.

2.2.4 Módulo SIM808

Esta placa impresa denominada SIM808 (GPRS / GSM + GPS) es un GSM (sistema global para las comunicaciones móviles) y GPS (Sistema de posicionamiento global), el cual combina ambas tecnologías tanto de comunicaciones móviles como el sistema de posicionamiento global GPS en una misma tarjeta electrónica, ideal para proyectos donde se requiere la capacidad de comunicación [88].

El módulo Sim808 (figuras 13), es una tarjeta electrónica de banda cuádruple (850/900/1800/1900 MHz) con la capacidad de generar llamadas telefónicas, enviar/recibir Mensajes de texto, procesar paquetes de datos y tecnología GPS [89].



Figura 13: Parte superior del módulo SIM808, GPS-GSM, con sus respectivas antenas.

Este dispositivo fue seleccionado considerando que nos ayudará a obtener la ubicación geográfica exacta del automóvil cuando ésta sea solicitada a través de un SMS, así como también nos facilitará el aviso de la activación del sistema mediante una llamada telefónica al propietario. Este módulo es sumamente importante para nuestra oferta de diseño y en la (tabla 4) se dan a conocer sus características de hardware.

Características Generales
Chip SIM808.
Conector para Batería LI-ion (Iones de Litio) para hacer que el dispositivo sea portátil. Rango: 3.5-4v.
Conector de alimentación tipo JACK 2.1*5.5mm. Rango: 5-26v.
Compartimiento instalado para tarjeta SIM tamaño estándar.
Conectores UFL de antenas externas GPS y GSM.
Conectores IDC para establecer comunicación con la placa.

Tabla 4: Características de hardware del módulo SIM808. Extraída de: *Diseño de un sistema electrónico para localizar personas con Alzheimer*. Ortiz N., Vicente A. y Muñoz O. (2016). República Dominicana.

En la (figura 14), se muestra el compartimiento donde se insertará la tarjeta SIM, que es una tarjeta inteligente que les permite a las empresas de telecomunicaciones brindarles un servicio a sus usuarios bajo la red GSM/GPRS. Para el funcionamiento de este diseño es primordial que la tarjeta esté configurada con un número telefónico registrado en cualquier compañía telefónica. Siempre que la tarjeta tenga saldo disponible, le permitirá al sistema enviar SMS a los propietarios de vehículos que consideren utilizar la propuesta de diseño con las coordenadas donde está ubicado el vehículo. Si se da la ocasión de que el propietario necesite cambiar la tarjeta SIM, esta puede ser desmontada, facilitando la transferencia de información almacenada en ella de un módulo a otro.

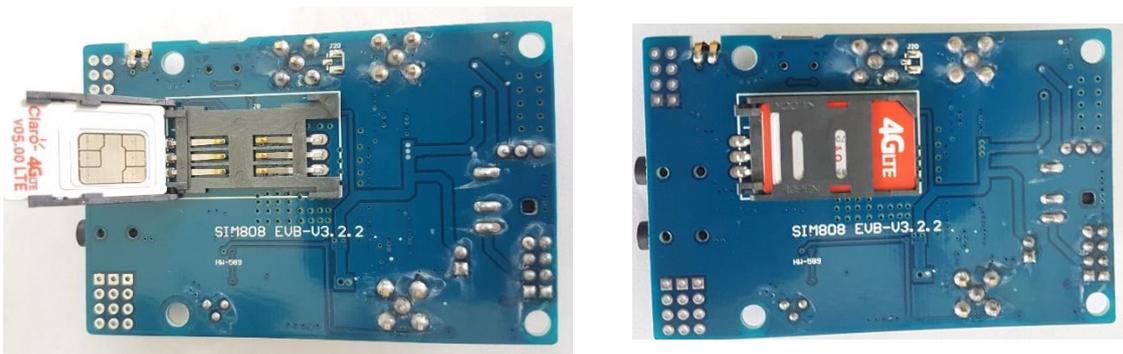


Figura 14: Parte inferior del módulo808 con tarjeta SIM instalada.

El componente principal de módulo GPS-GSM que nos ayudará en el desarrollo de sistema, es el chip SIM808 (figura 15) que, dependiendo de su configuración y programación y tomando en cuenta sus características (tabla 5) nos brindará su más alta eficiencia.



Figura 15: Chip SIM808. Extraída de: SIMCOM. GSM/GPRS+GPS Module.

Características GSM	Características GPS
Quad-band 850/900/1800/1900MHz. Selecciona entre cuatro bandas	Sensibilidad:
Potencia de transmisión: Clase 4 (2W) para GSM 850 y EGSM 900, Clase 1 (1W) para DCS 1800 y PCS 1900	Rastreo: -165 dBm
Almacenamiento de SMS en la tarjeta SIM	Arranque en frío: -147 dBm
Interfaz SIM	TTF:
	Arranque en frío: 30s
	Arranque en temperatura ambiente: 28s
	Arranque en caliente: 1s
	Precisión:
	Posición Horizontal: <2.5 m

Tabla 5: Características técnicas del chip SIM80. Extraída de: *Diseño de un sistema electrónico para localizar personas con Alzheimer*. Ortiz N., Vicente A. y Muñoz O. (2016). República Dominicana.

2.2.5 Módulo de Bluetooth HC-06

El módulo de Bluetooth HC-06 (figura 16), es una pequeña tarjeta electrónica relativamente económica, configurada con un comportamiento de esclavo (Slave) desde su fabricación. Esto quiere decir que este dispositivo solo puede recibir datos, pero no enviar. Este es uno de los más populares para aplicaciones con microcontroladores PIC y Arduino [90]. Sus características se presentarán en la siguiente tabla:

Características HC-06	
Voltaje de alimentación	3.3VDC - 6VDC
Voltaje de operación:	3.3VDC
Corriente de operación:	<40mA
Alcance:	5m-10m
Compatible con el protocolo	V2.0

Tabla 6: Características técnicas del módulo Bluetooth HC-06. Extraída de Módulo Bluetooth HC-06 Serial Rs232 (TTL) Electronilab (2018).

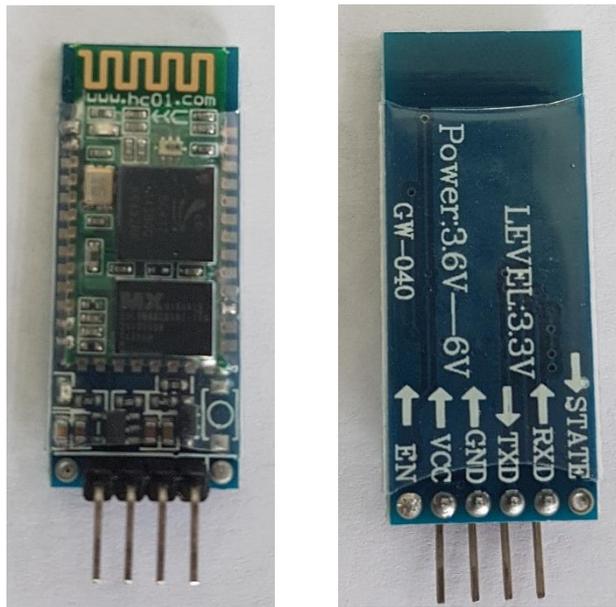


Figura 16: Vista frontal (izquierda) y vista trasera (derecha) del módulo de Bluetooth HC-06.

Esta tarjeta electrónica contiene un total de 4 pines, que van conectados al Arduino UNO, el cual recibirá los datos que el usuario enviará mediante un teléfono móvil. Esta información transmitida será procesada por este módulo de control, de manera tal que le facilitará al propietario del vehículo abrir o cerrar las puertas del vehículo, la cajuela y desactivar la corneta (sonido de la alarma), en caso de que sea activada. El cumplimiento de este proceso será efectivo gracias al microprocesador ATMEGA328P, el cual es el cerebro del sistema.

2.2.5.1 Conectores del módulo Bluetooth HC-06.

- **Voltaje de colectores (VCC).**

Voltaje positivo de alimentación (3.3V – 6V). Esta entrada de voltaje va conectada de forma directa a una de las salidas del módulo de control (Arduino UNO), las cuales son de 3.3V o 5V DC [91].

- **Tierra (GND)**

Este se refiere al voltaje negativo de alimentación (tierra). Va conectada al pin GND del Arduino para que pueda producirse la comunicación serial ⁹².

- **Conector de transmisión (TX):**

Se refiere al pin de transmisión de datos (del módulo HC-06 al Arduino UNO). Por este pin, el HC-06 transmite los datos que este recibe vía bluetooth desde el móvil. El mismo debe ir conectado al pin RX del Arduino [93].

- **Conector de recepción (RX):**

Este conector se refiere al pin de recepción de datos. Este debe ser conectado al pin TX del Arduino [94].

2.2.6 Sensor de golpe AUDIOVOX AS-9492

En todo sistema de alarma es imprescindible la instalación de un sensor de golpe. La función de este dispositivo es enviar una señal al módulo de control del sistema de alarma. Esto ocurre mediante la conversión de vibraciones en una corriente eléctrica al momento en que se produzca un golpe o algún movimiento de forma violenta en el mismo. Dependiendo de qué tan severo sea este movimiento o choque y de cómo esté calibrado el sensor, se podría activar una señal sonora de aviso, en caso de que sea un golpe leve, o bien, el disparo completo de la alarma si se produce un choque de mayor magnitud. La señal de aviso, en la mayoría de los casos, consiste en cinco toques del claxon, cada uno de aproximadamente medio segundo de duración, mientras que el disparo completo de la alarma produce estas pulsaciones con mayor duración. Este comportamiento se efectúa siempre y cuando el sistema se encuentre en estado activo.

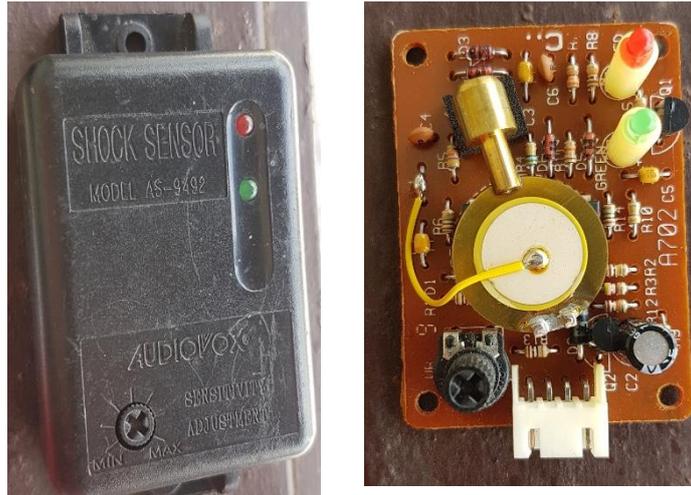


Figura 17: Ilustración del sensor de golpe AUDIOVOX, AS-9492. Plástico protector (izquierda) y estructura interna (derecha).

Este dispositivo está compuesto por un contacto de metal largo y flexible (observar figura 17, derecha), colocado sobre otra pieza del mismo material. Cuando estos hacen contacto, la corriente fluye entre ellos, de manera que una sacudida substancial hará mover al contacto flexible de modo que toque el de abajo, cerrando así el circuito brevemente [95]. La (tabla 7) describe las características fundamentales del sensor de golpe escogido como parte complementaria para la elaboración de este proyecto.

Especificaciones Sensor de Golpe AS-9492	
Voltaje de operación	12VDC
Dimensiones:	1.20 x 3.00 x 3.60 pulgadas
Rotación máxima de ajuste	270°

Tabla 7: Características fundamentales del sensor de golpe AS-9492.

2.2.6.1 Conectores del sensor de golpe

Esta pequeña tarjeta tiene un total de 4 conectores, los cuales realizan una función diferente. Estas se explican a continuación:

- **Voltaje de colectores (VCC):**

Este conector es la entrada de voltaje positivo al sensor. Para este, el voltaje de alimentación es de 12VDC. Este es el primer pin de derecha a izquierda, observando el sensor de frente.

- **Tierra (GND):**

Este se refiere al voltaje negativo de alimentación y va conectada al negativo de la batería, que para este dispositivo es de 12VDC. Este conector es el segundo de derecha a izquierda.

- **Pre-detección:**

Se utiliza para dar señales de aviso en caso de que el sensor reciba vibraciones leves [F11]. Esto ocurre cuando el contacto con el vehículo no es de mucha intensidad o cuando el mismo no se produce con violencia.

- **Full Trigger:**

Este conector se utiliza para activar totalmente el sistema de alarma. Esto ocurre cuando el sensor considera un golpe de mayor magnitud que en el caso anterior. Una vez ocurre esto, el cerebro del sistema mantiene la corneta sonando por un tiempo determinado.

