



TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO

**ESQUEMA ALTERNATIVO DE BAJA ENERGÍA EN
SISTEMA NO CONVENCIONAL DE INMOVILIZACIÓN PARA
LA PROTECCIÓN DE VEHÍCULOS AUTOMOTORES**

TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

**PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO EN SISTEMAS AUTOMOTRICES**

**PRESENTA:
ERICK NETZAHUAL RODRIGUEZ**

**NOMBRE DEL ASESOR:
DR. JORGE BEDOLLA HERNÁNDEZ**



APIZACO, TLAX., ABRIL 2026



Educación
Secretaría de Educación Pública



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto Tecnológico de Apizaco
Departamento Ingeniería Eléctrica y Electrónica

Tzompantepec, Tlaxcala, 29/enero/2026
Departamento: Ingeniería Eléctrica y Electrónica
No. De oficio: I.E.E. /044/2026

Asunto: Liberación de Proyecto
para la Titulación Integral

LIC. CECILIA YARELLY ARREGUÍN LARA
JEFA DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES
PRESENTE

Por este medio le informo que ha sido liberado el siguiente proyecto para la Titulación Integral:

Nombre del egresado:	ERICK NETZAHUAL RODRÍGUEZ
Carrera:	INGENIERÍA EN SISTEMAS AUTOMOTRICES
No. De Control:	20371211
Nombre del proyecto:	"ESQUEMA ALTERNATIVO DE BAJA ENERGÍA EN SISTEMA NO CONVENCIONAL DE INMOVILIZACIÓN PARA LA PROTECCIÓN DE VEHÍCULOS AUTOMOTORES".
Producto	TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados.

ATENTAMENTE
Excelencia en Educación Tecnológica
Pensar para Servir, Servir para Triunfar®

M.I.E. MARIO EDUARDO LEAL LÓPEZ
JEFE DEL DEPTO. DE INGENIERÍA
ELÉCTRICA Y ELECTRÓNICA



DR. JORGE BEDOLLA HERNÁNDEZ

Nombre y firma del asesor

MELL/isa*
C.p. Archivo



2026
año de
Margarita Maza





Tzompantepec, Tlaxcala, **19/Marzo/2026**

ERICK NETZAHUAL RODRIGUEZ
EGRESADO(A) DE LA CARRERA DE INGENIERÍA EN SISTEMAS AUTOMOTRICES
CON NÚMERO DE CONTROL 20371211.
P R E S E N T E.

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción **TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL** y cuyo tema es: **"ESQUEMA ALTERNATIVO DE BAJA ENERGÍA EN SISTEMA NO CONVENCIONAL DE INMOVILIZACIÓN PARA LA PROTECCIÓN DE VEHÍCULOS AUTOMOTORES"**, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga la:

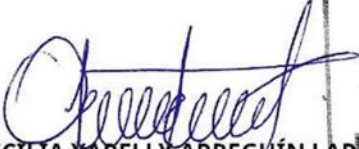
AUTORIZACIÓN DE IMPRESIÓN

Debiendo entregar **1 USB** del mismo, apropiadamente empastados, a la brevedad, para presentar su Acto de Recepción Profesional.

Sin otro particular por el momento me despido.

ATENTAMENTE

Excelencia en Educación Tecnológica
Pensar para Servir, Servir para Triunfar


CECILIA YARELY ARREGUÍN LARA
JEFA DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES



ccp. Archivo
CYAL/Gvm*



2026
año de
Margarita Maza



Agradecimientos

Hoy es un día especial en el que culmina mi etapa en mi formación como Ingeniero en Sistemas Automotrices. Agradezco profundamente a Dios por darme la fuerza, la claridad y la perseverancia necesarias para llegar hasta aquí.

A mis padres, mi mayor motivación y mi orgullo más grande, gracias por ser mi base, mi luz y mi dirección. Gracias por cada sacrificio silencioso, por cada palabra de aliento y por enseñarme que la constancia y el amor pueden construir caminos que parecían imposibles. Este logro también es suyo, porque sin su ejemplo, su apoyo y su fe en mí, este capítulo no tendría el mismo significado. A mi familia en general, gracias por su cariño y presencia constante. A mis amigos, gracias por acompañarme en cada paso, por las risas, los desvelos y por recordarme siempre que los sueños se alcanzan con disciplina y corazón.