2.2.7 Batería de litio

En 1970 se comenzó a comercializar este tipo de batería creada por G.N Lewis. En los años 80, se hicieron esfuerzos para desarrollar baterías recargables de litios, pero al ser cargadas generaban una alta temperatura térmica, lo que ocasionaba una reacción muy violenta [96]. En nuestra propuesta de diseño utilizaremos una batería Ion litio

(figura 18) sus densidades energéticas son un poquito más baja que las de metal, aun así, nos proporcionara el rango de voltaje necesario (3-4 V) para la activación del Arduino Uno junto al módulo Bluetooth y el módulo GSM-GPRS. La batería es recargable y aunque su ciclo de carga y descarga es limitado, permitirá que el sistema continúe funcionando en caso de que el sistema convencional del vehículo sea removido.

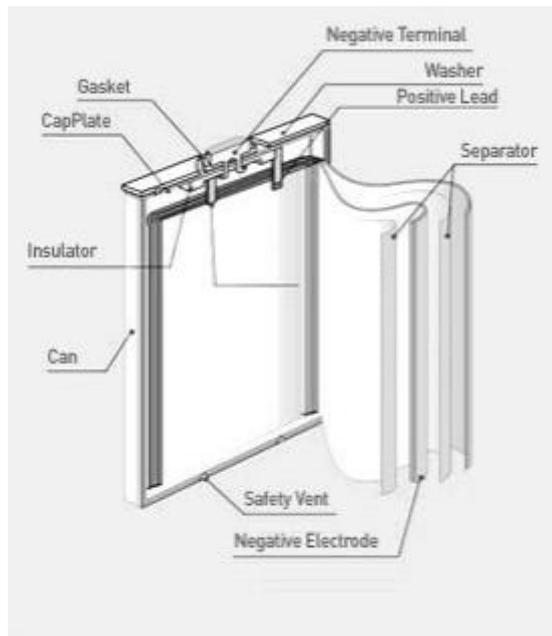


Figura 18: Batería de Ion de litio.

2.3 Tecnología de comunicación interna para el sistema antirrobo de vehículos fundamentado en radio frecuencia (SAIRF).

2.3.1 Protocolo de comunicación UART

El Transmisor-Receptor Asíncrono Universal (UART), en inglés "Universal Asynchronous Receiver/Transmitter", es un protocolo de comunicación que sirve como interfaz de comunicación para la transmisión y recepción de información de manera serial entre dos dispositivos. El funcionamiento del mismo consiste en la estructuración de

paquetes de datos con un tamaño de 8 bits (1 byte) para ser transmitidos bit por bit a un segundo dispositivo, cuyo UART al recibirlo realiza el mismo proceso, pero de forma inversa [97]. Para que pueda producirse la comunicación entre dos dispositivos UART, las conexiones deben ser realizadas como indica la figura siguiente:

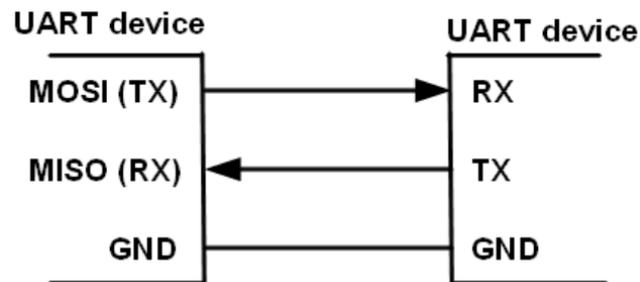


Figura 19: Conexión entre dos dispositivos UART extraída de Geeky Theory (2017).

Para un correcto funcionamiento de los dispositivos, deberán conectarse el punto de transmisión del primer dispositivo con el punto de recepción del segundo y viceversa, además de conectar cada tierra, respectivamente. En este proyecto, este tipo de comunicación se utilizará para poder lograr el intercambio de información entre el Arduino UNO, con el módulo GSM/GPRS, SIM808.

2.3.2 Comandos AT

Los comandos AT, abreviados de la palabra en inglés “Attention”, conforman un lenguaje que en principio fueron utilizados para establecer comunicación únicamente con los módems inalámbricos [98], sin embargo, su aplicación se ha extendido a los móviles que cuentan con la tecnología GSM. Este es el caso del módulo GPRS/GSM, SIM808, que, como todos los demás dispositivos de comunicación, trae este conjunto de

instrucciones pre-grabadas en su interior para ejecutar acciones específicas, tales como el envío y recepción de mensajes, además de la realización o recepción de llamadas.

Gracias a la integración de estas instrucciones, las rutinas de los programas son acortadas, lo cual aumenta la efectividad en el funcionamiento del sistema. En este proyecto, los comandos AT hacen posible que tanto la programación como la comunicación entre el SIM808 y el módulo de control (Arduino UNO), tengan una menor complejidad y extensión, lo que resulta de gran importancia, ya que, es lo que hace que este proyecto sea considerado como tecnológico, creativo e innovador. En la (tabla 8) se muestran los principales códigos utilizados en este tipo de tecnología.

Comando	Función
AT	Esta instrucción es usada para comprobar el funcionamiento del SIM808.
AT+CGMI	Este comando sirve para ver el nombre del fabricante.
ATI	Se utiliza para ver la información del producto.
AT+IPR=?	Se usa para preguntar el braud rate en el que opera el SIM.
AT+IPR?	Sirve para preguntar el braud rate actual.
AT+COPS?	Se utiliza para preguntar el nombre de la compañía del SIM.
AT+CGSN	Su función es verificar el IMEI del chip utilizado.
AT+CMGL=ALL	Sirve para ver todos los mensajes que nos han llegado al SIM.
ATD<n>	Es utilizado para realizar llamadas
AT+CMGS=04455	Este código se utiliza para enviar un SMS.
ATA	Se utiliza para contestar una llamada.
ATH	Es usado para colgar una llamada.
AT+CGPS=1	Habilita el uso del GPS.

Tabla 8: Comandos AT utilizados para establecer comunicación con el SIM 808. Obtenido del manual: *Instructivo de comandos AT.*

2.4 Descripción del funcionamiento del sistema de alarma antirrobo de vehículos.

2.4.1 Representación del funcionamiento del sistema de alarma antirrobo de vehículos.

Para garantizar el funcionamiento correcto del sistema, es preciso el cumplimiento de una serie de procedimientos que hacen posible la realización de las funciones en el mismo, a través del constante análisis del estado de los módulos, sensores y accesorios del vehículo que forman parte del mismo. El funcionamiento del sistema se ilustra a continuación en el diagrama de flujo contenido en la (figura 20).

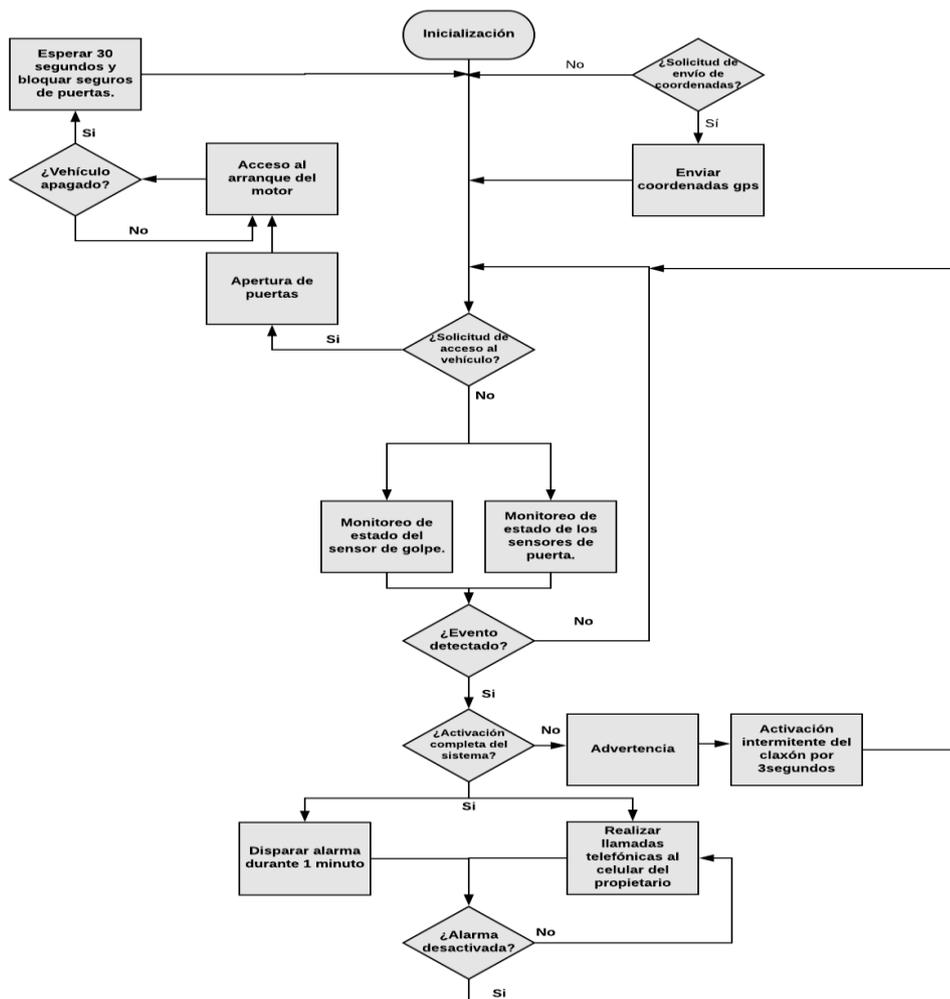


Figura 20: Representación del funcionamiento del sistema de alarma en general mediante un diagrama de flujo. *Herramienta de diseño: Lucidchart.*

2.4.2 Representación rutinas de operación entre el control de mando y el Módulo de Bluetooth HC-06.

En este esquema se representa la forma de operación existente entre el control de mando (teléfono móvil) y los accesorios del vehículo, los cuales son controlados a través de una aplicación (APK), diseñada con una interfaz amigable para el buen manejo por parte del usuario. A continuación, se presenta el diagrama de flujo:

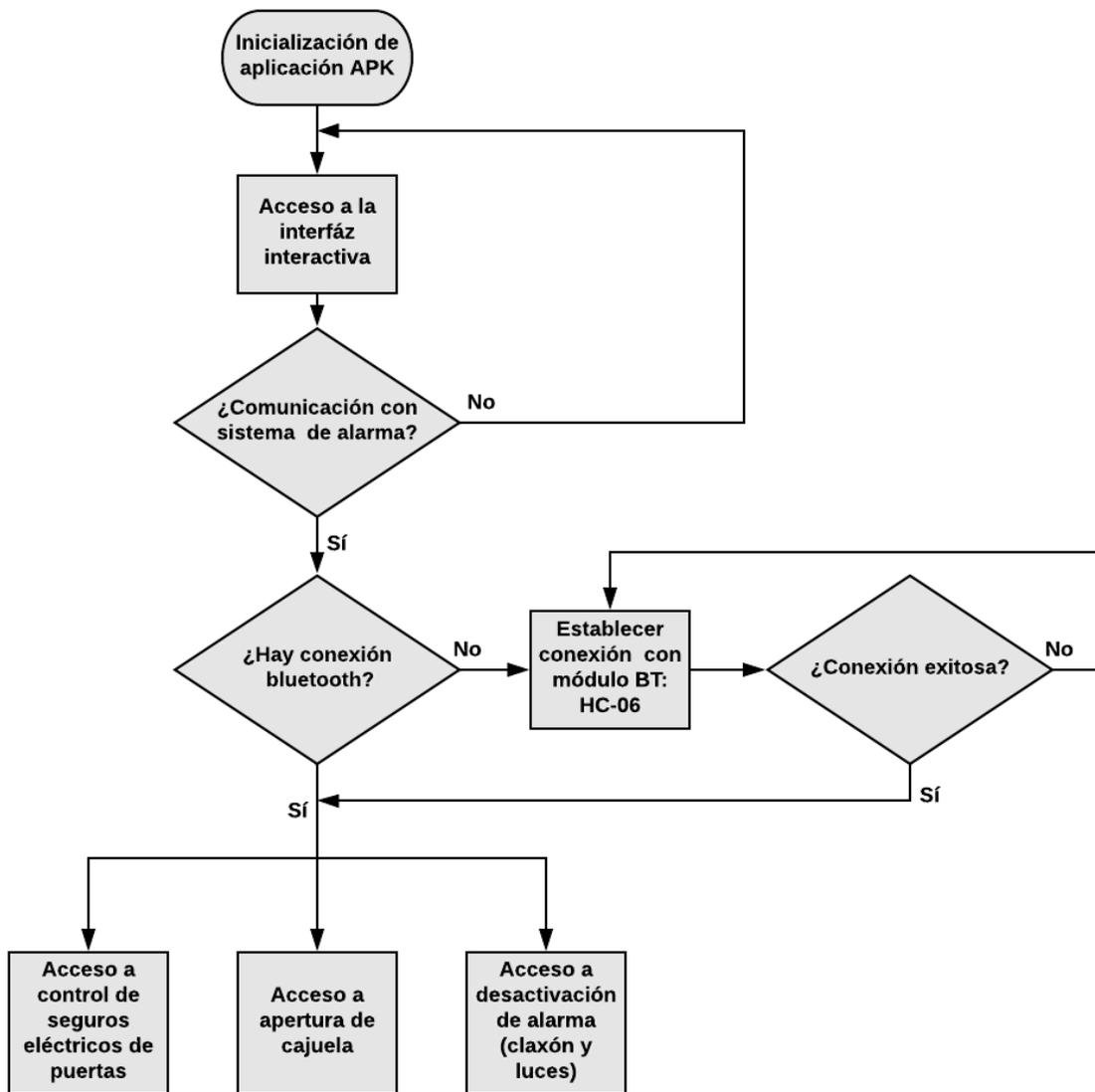


Figura 21: Representación del funcionamiento entre el control de mando y el módulo de Bluetooth para el acceso, a través de una aplicación APK para teléfonos inteligentes. *Herramienta de diseño: Lucidchart.*

2.4.3 Representación pictórica de las conexiones del prototipo del sistema SAIRF.

El diseño del sistema de alarma antirrobo de vehículos se divide en dos partes fundamentales: la parte de accesibilidad y control, y la parte de asistencia GSM-GPRS. La primera está compuesta por el módulo de control, ARDUINO UNO (A), por el módulo Bluetooth (HC-06), la aplicación móvil (APK), el teléfono inteligente, los accesorios del automóvil y el sensor de golpe (AUTOVOX AS-9492). Su función principal consiste en la manipulación de los periféricos del vehículo, así como la desactivación del claxon cuando sea disparado por el sistema, además de controlar la apertura o cierre de los seguros eléctricos del automóvil.

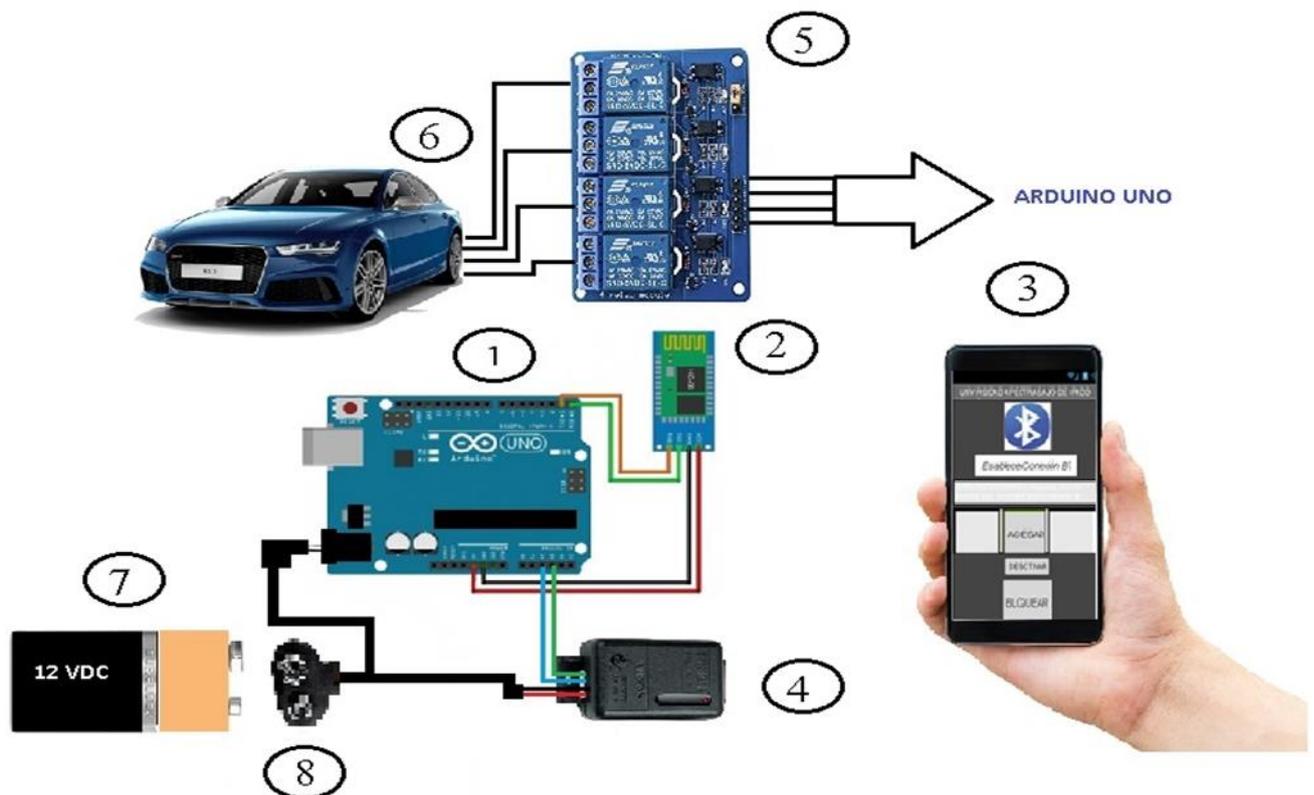


Figura 22. Diagrama pictórico sobre la fase de accesibilidad y control. Imágenes de los dispositivos obtenidas de google.com.do. Herramienta de diseño: Paint

Según se puede observar en la figura 22, las partes que complementan la fase de accesibilidad y control del sistema son:

1. **Arduino UNO (A).** Se encarga de procesar los datos que recibe del módulo de Bluetooth y del sensor de golpe para controlar los accesorios del vehículo mediante los relés.
2. **Módulo Bluetooth HC-06.** Se utiliza para recibir las informaciones enviadas por el teléfono móvil y transmitir las al Arduino UNO.
3. **Teléfono móvil.** Es usado para controlar los accesorios del vehículo mediante una aplicación (APK), que se comunica con el módulo HC-06 vía Bluetooth.
4. **Sensor de Golpe AS-9492.** Se encarga de enviar una señal de aviso al Arduino UNO cuando este recibe vibraciones producidas por golpes en el vehículo o por contacto directo con el mismo.
5. **Juego de relés.** Sirven para activar o desactivar los seguros eléctricos del vehículo, las luces, el claxon y el acceso al encendido del motor.
6. **Vehículo.** Artefacto protegido.
7. **Batería.** Es de vital importancia para el funcionamiento del sistema.
8. **Conector de baterías.** Sirve para fijar la conexión de la batería al sistema.

La segunda parte está formada por el módulo GSM-GPRS (SIM808) y el ARDUINO UNO (B). Esta fase consiste en la realización de llamadas telefónicas en caso de la activación de la alarma, además del envío de coordenadas geográficas. La figura 23 representa el diagrama correspondiente a esta fase.

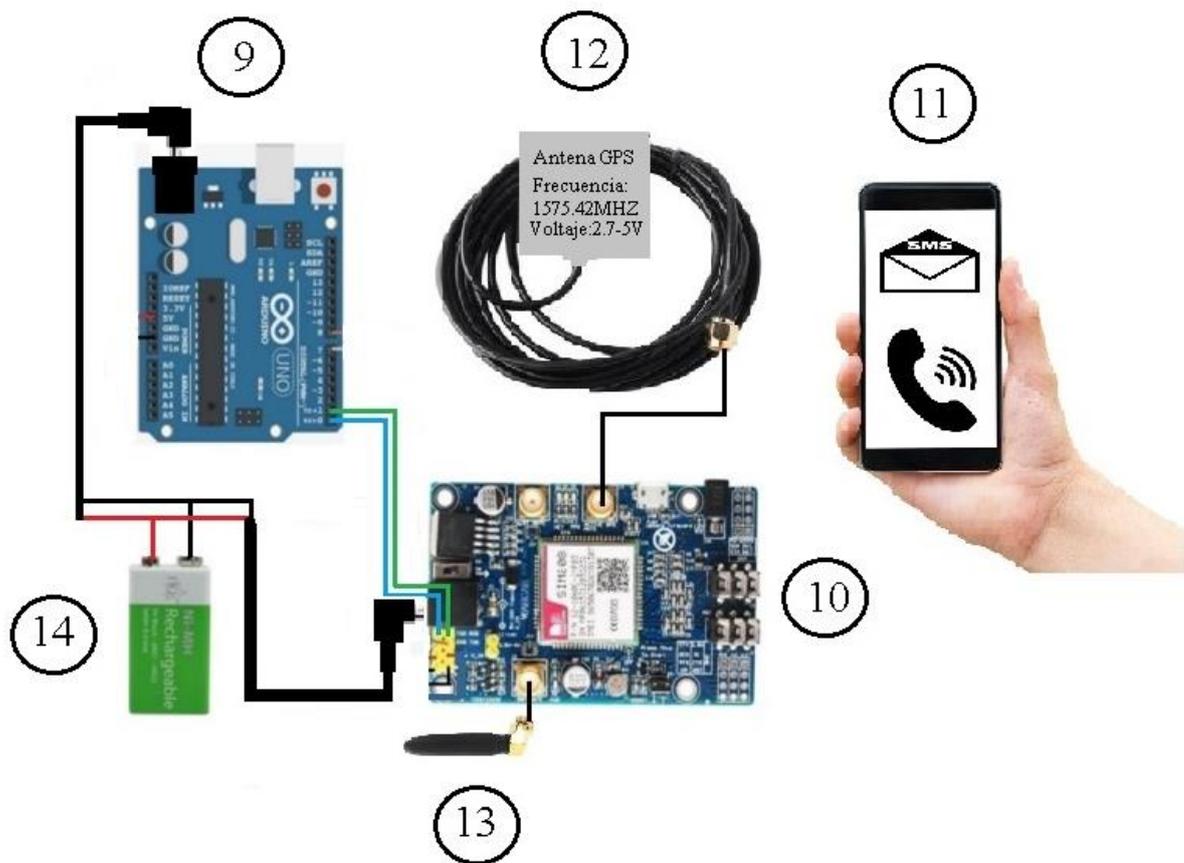


Figura 23. Representación pictórica de la etapa de asistencia GPS-GPRS. Imágenes de los dispositivos obtenidas de google.com.do. Herramienta de diseño: Paint.

La etapa de asistencia GPS-GPRS está formada por los siguientes componentes:

9. **Arduino UNO (B):** Se encarga del procesamiento de solicitudes y del envío de informaciones con el SIM808 mediante conexión entre sus puertos UART (serial).
10. **SIM808:** Se encarga de realizar llamadas al teléfono celular del propietario y recibir mensajes desde el mismo, así como también, del envío de coordenadas geográficas.
11. **Teléfono móvil:** Utilizado para poder visualizar las llamadas de alertas del sistema de alarma y para la comunicación con el SAIRF mediante SMS.

12. **Antena GPS:** Permite al módulo leer las señales satelitales para así obtener las coordenadas geográficas.

13. **Antena GSM:** Hace posible al SIM808 establecer conexión con la red móvil.

14. **Batería:** Es de vital importancia para el funcionamiento del sistema.

2.5 Programas fundamentales para el funcionamiento del SAIRF.

Para el cumplimiento de las expectativas de este proyecto, es indispensable la realización de un conjunto de programas que sirven para el correcto funcionamiento de todas las partes del diseño SAIRF. Los códigos fueron elaborados en la plataforma de Arduino, logrando así la comunicación entre cada uno de los módulos que forman parte del sistema. Los programas presentados en este apartado no son los códigos completos pertenecientes al sistema en general. Más bien, estos son una representación a las dos fases en las que se divide el SAIRF.

2.5.1 Códigos para la fase de accesibilidad y control.

```
//UNAPEC
//TRABAJO DE GRADO
//TEMA: "PROPUESTA DE DISEÑO DE UN SISTEMA DE ALARMA INTELIGENTE PARA PREVENIR ROBOS DE VEHICULOS
//UTILIZANDO EL SISTEMA GLOBAL DE LAS COMUNICACIONES MÓVILES Y GEOLOCALIZACIÓN
//EN LA REPUBLICA DOMINICANA (2018)"
//AUTORES: ROBERT A. PEREZ Y LUIS S. PUJOLS

//DECLARACION DE PINES:
const int SegurosElectricos=13; //1)
const int ClaxonLuces=12; //2)
const int AbrirBaul=8; //3)
const int ActivacionAlarma = 7; //4)
int estado=0; //5)

//Comentarios:
// 1) Esta intrucción sirve para declarar el pin 13 del ARDUINO UNO como "Seguros/Eléctricos"
// 2) Esta intrucción sirve para declarar el pin 12 del ARDUINO UNO como "Claxon/Luces"
// 3) Esta intrucción sirve para declarar el pin 8 del ARDUINO UNO como "Abrir/Baúl"
// 4) Esta intrucción sirve para declarar el pin 7 del arduino como "ActivaciónAlarma"
// 5) Esta intrucción sirve para igualar el "estado" a Cero(0) para el arranque del programa.

//DECLARACIONES DE ENTRADAS Y SALIDAS:
```

```

void setup() {

    Serial.begin(9600);           //6)
    pinMode(SegurosElectricos,OUTPUT); //7)
    pinMode(ClaxonLuces, OUTPUT); //8)
    pinMode(AbrirBaul, OUTPUT); //9)
    pinMode(ActivacionAlarma,INPUT); //10)
    digitalWrite(ClaxonLuces,HIGH); //11)
    digitalWrite(SegurosElectricos,HIGH); //12)
    digitalWrite(AbrirBaul,HIGH); //13)
}

//6) Es usado para arrancar la transmisión de datos.
// 7) "SegurosElectricos" declarado como salida.
// 8) "ClaxonLuces" declarado como salida.
// 9) "AbrirBaul" declarado como salida.
// 10) "ActivacinAlarma" declarado como entrada.
// 11) Este pin se coloca *inicialmente* en uno lógico.
// 12) Este pin se coloca *inicialmente* en uno lógico.
// 13) Este pin se coloca *inicialmente* en uno lógico.
//Nota: "Los relés utilizados en este proyecto son activados con *LOW* o Cero lógico"

//Inicio de programación
void loop(){

    if(Serial.available()>0){
        estado = Serial.read(); //Función para que el módulo bluetooth reciba los datos enviados desde el celular.
    }
    if (estado == '1'){ //Si se pulsa el primer botón en la aplicación móvil, el arduino recibe '1'.
        digitalWrite(SegurosElectricos,HIGH);
        estado = '0';
    }
    if(estado=='2'){ //Si se pulsa el primer botón en la aplicación móvil, el arduino recibe '2'.
        digitalWrite(SegurosElectricos,LOW);
        estado = '0';
    }
    if(estado=='3'){ //Si se pulsa el primer botón en la aplicación móvil, el arduino recibe '3'.
        digitalWrite (ClaxonLuces,HIGH); //Sirve para desactivar el claxon en caso de que se active.
        estado = '0'; //Sirve para estabilizar el sistema.
    }
    if(estado=='4'){ //Si se pulsa el primer botón en la aplicación móvil, el arduino recibe '4'.
        digitalWrite(AbrirBaul,LOW); //Abrir baúl.
        delay (1000); // Durar 1 segundo activado.
        digitalWrite(AbrirBaul,HIGH); //Desactivar apertura de baúl.
        estado = '0'; //Sirve para estabilizar el sistema.
    }
}

```

```

if (digitalRead (ActivacionAlarma)){ //En esta parte se monitorea el pin 7 del arduino (sensores de puerta)
  delay(100);           // para activar la alarma en caso de abrir una puerta cuando el sistema
  digitalWrite(ClaxonLuces,LOW); // se encuentre activado
  estado = '0';
}

```

Estos códigos son utilizados para hacer funcionar la etapa de accesibilidad y control. Estos son cargados al Arduino UNO (A) y haciendo las respectivas conexiones de lugar entre los accesorios del vehículo, el módulo HC-06, el sensor de golpe y la tarjeta controladora, esta fase funciona de forma correcta. La construcción de este programa está bajo nuestra absoluta responsabilidad.

2.5.2 Códigos para la fase de asistencia GSM-GPRS.

2.5.3 Realización de llamada telefónica.

```

//UNAPEC
//TRABAJO DE GRADO
//TEMA: "PROPUESTA DE DISEÑO DE UN SISTEMA DE ALARMA INTELIGENTE PARA PREVENIR ROBOS DE VEHICULOS
//UTILIZANDO EL SISTEMA GLOBAL DE LAS COMUNICACIONES MÓVILES Y GEOLOCALIZACIÓN
//EN LA REPUBLICA DOMINICANA (2018)"
//Sustentantes: ROBERT A. PEREZ Y LUIS S. PUJOLS

```

```

#include <DFRobot_sim808.h>
#include <SoftwareSerial.h>
#define PHONE_NUMBER "*****"
#define puerta 8
#define MESSAGE_LENGTH 5
char message[MESSAGE_LENGTH];
int messageIndex = 0;
char datetime[24];
char phone[16];
DFRobot_SIM808 sim808(&Serial);

```

```

void setup() {
  pinMode(salida_1, OUTPUT);
  pinMode(puerta, INPUT);
  digitalWrite(salida_1, LOW);
  Serial.begin(9600);
  //Inicialización del SIM808
  while(!sim808.init()) {
    delay(1000);
    Serial.print("Error de inicialización");
  }
  Serial.println("Inicialización completada");
}
void loop(){

  if(digitalRead(puerta)){
    Serial.print("llamando\n");
    delay(200);
    call();
  }

  void call(){
    sim808.callUp(PHONE_NUMBER);
    delay(15000);
    sim808.hangup();

  }
}

```

Este es el código utilizado para realizar la llamada de aviso al teléfono del propietario cuando la llamada del vehículo sea activada . Este código [99] fue tomado de la librería de arduino y modificado a nuestra conveniencia para poder llegar a cumplir con las metas propuestas.

2.5.4 Lectura de mensaje y envío de coordenadas.

El programa que se presenta a continuación es el que se utiliza para poder obtener la ubicación geográfica del vehículo. Para la elaboración del mismo, se modificó la librería del Arduino para poder hacer este programa que funcione luego de que se produzca una condición.

```

void setup() {
  //mySerial.begin(9600);
  Serial.begin(9600);

  while(!sim808.init()) {
    delay(1000);
    Serial.print("Error de inicialización");
  }
  if( sim808.attachGPS()){
    Serial.println("Activación de GPS");
    Serial.println("Enviar mensaje para envío de coordenadas" );
  }
  else {
    Serial.println("Error activando GPS");
  }
}

Serial.print("latitude :");
Serial.println(sim808.GPSdata.lat,6);

sim808.latitudeConverToDMS(); //Función para convertir las coordenadas en polar y decimal.
Serial.print("latitude :");
Serial.print(sim808.latDMS.degrees);
Serial.print("\^");
Serial.print(sim808.latDMS.minutes);
Serial.print("\'");
Serial.print(sim808.latDMS.seconeds,6);
Serial.println("\");
Serial.print("longitude :");
Serial.println(sim808.GPSdata.lon,6);
sim808.LongitudeConverToDMS();
Serial.print("longitude :");
Serial.print(sim808.longDMS.degrees);
Serial.print("\^");
Serial.print(sim808.longDMS.minutes);
Serial.print("\'");

void loop() {
  //Función para detectar mensajes no leídos
  messageIndex = sim808.isSMSunread();
  //Serial.print("messageIndex: ");
  //Serial.println(messageIndex);

  //Mensaje no leído encontrado.
  if (messageIndex > 0) {
    leer_sms();
  }
}

void gps_data(){
  while( a == 1){
  if (sim808.getGPS()) {
    a = 0;
  }
}
}

```

```

Serial.print(sim808.GPSdata.year);
Serial.print("/");
Serial.print(sim808.GPSdata.month);
Serial.print("/");
Serial.print(sim808.GPSdata.day);
Serial.print(" ");
Serial.print(sim808.GPSdata.hour);
Serial.print(":");
Serial.print(sim808.GPSdata.minute);
Serial.print(":");
Serial.print(sim808.GPSdata.second);
Serial.print(":");
Serial.println(sim808.GPSdata.centisecond);

Serial.print(sim808.longDMS.seconeds,6);
Serial.println("\");

Serial.print("speed_kph :");
Serial.println(sim808.GPSdata.speed_kph);
Serial.print("heading :");
Serial.println(sim808.GPSdata.heading);

sim808.detachGPS(); //Apagar GPS
}
}
}

void leer_sms(){
a = 1;
sim808.readSMS(messageIndex, message, MESSAGE_LENGTH, phone, datetime);
//*****In order not to full SIM Memory, is better to delete it*****
sim808.deleteSMS(messageIndex);
Serial.print("From number: ");
Serial.println(phone);
Serial.print("Datetime: ");
Serial.println(datetime);
Serial.print("Mensaje recibido:");
Serial.println(message);
if(message[0]=='G' && message[1]=='p' && message[2]=='s'){
Serial.println("*****_Obteniendo datos GPS___*****");
gps_data();
}
}
}

```

3. CONTRASTE Y VERIFICACION DEL DISEÑO.

3.1 Resultados

3.1.1 Alimentación del sistema para pruebas de funcionamiento.

Para fines de pruebas de funcionamiento de este proyecto, se utilizaron las siguientes fuentes de alimentación:

- Una computadora Laptop para los Arduino UNO (A y B), conectados vía cable USB, el mismo cable utilizado para cargar los programas en esta tarjeta.
- Una fuente 12VDC/2Amperes, para el módulo GPS-GSM/GPRS, SIM808. Los demás módulos eran alimentados a través del Arduino UNO.

Aunque estos fueron los tipos de fuentes usados en las pruebas de funcionamiento, no son las correspondientes al diseño final, ya que, aparte de lograr el funcionamiento esperado por parte del sistema, se pretende también implementar un sistema portátil que no dependa completamente de la batería del vehículo, mediante la aplicación de baterías pequeñas con las características correspondientes para un funcionamiento duradero.

3.1.2 Prueba funcional del sistema.

3.1.2.1 Presentación de conexiones y hardware.

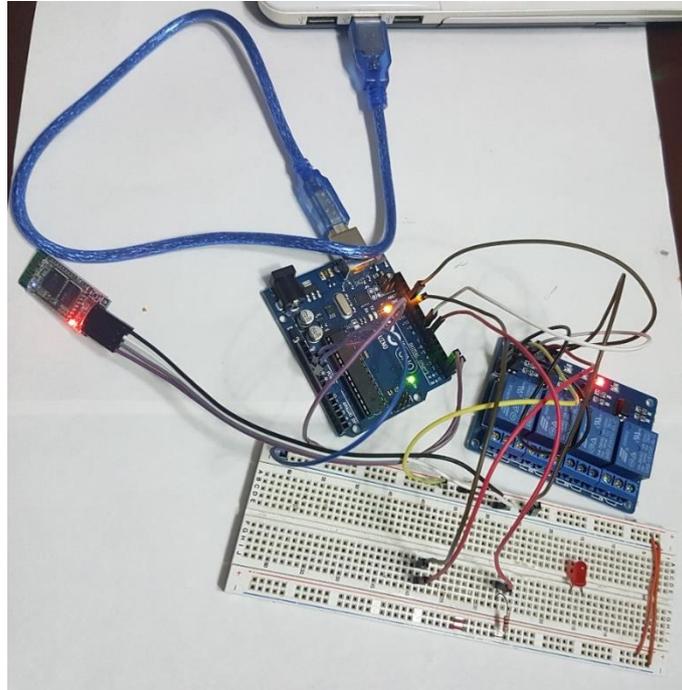


Figura 24. Conexiones correspondientes para la comunicación con la fase de accesibilidad y control del SAIRF.

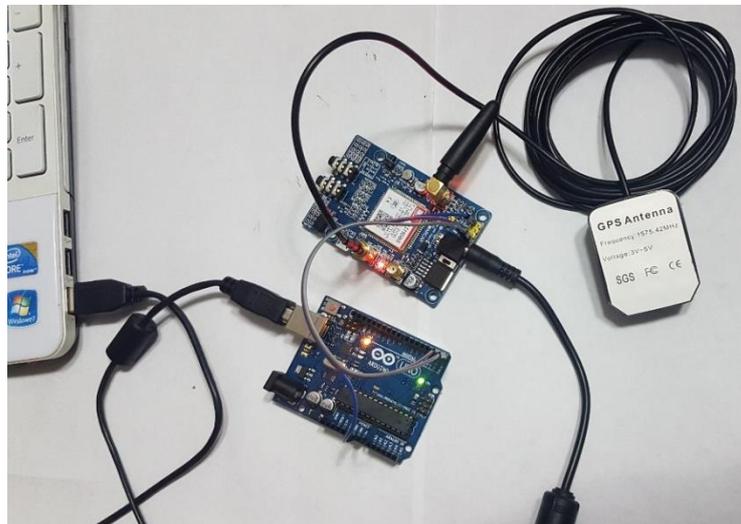


Figura 25. Conexiones correspondientes para la comunicación con la fase de asistencia GPS-GPRS.

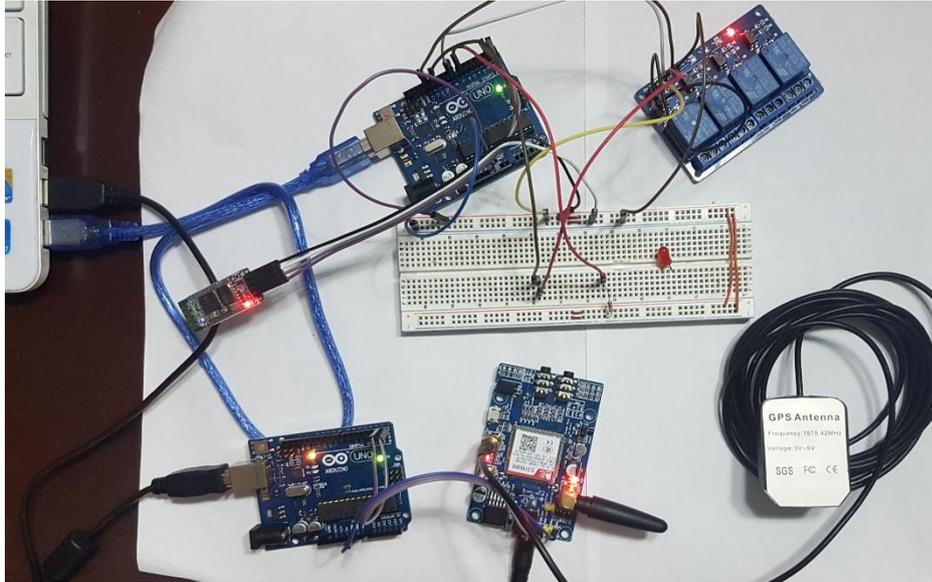


Figura 26. Conexión completa del SAIRF.

3.2 Aplicación móvil.

Para la elaboración de la aplicación móvil que controla el acceso-bloqueo de los seguros eléctricos del vehículo, la apertura de la cajuela y la desactivación de la corneta y luces fue preciso el diseño tanto de la estructura externa (interfaz), como de la estructura interior de la misma. Ambas partes del diseño de la misma se explican en los apartados 3.2.1 y 3.2.1.1.

3.2.1 Diseño de la interfaz APK.

El diseño de la interfaz de la aplicación para la fase de accesibilidad y control fue desarrollado en MIT APP INVENTOR. Este es un entorno de desarrollo de software que pertenece a la empresa GOOGLE, el cual brinda facilidades a cualquier usuario de crear y personalizar aplicaciones para usos específicos [100]. Esta es una página de fácil manejo y entendimiento para personas sin experiencias en esta área de la tecnología.



Figura 27. Ilustración de la interfaz de la aplicación para teléfonos inteligentes.

En la figura 27 se muestra el diseño de la interfaz de la aplicación para pruebas de funcionamiento del SAIRF. Este fue completamente diseñado con MIT APP INVENTOR[101].



Figura 28. Apariencia del ícono de la aplicación instalada en un teléfono inteligente.

3.2.2 Diseño interno de la aplicación APK.

El diseño interno de esta aplicación consiste en la interconexión entre pequeños bloques, los cuales hacen posible la comunicación con el sistema de alarma al momento de pulsar uno de los botones diseñados en la interfaz de la aplicación. Cabe destacar que se crea un diagrama en bloques por cada botón que tenga el diseño, otro para hacer que despliegue en la pantalla del celular los nombres de los dispositivos Bluetooth que están a su alrededor, y otro para poder seleccionar uno en específico, en este caso, el módulo HC-06.

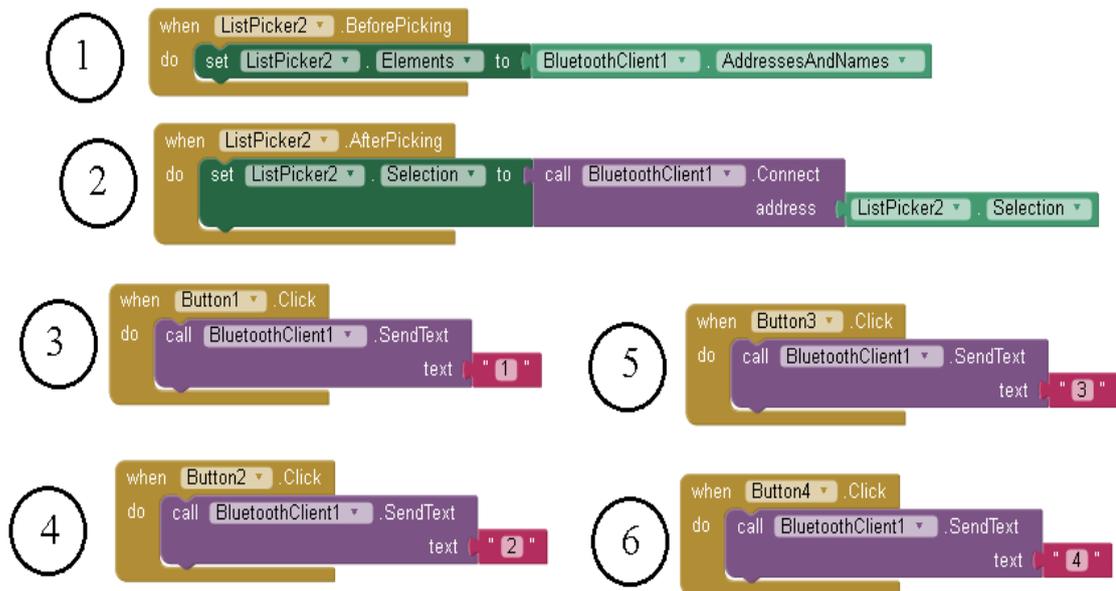


Figura 29. Representación del diseño interno de la aplicación.

La descripción del diseño interno de la aplicación para la accesibilidad y control del SAIRF se explica a continuación:

1. Sirve para el reconocimiento de los dispositivos Bluetooth que se encuentran próximos al teléfono celular.

2. Sirve para poder seleccionar el módulo HC-06, cuyo nombre se despliega en la pantalla al pulsar el boton con el símbolo de Bluetooth.
3. Envía '1' al Arduino UNO cuando se pulsa el boton 1 (SegurosEléctricos). Sirve para desactivar los seguros del vehículo.
4. Envía '2' al Arduino UNO cuando se pulsa el boton 2 (SegurosEléctricos). Sirve para activar los seguros del vehículo.
5. Envía '3' al Arduino UNO cuando se pulsa el boton 3 (ClaxonLuces). Sirve para desactivar las señales sonoras que emite el sistema al ser disparado.
6. Envía '4' al Arduino UNO cuando se pulsa el boton 4 (AbrirBaúl). Sirve para aperturar la cajuela.

3.3 Recepción de ubicación geográfica.

El envío de las coordenadas por parte del módulo SIM808 sucede cuando el mismo recibe un mensaje con las letras "GPS" por parte del propietario. Este envía las coordenadas correspondientes cada vez que se le envía un mensaje. Cabe destacar que cada mensaje enviado por esta tarjeta tiene un costo, por esto el SIM ingresado en la misma debe tener saldo disponible.

Estas pruebas fueron realizadas en lugares cerrados y en lugares abiertos. Como se esperaba, en los lugares cerrados el proceso era más lento que en los sitios abiertos, debido a la limitación de señal existente en los mismos. A continuación, ilustran figuras como ejemplo del funcionamiento:

```
COM6 (Arduino/Genuino Uno)
AT+CMGR=1
AT+CMGD=1Recibido del número: ***** 1915
Fecha: 18/03/23,05:45:45-16
Mensaje recibido: Gps
*****_Obteniendo datos GPS___*****
2018/3/23 9:45:52:0
latitude :18.299295
latitude :18^17'57.463531"
longitude :69.471481
longitude :69^28'17.332763"
speed_kph :0.02
heading :101.16
AT+CGNSPWR=0
AT+CMGF=1
AT+CMGL="REC UNREAD",1
AT+CMGL="REC UNREAD",1
AT+CMGF=1
```

Figura 31. Datos obtenidos en el monitor serial del software Arduino.

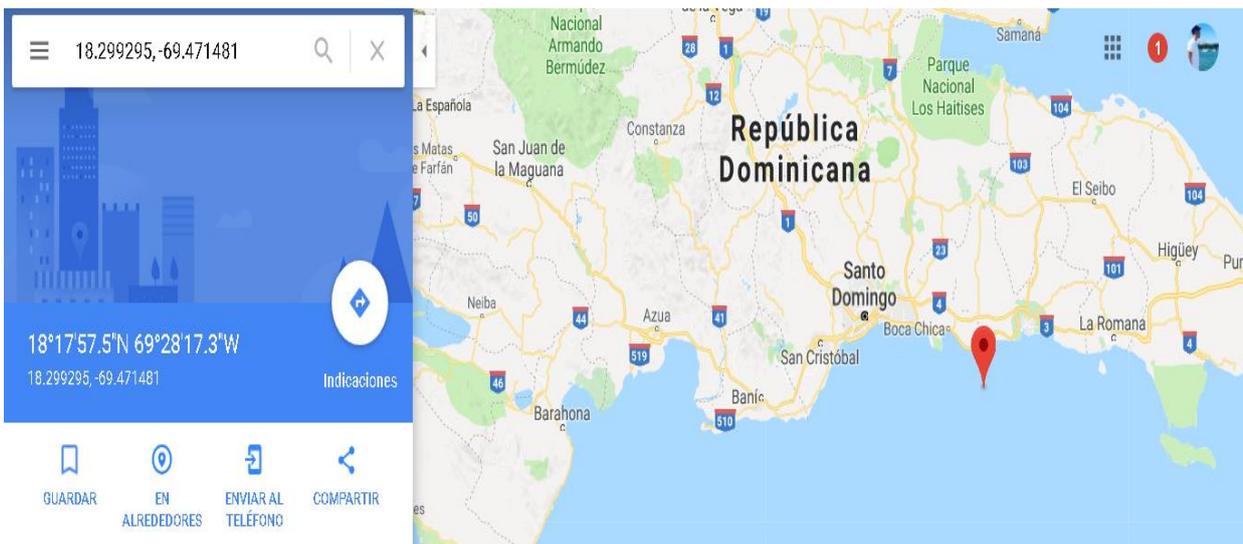


Figura 30. Ubicación en el mapa de google de las coordenadas enviadas por el sistema.

En la figura 31 se colocan las coordenadas dadas por el módulo, mostradas en la figura 30. Al momento del ejemplo de las figuras 30 y 31, las coordenadas exactas de ese lugar eran (18.499102,-69.785822), mientras que el sistema mostraba (18.299295,-

69.471481), lo que significa que el sistema presenta un pequeño margen de diferencia con respecto a las coordenadas reales.

3.4 Factibilidad de la propuesta de diseño

El análisis de factibilidad del proyecto y los beneficios que su implementación le proveerán al usuario se harán tomando en cuenta diferentes parámetros como: las cotizaciones de planes de seguros para Vehículos ofrecidas por el Banco BHD, para un automóvil de la marca Toyota Corolla (2015), con un valor monetario de \$815,000.00 pesos dominicanos. Se hará una comparación entre los gastos de implementación del sistema propuesto (Tabla 12 apéndice C), con los deducibles impuestos por el seguro vehicular del banco BHD en el momento que se reporta un robo total del vehículo. Los montos a pagar anualmente por cada tipo de seguro cotizado por el BHD para el vehículo mencionado serán presentados en (tabla 13 del Apéndice C), incluyendo los montos de los deducible que pagarían los propietarios de este automóvil al ser hurtado.

Los porcentajes de los deducibles que se tomarán en cuenta para desarrollar el análisis de factibilidad, son los que el seguro presenta como pérdida total por robo o hurto del vehículo (figura 32 del apéndice C) exceptuando la pérdida parcial que hace referencia al ultraje de alguna parte del vehículo, pero no su totalidad. Al instalar este sistema antirrobo al Toyota Corolla seleccionado, el propietario del automóvil tendrá la posibilidad de evitar un aumento de su prima de seguro o su coste, ya que tendrá la posibilidad de acceder a la aplicación instalada en su teléfono móvil diseñada exclusivamente para el sistema propuesto y obtener la ubicación del vehículo en tiempo real. Conociendo esta información el propietario puede obviar el pago del deducible a la aseguradora, donde el monto mínimo a pagar para este auto es de RD\$8,150 pesos que le

corresponde al paquete Trebol clásico (Tabla 12 apéndice c). El dueño del vehículo al utilizar esta tecnología al costo de RD\$ 6,197.20 pesos, se estaría ahorrando el valor de RD\$1,952.80 pesos cada vez que este automóvil sea robado, pudiendo obtener ahorros progresivamente mayores dependiendo de planes más avanzados y costosos del seguro vehicular que optaría en caso de no tener el sistema antirrobo.

CONCLUSIONES

En este trabajo de tres capítulos, se ha logrado compactar el desarrollo lógico de un sistema electrónico de alarma contra robo, que responde a situaciones reales y de carácter puntual, el cual es dirigido a aquellas personas interesadas en el monitoreo y protección de su vehículo propio. Su estructura ha sido formada mediante la implementación módulos de comunicación inalámbrica, como el SIM808 y el HC-06, así como también dispositivos de control (Arduino UNO), que han generado resultados adecuados. Es gracias a la implementación de estas tecnologías la creación funcional del prototipo de este proyecto.

Tras hacer las correspondientes pruebas de funcionamiento del SAIRF, se pudo llegar a las siguientes conclusiones:

- La interfaz de accesibilidad y control diseñada para teléfonos inteligentes permite la interacción entre los usuarios y el sistema por medio de una aplicación amigable y sencilla de usar.
- El programa de la plataforma Arduino que controla el módulo SIM808, se mantiene realizando llamadas de alerta al teléfono personal del propietario mientras el sistema de alarma permanece encendido. Este número de destino puede ser editado en cualquier momento con solo hacer modificaciones en este programa. Es capaz de reconocer un mensaje de texto específico como condición para el envío de las coordenadas geográficas en las que se encuentra el vehículo.
- Todos los componentes y módulos se integran para en conjunto, cumplir con el funcionamiento de un sistema de alarma inteligente antirrobo de vehículos implementando el uso de las comunicaciones móviles y geolocalización

RECOMENDACIONES

1. Añadir a este sistema de protección el uso cámaras en el vehículo, compatibles con Arduino, para almacenar videos en la nube de DROPBOX y monitorear el estatus del automóvil mediante conexión WIFI.
2. Implementar el uso de antenas de mayor capacidad para aumentar la velocidad en el intercambio de informaciones entre el sistema y el teléfono móvil.
3. Implementar en la interfaz de accesibilidad y control un sistema de registro para las personas, el cual cuente con una contraseña única para cada usuario.
4. Buscar más cotizaciones sobre diferentes aseguradoras de vehículos para hacer comparaciones sobre los deducibles y cuanto se podrian ahorrar por cada robo dependiendo el plan adquirido por el propietario del vehiculo.

REFERENCIAS BIBLIOGRAFICAS

[1] DGII. (2017). *Parque vehicular de RD creció 6.7 % en 2016*. Periódico Hoy.

URL: <http://hoy.com.do/parque-vehicular-de-rd-crecio-6-7-en-2016/>

[2] Oficina Nacional de Estadísticas (ONE). (2017). *Cantidad de vehículos registrados por mes, según tipo de vehículo, 2017, enero-noviembre*. República Dominicana.

[3], [4] y [5] Departamento de Información y Estadísticas. (2017). *Vehículos Robados Por Provincias 2017*. Policía Nacional.

URL:http://www.policianacional.gob.do/wp-content/uploads/2017/02/Vehiculos_robados_por_provincia_1er_trimestre_2017.pdf

[6], [7], [8], [9], [10] y [11] El Economista. (2016). *Los cinco mejores sistemas antirrobo para proteger el coche*.

URL: <http://www.economista.es/ecomotor/motor/noticias/7647531/06/16/Los-cinco-mejores-sistemas-antirrobo-para-el-coche.html>

[12], [13] y [14] Megane, D. (2016). *Inmovilizador electrónico*. Aficionados a la mecánica.

URL: <http://www.aficionadosalamecanica.com/inmovilizador.htm>

[15] Perez, J. & Gardey, A. (2013). *Definición de Alarma*.

URL: <https://definicion.de/alarma/>

[16] Admin., (20¹²). *Tipos de Alarmas de Coches*. Guías Prácticas.

URL: <http://www.guiaspracticass.com/alarmas-de-coche/tipos-de-alarmas-de-coche>

[17], [18], [19], [20], [21] y [22] Bremicker, A. (2012). *Historia de los Sistemas de Alarmas*.

URL:<https://www.abus.com/es/Guia/Proteccion-antirrobo/Sistemas-de-alarma/Historia-de-los-sistemas-de-alarma>

[23], [28], [29], [30], [31] y [32] Auto Alarmas. *Componentes básicos en un sistema de seguridad inalámbrico para tu vehículo.*

URL: <https://autoalarmas.wordpress.com/>

[24], [25], [26] y [27] Nemesis, CAR SECURITY SYSTEM. Pdf manual.

URL: http://nemesisla.com/descargas/Nemesis_UG_Alarma_GT-4.pdf

[33] Camargo, J. (2009). *Modelo de Cobertura Para Redes Inalámbricas de Interiores.* Escuela Superior de Ingenieros de Sevilla.

URL: <http://bibing.us.es/proyectos/abreproy/11761/direccion/>

(34) Camargo, J. (2009). *Modelo de Cobertura Para Redes Inalámbricas de Interiores.* Escuela Superior de Ingenieros de Sevilla.

URL: <http://bibing.us.es/proyectos/abreproy/11761/direccion/>

[35] Fernández. N. (2006). *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.* Universidad De Oviedo. España. 12.

URL: <http://di002.edv.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

[36] Fernández. N. (2006). *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.* Universidad De Oviedo. España. 12.

URL: <http://di002.edv.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

[37] Fernández. N. (2006). *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.* Universidad De Oviedo. España. 12.

URL: <http://di002.edv.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

[38] Fernández. N. (2006). *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.* Universidad De Oviedo. España. 12.

URL: <http://di002.edv.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

[39] Fernández. N. (2006). *Modelo de cobertura en redes inalámbricas basado en radiosidad por refinamiento progresivo.* Universidad De Oviedo. España. 12.

URL: <http://di002.edv.uniovi.es/~cueva/investigacion/tesis/Nestor.pdf>

[40] Torres, A. (2007). *Mejora de los sistemas de cartografía del territorio colombiano*. IGAC. Colombia. 104.

URL: <http://cia.corantioquia.gov.co/cgi-bin/koha/opac-detail.pl?biblionumber=11900>

[41] Torres, A. (2007). *Mejora de los sistemas de cartografía del territorio colombiano*. IGAC. Colombia. 104.

URL: <http://cia.corantioquia.gov.co/cgi-bin/koha/opac-detail.pl?biblionumber=11900>

[42] Torres, A. (2007). *Mejora de los sistemas de cartografía del territorio colombiano*. IGAC. Colombia. 104.

URL: <http://cia.corantioquia.gov.co/cgi-bin/koha/opac-detail.pl?biblionumber=11900>

[43] Clark, R. (2012). *Modeling Water Quality in Distribution Systems*. 2nd Edición. American Water Works Association. Denver, Colorado.

URL: <https://app.knovel.com/hotlink/toc/id:kpMWQDSE02/modeling-water-quality/modeling-water-quality>

[44] Pistoia, G. (2009). *Battery Operated Devices and Systems*. Amsterdam: Elsevier.

URL: <https://app.knovel.com/hotlink/toc/id:kpBODSFPE1/battery-operated-devices/battery-operated-devices>

[45] Pozo, A., Ribeiro, A., y Sandoval, F. (2000). *Sistema de posicionamiento global (gps): descripción, análisis de errores, aplicaciones y futuro*. Instituto de Automática Industrial. Madrid, España.

URL: www.peoplematters.com/Archivos/Descargas/GPS.pdf

[46] Pozo, A., Ribeiro, A., & Sandoval, F. (2000). *Sistema de posicionamiento global (gps): descripción, análisis de errores, aplicaciones y futuro*. Instituto de Automática Industrial. España.

URL: www.peoplematters.com/Archivos/Descargas/GPS.pdf

[47] Torres, A. 2007. *Mejora de los Sistemas de Cartografía del Territorio Colombiano*. IGAC. Colombia. 104.

URL: <http://cia.corantioquia.gov.co/cgi-bin/koha/opac-detail.pl?biblionumber=11900>

[48] Pozo, A., Ribeiro, A., & Sandoval, F. (2000). *Sistema de posicionamiento global (gps): descripción, análisis de errores, aplicaciones y futuro*. Instituto de Automática Industrial. España.

URL: www.peoplesmatters.com/Archivos/Descargas/GPS.pdf

[49] Hernando J., Mendo L., & Riera J. (2015). *Comunicaciones móviles*. Universitaria Ramón Areces. España. 31-32.

URL:

<https://books.google.es/books?hl=en&lr=&id=lnqnDAAAQBAJ&oi=fnd&pg=PA21&dq=sistema+global+para+las+comunicaciones+m%C3%B3viles&ots=LmmP5ZAHrv&sig=fW5PPeKQqheBXDDE4QMRH1sGYFs#v=onepage&q=sistema%20global%20para%20las%20comunicaciones%20m%C3%B3viles&f=false>

[50] Grandes, R. (2011). *Sistema de Control Inalámbrico con Tecnología GSM, Para Optimizar el Tiempo de Configuración de Pantallas LEDS en la Empresa Trans Veloz*. Universidad Técnica de Ambato. Ecuador. 28-29.

URL: http://repo.uta.edu.ec/bitstream/123456789/429/1/Tesis_t636ec.pdf

[51] The 3rd Generation Partnership Project. (2011). *UMTS Forum Report 44*. Suiza.

URL:

http://www.umtsforum.org/component/option,com_docman/task,cat_view/gid,485/Itemid,213/

[52] Chabla, B., & Danilo, R. (2016). *Tesis Diseño e implementación de un sistema completo de seguridad que contempla video vigilancia móvil y posicionamiento global GPS en tiempo real, con monitoreo remoto para vehículos blindados de transporte de valores*. Universidad de las Fuerzas Armadas ESPE. Ecuador.

URL: <http://repositorio.espe.edu.ec/handle/21000/11524>

[53] Reyes, J., & Huertas, M. (2014). *Tesis diseño e implementación de un módulo de alarma para el monitoreo y control de del vehículo a través de GSM y GPS*. Universidad de las Fuerzas Armadas ESPE. Ecuador.

Url: <http://repositorio.espe.edu.ec/handle/21000/9270>

[54] Rohde & Schwarz. (2015). *Principios básicos de GSM, GPRS y EDGE Evolution*. España.

URL: https://www.rohde-schwarz.com/es/soluciones/comunicaciones-inalambricas/gsm-gprs-edge-evolution-vamos/fundamentos/principios-basicos-de-gsm_106328.html

[55] Gasca, M., Camargo, L., & Medina, B. (2014). *Metodología para el desarrollo de aplicaciones móviles*. Tecnura, 18 (40), 20-35.

URL: <http://www.redalyc.org/html/2570/257030546003/>

[56] Del Valle, A. (2015). *Diseño, Integración y Optimización de Estaciones Base de Segunda Generación*. Escuela Técnica Superior de Ingeniería. España. 29.

URL:

<http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%C3%8DTULO+3++FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

[57] Gorriacho, J., & Gorriacho, M. (2004). *Comunicaciones Móviles*. Universitat Politècnica de Catalunya. España.

URL:

<http://upcommons.upc.edu/bitstream/handle/2099.3/36642/9788498800531.pdf?sequence=1&isAllowed=n>

[58] Chuquitarco, M., & Naranjo, R. (2012). *Diseño e instalación de un sistema de rastreo satelital mediante GPS y GPRS al vehículo Chevrolet-Aveo*. Universidad de las Fuerzas Armadas ESPE. Ecuador.

URL: <http://repositorio.espe.edu.ec/handle/21000/5879>

[59] Chabla B. & Danilo R. (2016). *Tesis Diseño e implementación de un sistema completo de seguridad que contempla vídeo vigilancia móvil y posicionamiento global GPS en tiempo real, con monitoreo remoto para vehículos blindados de transporte de valores*. Universidad de las Fuerzas Armadas ESPE. Ecuador.

URL: <http://repositorio.espe.edu.ec/handle/21000/11524>.

[60] Maeso, A., & Trillo, M. (1999) *Radiaciones Rf de Antenas de Telefonía Móvil y salud pública: El estado actual de la cuestión*. Radio proteccion 20 (7). 24-36.

URL: <https://www.dxmaps.com/docs/protrad.pdf>

[61] Sauter, M. (2011). *From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband*. Wiley. Estados Unidos. 21-22.

URL: https://aliazizjasem.files.wordpress.com/2012/01/mobile_networks2.pdf

[62] Del Valle, A. (2015). *Diseño, Integración y Optimización de Estaciones Base de Segunda Generación*. Escuela Técnica Superior de Ingeniería. España. 36-38.

URL: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+2+-+LA+EVOLUCI%D3N+DE+LA+TELEFON%CDA+M%D3VIL%252F2.2+La+evolu+ci%F3n+de+las+redes+de+telefon%EDA.pdf>

[63] Organista, J., McAnally, L., & Lavigne, G. (2013). *El teléfono inteligente (smartphone) como herramienta pedagógica*. Apertura, 5 (1). 6-19.

URL: <http://www.redalyc.org/pdf/688/68830443002.pdf>

[64] European Telecommunications Standards Institute. *ETSI TS 145 005: Digital cellular telecommunications system*. Global System for Mobile Communications. Francia. 14-16.

URL: http://www.etsi.org/deliver/etsi_ts/145000_145099/145005/10.00.00_60/ts_145005v100000p.pdf

[65] Sauter, M. (2006). *Communication Systems for the Mobile Information Society*. Wiley. Estados Unidos. 21-22.

URL:

<https://books.google.com.do/books?id=IZ2KDhn9iOgC&pg=PA21&dq=gsm+table+frequency+band&hl=es-419&sa=X&ved=0ahUKEwjns-bHmfTYAhUEzVMKHRVaB-QQ6AEIJjAA#v=onepage&q=gsm%20table%20frequency%20band&f=false>

[66] Dhanshetti, S. (2011). *Advance Module Communication System*. Industrial Training Institute. India. 154-155.

URL:

<https://books.google.com.do/books?id=HaqiBgAAQBAJ&pg=PA159&dq=subscriber+identity+module&hl=es-419&sa=X&ved=0ahUKEwjg9bzNnfTYAhVE2FMKHbShAbYQ6AEIPzAD#v=onepage&q=subscriber%20identity%20module&f=false>

[67] Reyes, J., Huertas, M. (2014). *Diseño e implementación de un módulo de alarma para el monitoreo y control de del vehículo a través de GSM y GPS*. Universidad de las Fuerzas Armadas ESPE. Ecuador.

URL: <http://repositorio.espe.edu.ec/handle/21000/9270>

[68] Sauter, M. (2011). *From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband*. Wiley, Estados Unidos. 21-22.

URL:

https://aliazizjasem.files.wordpress.com/2012/01/mobile_networks2.pdf

[69] Goleniewski, L., Wilson, K. (2006). *Telecommunications Essentials*. Addison-Wesley Professional. Estados Unidos.

URL: <http://proquestcombo.safaribooksonline.com/book/networking/telecommunications/0321427610>

[70] Del Valle, A. (2011). *Diseño, Integración y Optimización de Estaciones Base de Segunda Generación*. Escuela Superior de Ingenieros de Sevilla. España

. URL: bibing.us.es/proyectos/abreproy/11980/

[71] Del Valle, A. (2011). *Diseño, Integración y Optimización de Estaciones Base de Segunda Generación*. Escuela Superior de Ingenieros de Sevilla. España.

URL: bibing.us.es/proyectos/abreproy/11980/

[72] Del Valle, A. (2011). *Diseño, Integración y Optimización de Estaciones Base de Segunda Generación*. Escuela Superior de Ingenieros de Sevilla. España.

URL: bibing.us.es/proyectos/abreproy/11980/

[73] Zheng, P., Peterson, L., Davie, S., & Farre, A. (2009). *Wireless Networking Complete*. Morgan Kaufmann. Estados Unidos.

URL: <https://www.elsevier.com/books/wireless-networking-complete/zheng/978-0-12-375077-8>

[74] GSM Favorites. (2018). *Introduction to Bluetooth*. ActiveXperts Software. Inglaterra.

URL: <http://www.gsmfavorites.com/documents/bluetooth/introduction/>

[75] Camargo, J. (2009). *Modelo de Cobertura para Redes Inalámbricas de Interiore*. Escuela Superior de Ingenieros de Sevilla. España. 11.

URL: <http://bibing.us.es/proyectos/abreproy/11761/direccion/>

[76] Goleva, R., Ganchev, I., Dobre, C., Garcia, N., & Valderrama, C. (2018). *Enhanced Living Environments - From Models to Technologies*. Institution of Engineering and Technology.

URL: <https://app.knovel.com/hotlink/toc/id:kpELEFMT0G/enhanced-living-environments/enhanced-living-environments>

[77] Garg, V. (2007). *Wireless Communications and Networking*. Elsevier.

URL:

<https://app.knovel.com/hotlink/toc/id:kpWCN00002/wireless-communications-3/wireless-communications-3>

[78], [79], [76] , [81] & [82] Scarfone, K. & Padgett, J. (2017). *Guide to Bluetooth security*. Estados Unidos: National Institute of Standards and Technology. Pp 2-2.

URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf>

[77] Ibarrola, J. (2007). *Tipos de Bluetooth*. Argentina: Alegs.

URL: <http://www.alegsa.com.ar/Notas/166.php>

[78] Hernandez, A., Robleda, J., & Huerta, J. (2018). *Bluetooth y Homerf*. McGraw Hill Education. pp 8.

URL: https://www.mhe.es/cf/ciclos_informatica/844819974X/archivos/unidad5_recurso1.pdf

[79] Gutierrez, D. (2009). *Sistema pasarela Bluetooth para una red de sensores Zigbee*. España: Biblioteca Universidad de Sevilla.

URL:

<http://bibing.us.es/proyectos/abreproy/40048/fichero/VOLUMEN+1.+MEMORIA%252F4.+Tecnolog%C3%ADa+Bluetooth.pdf>

[80] Ibarrola, J. (2007). *Tipos de Bluetooth*. Alegs. Argentina.

URL: <http://www.alegsa.com.ar/Notas/166.php>

[83] Vainio, J. (2000). *Bluetooth Security*. Helsinki University of Technology.

URL: <http://www.yuuhaw.com/bluesec.pdf>

[84] Ortiz N., Vicente A. y Muñoz O. (2016). *Diseño de un sistema electrónico para localizar personas con alzheimer*. (Trabajo de grado) Universidad APEC, República Dominicana.

[85] Domínguez, C., & Mora, M. (2016). *Sistema integral para la reconfiguración dinámica de los Tiempos entre Paradas de una ruta predefinida de transporte público*. Escuela Superior Politécnica del Litoral. Ecuador.

URL: <https://www.dspace.espol.edu.ec/retrieve/97515/D-103448.pdf>

[86] Arduino. (2018). *Introduction: What is Arduino?*. Creative Commons. Estados Unidos.

URL: <https://www.arduino.cc/en/Guide/Introduction>

[87] Ortiz N., Vicente A. y Muñoz O. (2016). *Diseño de un sistema electrónico para localizar personas con alzheimer*. (Trabajo de grado) Universidad APEC, República Dominicana.

[88] Rambal. (2018). *Shield SIM808 GPRS/GSM+GPS*. Rambal Ltda. Chile.

URL: http://rambal.com/index.php?controller=attachment&id_attachment=904

[89] SIMCOM Wireless Solutions. (2015). *GSM/GPRS+GPS Module*. SIM Technology Group Ltd. Estonia.

URL: http://simcom.ee/documents/SIM808/SIM808%20SPEC_V1507.pdf

[90], [91], [92], [93] & [94] Naylamp Mechatronics. (2017). *Tutorial Básico de Uso del Módulo Bluetooth HC-06 y HC-05*. Peru.

URL: http://www.naylampmechatronics.com/blog/12_Tutorial-B%C3%A1sico-de-Uso-del-M%C3%B3dulo-Bluetooth-H.html

[95] Auto Radio Honorio. *Sensores de golpe*. Argentina.

URL: <http://www.honorio.com.ar/sensochoque.htm>

[96] Celdas, pilas y baterías de ionlítico. Universidad del Valle - Cochabamba

[97] Ortiz N., Vicente A. y Muñoz O. (2016). *Diseño de un sistema electrónico para localizar personas con alzheimer*. (Trabajo de grado) Universidad APEC, República Dominicana.

[98] Agnihotri, N. (2012). *AT Commands, GSM AT command set*.

URL: <https://www.engineersgarage.com/tutorials/at-commands>

[99] Jason. *DFRobot_sim808.h*. (2016)

URL:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiJt_OQgNPZAhWDylMKHWpvBPUQFggmMAA&url=https%3A%2F%2Fgithub.com%2FDFRobot%2FDFRobot_SIM808&usg=AOvVaw2moF-hAIu9xi1V46LMBQ4e

[100] WIKIPEDIA. 2018.

URL: https://es.wikipedia.org/wiki/App_Inventor

[101] GOOGLE.

URL: <http://ai2.appinventor.mit.edu>

GLOSARIO

GSM. - Del inglés, *Global System for Mobile communications*. Es un sistema de telefonía celular para la transmisión digital de voz y datos.

GPS. - Del inglés, *Global Positioning System*. Es un sistema que permite determinar la posición de un objeto en la tierra.

GPRS. - Del inglés, *General Packet Radio Service*. Es una extensión de GSM para la conmutación de paquetes de datos.

I2C.- Del inglés *Inter-Integrated Circuit*. Es un protocolo de comunicación utilizado generalmente entre microcontroladores.

MCU. - Del inglés, *MicroController Unit*. Unidad de microcontrolador.

PWM. - Del inglés, *Pulse Width Modulation*. Se refiere a una técnica conocida como modulación por ancho de pulso.

Tx. - Abreviatura de la palabra en inglés *Transmission* para telecomunicaciones.

Rx. - Abreviatura de la palabra en inglés *Reception* para telecomunicaciones.

ANEXOS

APÉNDICE A: Programas del sistema.

A1. Accesibilidad y control.

//UNAPEC

//TRABAJO DE GRADO

//TEMA: "PROPUESTA DE DISEÑO DE UN SISTEMA DE ALARMA INTELIGENTE PARA PREVENIR ROBOS DE VEHICULOS

//UTILIZANDO EL SISTEMA GLOBAL DE LAS COMUNICACIONES MÓVILES Y GEOLOCALIZACIÓN

//EN LA REPUBLICA DOMINICANA (2018)"

//AUTORES: ROBERT A. PEREZ Y LUIS S. PUJOLS

//DECLARACION DE PINES:

const int SegurosElectricos=13; //Esta intrucción sirve para declarar el pin 13 del ARDUINO UNO como "Seguros/Eléctricos"

const int ClaxonLuces=12; //Esta instrucción sirve para declarar el pin 12 del ARDUINO UNO como "Claxon/Luces"

const int AbrirBaul=8; // Esta instrucción sirve para declarar el pin 8 del ARDUINO UNO como "Abrir/Baúl"

const int ActivacionAlarma = 7; // Esta instrucción sirve para declarar el pin 7 del Arduino como "Activación Alarma"

int estado=0; // Esta instrucción sirve para igualar el "estado" a Cero(0) para el arranque del programa.

//DECLARACIONES DE ENTRADAS Y SALIDAS:

void setup(){

Serial.begin(9600); //Arranque de la comunicación serial

pinMode(SegurosElectricos,OUTPUT); //"Seguros Electricos" declarado como salida.

pinMode(ClaxonLuces, OUTPUT); //"ClaxonLuces" declarado como salida.

```

pinMode(AbrirBaul, OUTPUT);    // "AbrirBaul" declarado como salida.

pinMode(ActivacionAlarma,INPUT); // "ActivacinAlarma" declarado como entrada.

digitalWrite(ClaxonLuces,HIGH); // Este pin se coloca *inicialmente* en uno lógico,
para que su relé de activación comience apagado al iniciar el programa

digitalWrite(SegurosElectricos,HIGH); // Este pin se coloca *inicialmente* en uno
lógico, para que su relé de activación comience apagado al iniciar el programa

digitalWrite(AbrirBaul,HIGH);    // Este pin se coloca *inicialmente* en uno lógico,
para que su relé de activación comience apagado al iniciar el programa

}

//Nota: "Los relés utilizados en este proyecto son activados con *LOW* o Cero lógico"

```

```

void loop(){
if(Serial.available(>0){
estado = Serial.read();
}
if (estado =='1'){
digitalWrite(SegurosElectricos,HIGH);
estado = '0';
}
if(estado=='2'){
digitalWrite(SegurosElectricos,LOW);
estado = '0';
}
if(estado=='3'){
digitalWrite (ClaxonLuces,HIGH);
estado = '0';
}
if(estado=='4'){

```

```

digitalWrite(AbrirBaul,LOW);
delay (800);
digitalWrite(AbrirBaul,HIGH);
estado = '0';
}
if (digitalRead (ActivacionAlarma)){
delay(100);
digitalWrite(ClaxonLuces,LOW);
estado = '0';
}
}
//FIN

```

A2. Assistance GPS-GPRS

```

#include <DFRobot_sim808.h>
#include <SoftwareSerial.h>

DFRobot_SIM808 sim808(&Serial);

#define MESSAGE_LENGTH 160
#define puerta 7
#define PHONE_NUMBER "*****"

char message[MESSAGE_LENGTH];
int messageIndex = 0;

char phone [16];

char datetime[24];

```

```

int a = 1;

void setup() {
//mySerial.begin(9600);

Serial.begin(9600);

while(!sim808.init()) {

delay(1000);

Serial.print("Sim808 init error\r\n");

}

if( sim808.attachGPS()){

Serial.println("Open the GPS power success");

Serial.println("Init Success, please send SMS message to me!");

}

else {

Serial.println("Open the GPS power failure");

}

}

void loop() {

//***** Detecting unread SMS *****

messageIndex = sim808.isSMSunread();

//Serial.print("messageIndex: ");

//Serial.println(messageIndex);

//***** At least, there is one UNREAD SMS *****

if (messageIndex > 0) {

leer_sms();

}

}

```

```

if(!digitalRead(puerta)){
Serial.print("llamando\n");
delay(200);

call();

}
}

void gps_data(){
while( a == 1){
if (sim808.getGPS()) {
a = 0;

Serial.print(sim808.GPSdata.year);

Serial.print("/");

Serial.print(sim808.GPSdata.month);

Serial.print("/");

Serial.print(sim808.GPSdata.day);

Serial.print(" ");

Serial.print(sim808.GPSdata.hour);

Serial.print(":");

Serial.print(sim808.GPSdata.minute);

Serial.print(":");

Serial.print(sim808.GPSdata.second);

Serial.print(":");

Serial.println(sim808.GPSdata.centisecond);

Serial.print("latitude :");

Serial.println(sim808.GPSdata.lat,6);

sim808.latitudeConverToDMS();

```

```

Serial.print("latitude :");
Serial.print(sim808.latDMS.degrees);
Serial.print("\^");
Serial.print(sim808.latDMS.minutes);
Serial.print("\");
Serial.print(sim808.latDMS.seconeds,6);
Serial.println("\");
Serial.print("longitude :");
Serial.println(sim808.GPSdata.lon,6);
sim808.LongitudeConverToDMS();
Serial.print("longitude :");
Serial.print(sim808.longDMS.degrees);
Serial.print("\^");
Serial.print(sim808.longDMS.minutes);
Serial.print("\");
Serial.print(sim808.longDMS.seconeds,6);
Serial.println("\");

Serial.print("speed_kph :");
Serial.println(sim808.GPSdata.speed_kph);
Serial.print("heading :");
Serial.println(sim808.GPSdata.heading);

//***** Turn off the GPS power *****
sim808.detachGPS();
}
}

```

```

}

void leer_sms(){

a = 1;

sim808.readSMS(messageIndex, message, MESSAGE_LENGTH, phone, datetime);

//*****In order not to full SIM Memory, is better to delete it*****

sim808.deleteSMS(messageIndex);

Serial.print("From number: ");

Serial.println(phone);

Serial.print("Datetime: ");

Serial.println(datetime);

Serial.print("Recieved Message: ");

Serial.println(message);

if(message [0]=='G' && message[1]=='p' && message[2]=='s'){

Serial.println("*****__Obteniendo datos GPS__*****");

    gps_data();

}

}

void call(){

sim808.callUp(PHONE_NUMBER);

delay(15000);

sim808.hangup();

}

//FIN

```

APÉNDICE B: Datos estadísticos

B1. Datos estadísticos de la Oficina Nacional de Estadísticas (ONE).



Cuadro 7.11

REPÚBLICA DOMINICANA: Cantidad de vehículos registrados por mes, según tipo de vehículo, 2017, enero-noviembre

Mes	Total	Automóviles ¹	Autobuses	Jeeps	Carga ²	Motocicletas	Volteo	Máquinas Pesadas	Otros ³
Total	168,903	39,825	87,800	26,067	10,272	3,457	505	708	269
Enero	19,126	4,081	10,510	3,036	1,104	294	33	53	15
Febrero	18,945	3,458	11,431	2,532	1,111	280	28	53	52
Marzo	18,657	3,958	10,105	2,733	1,268	380	61	120	32
Abril	15,218	3,218	8,791	2,179	700	224	45	46	15
Mayo	14,067	3,832	6,014	2,788	878	388	38	80	49
Junio	19,699	3,766	11,333	2,815	1,243	404	64	54	20
Julio	15,292	3,484	8,126	2,304	901	345	62	42	28
Agosto	15,526	3,805	8,115	2,277	847	326	54	78	24
Septiembre	13,201	2,758	7,452	1,713	960	229	39	40	10
Octubre	11,985	3,963	4,898	1,953	704	311	52	82	22
noviembre	7,187	3,502	1,025	1,737	556	276	29	60	2

1: Incluye privados, públicos urbanos e interurbanos

2: Incluye camiones y camionetas

3: Incluye Remolques, Ambulancias, Montacargas y Fúnebres

Fuente: Registros administrativos, Gerencia de Estudios Económicos y Tributarios, Dirección General de Impuestos Internos (DGII)

Tabla 9. Cantidad de vehículos registrados por mes. Obtenido de: Oficina Nacional de Estadísticas. (2018).

B2. Datos estadísticos de la Policía Nacional Dominicana (PN).



DEPARTAMENTO DE INFORMACION Y ESTADISTICAS, P.N.
VEHICULOS ROBADO POR PROVINCIA
1 DE ENERO AL 30 DE JUNIO 2017

PROVINCIA	TOTAL
Azua	1
Bahoruco	0
Barahona	2
Dajabon	0
Distrito Nacional	73
Duarte	8
El Seibo	0
Elias Piña	1
Españat	9
Hato Mayor	0
Hermanas Mirabal	3
Independencia	0
La Altagracia	9
La Romana	9
La Vega	16
Maria Trinidad Sanchez	2
Monseñor Nouel	9
Monte Plata	0
Montecristi	1
Pedernales	0
Peravia	0
Puerto Plata	12
Samana	1
San Cristobal	11
San Jose de Ocoa	0
San Juan	0
San Pedro	4
Sanchez Ramirez	1
Santiago	56
Santiago Rodriguez	0
Santo Domingo	83
Valverde	1
TOTAL GENERAL	312

Tabla 10: Cantidad de robo de vehículos. Primer semestre 2017. Obtenido de: Policía Nacional. (2018).



DEPARTAMENTO DE INFORMACION Y ESTADISTICAS, P.N.
VEHICULOS ROBADO POR PROVINCIA
1 DE JULIO AL 30 DE SEPTIEMBRE 2017

PROVINCIA	TOTAL
Azua	0
Bahoruco	0
Barahona	0
Dajabon	0
Distrito Nacional	27
Duarte	2
El Seibo	0
Elias Piña	0
Españat	2
Hato Mayor	0
Hermanas Mirabal	0
Independencia	0
La Altagracia	4
La Romana	6
La Vega	9
Maria Trinidad Sanchez	1
Monseñor Nouel	3
Monte Plata	0
Montecristi	1
Pedernales	0
Peravia	0
Puerto Plata	3
Samana	0
San Cristobal	5
San Jose de Ocoa	0
San Juan	0
San Pedro	3
Sanchez Ramirez	1
Santiago	21
Santiago Rodriguez	0
Santo Domingo	41
Valverde	3

Tabla 11. Cantidad de robo de vehículos. Primer semestre 2017.
 Obtenido de: *Policía Nacional. (2018).*

APÉNDICE C: Presupuesto del SAIRF

C1: Costos de dispositivos, materiales e instalación para elaboración de prototipo del sistema de alarma contra robos de vehículos.

Presupuesto Sistema De Alarma							
Componentes	Cantidad	Precio (US \$)	Precio (RD \$)	Costo de envío (US \$)	Precio de envío en (RD\$)	Tarifa Aduanal/Courier Local (RD \$)	Costo Total
120 Peces Multicolored Jumper	1	\$6.89	\$340.16	\$0.00	\$0.00	\$238.04	\$586.09
Arduino Uno R3 ATmega328P	2	\$19.99	\$986.91	\$8.24	\$406.81	\$227.55	\$1,651.50
Bluetooth HC-06 Slave Module	1	\$4.69	\$231.55	\$2.95	\$145.64	\$218.08	\$603.91
SIM808 Module GSM GPRS GPS	1	\$23.99	\$1,184.39	\$0.00	\$0.00	\$218.08	\$1,427.46
Instalación	\$2,000						
Total	5	\$55.56	\$2,743.00	\$11.19	\$552.45	\$901.75	\$6,197.20

Tabla 12: costo de los materiales utilizados para la elaboración de la propuesta.

C2: Cotización de planes para vehículo ofrecido por el Banco BHD y sus deducibles.

Planes de seguro del BHD (vehículo 2015)			
Tipos de Planes	Prima anual RD \$	Porcentaje del deducible	Monto a pagar por el robo total del vehículo
Trebol clásico	\$32,411.63	1%	\$8,150.00
Econo Trebol	\$19,865.20	30%	\$244,500.00
Trebol Plus	\$34,851.23	1%	\$8,150.00
Trebol Plus +	\$36,942.29	Cobertura	\$0.00
Valor monetario del vehículo	\$815,000.00		

Tabla 13: Cotización de planes para vehículo Toyota Corolla del año 2015.

C3: Cotizaciones de los planes ofrecidos por el banco BHD para un vehículo Toyota corolla del año 2015.

TREBOL CLASICO					TREBOL PLUS				
COBERTURA	LIMITES	% DEDUCIBLE	DEDUCIBLE MINIMO		COBERTURA	LIMITES	% DEDUCIBLE	DEDUCIBLE MINIMO	
DANOS A UN TERCERO	500,000.00				DANOS A UN TERCERO	500,000.00			
DANOS A MAS DE TERCERO	1,000,000.00				DANOS A MAS DE TERCERO	1,000,000.00			
DANOS A PROPIEDAD AJENA	500,000.00				DANOS A PROPIEDAD AJENA	500,000.00			
ACCIDENTES DEL CONDUCTOR	50,000.00				ACCIDENTES DEL CONDUCTOR	150,000.00			
GASTOS MEDICOS CONDUCTOR	5,000.00				GASTOS MEDICOS CONDUCTOR	15,000.00			
DEFENSA JURIDICA	INCLUIDA				DEFENSA JURIDICA	INCLUIDA			
FIANZA JUDICIAL	1,000,000.00				FIANZA JUDICIAL	1,000,000.00			
PERDIDA POR ROTURA DE VIDRIOS	INCLUIDA	10%	500.00		PERDIDA POR ROTURA DE VIDRIOS	INCLUIDA	10%	500.00	
PERDIDA PARCIAL POR DANOS	815,000.00	1%	5,000.00		PERDIDA PARCIAL POR DANOS	815,000.00	1%	5,000.00	
PERD. PARCIAL POR ROBO O HURTO	815,000.00	1%	5,000.00		PERD. PARCIAL POR ROBO O HURTO	815,000.00	1%	5,000.00	
PERD. TOTAL POR DANOS	815,000.00	1%	5,000.00		PERD. TOTAL POR DANOS	815,000.00	1%	5,000.00	
PERD. TOTAL POR ROBO O HURTO	815,000.00	1%	5,000.00		PERD. TOTAL POR ROBO O HURTO	815,000.00	1%	5,000.00	
PLAN RENTA O GASTOS TRANSPORTE	10 Dias (Compacto)				PLAN RENTA O GASTOS TRANSPORTE	15 Dias (Compacto)			
SERVICIO AL AUTOMOVILISTA	INCLUIDA				SERVICIO AL AUTOMOVILISTA	INCLUIDA			
ASISTENCIA EN VIAJES	INCLUIDA				ASISTENCIA EN VIAJES	INCLUIDA			
<input type="checkbox"/>	PRIMA NETA	IMP. SELECTIVO AL CONSUMO	PRIMA TOTAL		<input type="checkbox"/>	PRIMA NETA	IMP. SELECTIVO AL CONSUMO	PRIMA TOTAL	
	27,941.06	4,470.57	32,411.63			30,044.16	4,807.07	34,851.23	

ECONO TREBOL					TREBOL PLUS +				
COBERTURA	LIMITES	% DEDUCIBLE	DEDUCIBLE MINIMO		COBERTURA	LIMITES	% DEDUCIBLE	DEDUCIBLE MINIMO	
DANOS A UN TERCERO	500,000.00				DANOS A UN TERCERO	500,000.00			
DANOS A MAS DE TERCERO	1,000,000.00				DANOS A MAS DE TERCERO	1,000,000.00			
DANOS A PROPIEDAD AJENA	500,000.00				DANOS A PROPIEDAD AJENA	500,000.00			
ACCIDENTES DEL CONDUCTOR	50,000.00				ACCIDENTES DEL CONDUCTOR	150,000.00			
GASTOS MEDICOS CONDUCTOR	5,000.00				GASTOS MEDICOS CONDUCTOR	15,000.00			
DEFENSA JURIDICA	INCLUIDA				DEFENSA JURIDICA	INCLUIDA			
FIANZA JUDICIAL	1,000,000.00				FIANZA JUDICIAL	1,000,000.00			
PERDIDA POR ROTURA DE VIDRIOS	INCLUIDA	10%	500.00		PERDIDA POR ROTURA DE VIDRIOS	INCLUIDA			
PERDIDA PARCIAL POR DANOS	815,000.00	10%	30,000.00		PERDIDA PARCIAL POR DANOS	815,000.00	.5%	5,000.00	
PERD. PARCIAL POR ROBO O HURTO	815,000.00	10%	30,000.00		PERD. PARCIAL POR ROBO O HURTO	815,000.00	.5%	5,000.00	
PERD. TOTAL POR DANOS	815,000.00	30%	30,000.00		PERD. TOTAL POR DANOS	815,000.00			
PERD. TOTAL POR ROBO O HURTO	815,000.00	30%	30,000.00		PERD. TOTAL POR ROBO O HURTO	815,000.00			
SERVICIO AL AUTOMOVILISTA	INCLUIDA				PLAN RENTA O GASTOS TRANSPORTE	15 Dias (Compacto)			
ASISTENCIA EN VIAJES	INCLUIDA				SERVICIO AL AUTOMOVILISTA	INCLUIDA			
<input type="checkbox"/>	PRIMA NETA	IMP. SELECTIVO AL CONSUMO	PRIMA TOTAL		<input type="checkbox"/>	PRIMA NETA	IMP. SELECTIVO AL CONSUMO	PRIMA TOTAL	
	17,125.17	2,740.03	19,865.20			31,846.80	5,095.49	36,942.29	

Figura 32: Cotización de los Planes ofrecidos por el banco BHD.

APÉNDICE D: Contenido del CD

➤ ***Trabajo de grado digital.***

- Documento versión Word 2013.
- Documento versión PDF 2013.

➤ ***Video:*** “PROPUESTA DE DISEÑO DE UN SISTEMA DE ALARMA INTELIGENTE PARA PREVENIR ROBOS DE VEHICULOS UTILIZANDO EL SISTEMA GLOBAL DE LAS COMUNICACIONES MÓVILES Y GEOLOCALIZACIÓN EN LA REPUBLICA DOMINICANA (2018)”. En este video se muestra la prueba de funcionamiento del sistema.