Extiendo mi más sincero agradecimiento a mis docentes y profesionales del Instituto Tecnológico de Apizaco, quienes no solo compartieron su conocimiento, sino que también sembraron en mí la pasión por mejorar, crear y construir. Gracias por cada enseñanza, por cada reto y por inspirarme a ser un mejor profesionista y una mejor persona.

Hoy cierro una etapa importante, pero llevo conmigo cada consejo, cada guía y cada gesto de apoyo que hicieron posible este logro.

Resumen

El presente proyecto, titulado “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores”, tiene como propósito desarrollar un sistema de seguridad automotriz innovador que combine eficiencia energética y métodos no convencionales de inmovilización vehicular. La iniciativa surge ante la necesidad de contar con soluciones de protección que no solo sean efectivas ante intentos de robo, sino que también optimicen el consumo energético y la facilidad de operación para el usuario.

El sistema propuesto integra diversas tecnologías modernas de control de acceso, incluyendo Bluetooth, reconocimiento de huella digital y activación mediante llamada telefónica. Esta combinación permite una gestión segura y confiable del acceso al vehículo, habilitando la comunicación en tiempo real con actuadores simplificados responsables de controlar el suministro de combustible mediante el bloqueo de los inyectores.

De esta manera, se garantiza que el vehículo solo pueda ser operado por personas autorizadas, evitando su uso no permitido sin comprometer la eficiencia energética del sistema. Durante el desarrollo del proyecto, se llevaron a cabo pruebas y validaciones que confirmaron el cumplimiento de los resultados esperados. El sistema demostró su capacidad de inmovilización efectiva ante intentos de operación no autorizada, así como la funcionalidad de sus mecanismos de control en condiciones operativas reales. Adicionalmente, se validó la viabilidad de implementar un esquema alternativo de inmovilización que optimiza el consumo de energía, reduciendo la dependencia de sistemas tradicionales que consumen mayores recursos eléctricos.

El proyecto presenta una solución tecnológica integral para la protección de vehículos automotores, que combina seguridad, eficiencia energética y modernización de los sistemas de control de acceso. Los resultados obtenidos confirman que el enfoque propuesto no solo es

funcional y confiable, sino que también ofrece una alternativa innovadora y práctica frente a los métodos convencionales de inmovilización vehicular.

Índice

Capítulo I: Introducción	1
1.1 Planteamiento del problema.....	1
1.2 Revisión del Estado de la Técnica	3
1.3 Justificación	6
1.4 Objetivos	11
1.4.1 Objetivo General	11
1.4.2 Objetivos Específicos	11
Capítulo II: Marco Teórico.....	14
2.1 “Seguridad Vehicular y Sistemas de Inmovilización”.....	14
2.2 “Tecnologías de Autenticación Biométrica”	16
2.3 “Telefonía, Mensajería SMS y Comunicación Bluetooth”	19
Capítulo III: Metodología	22
3.1 Especificaciones técnicas del diseño	23
3.1.1 Especificaciones técnicas del diseño	23
3.1.2 Módulo de Autenticación Biométrica.....	25
3.1.3 Módulo de Comunicación Bluetooth.....	27
3.1.4 Módulo de Control por SMS	29
3.1.5 Módulo de Corte combustible	32
3.1.6 Módulo de control	34
3.2 Diseño detallado	35

3.2.1 Arquitectura funcional del sistema.....	35
3.2.1.2 Módulo Bluetooth.....	40
3.2.1.3 Módulo GSM.....	42
3.2.1.4 Módulo Biométrico.....	47
3.2.1.5 Módulo de Inmovilización no Convencional.....	49
3.2.1.6 Módulo de Alimentación	50
3.2.1.7 Módulo de Indicadores y comunicación.....	51
3.2.2 Cálculo de Diseño.....	53
3.3 Simulación	56
3.3.1 Objetivo de la simulación	56
3.3.2 Simulación de la Creación del código	57
3.3.3 Simulación del circuito en Proteus	60
3.4 Implementación o prototipado.....	66
3.5 Pruebas o Testing.....	87
Capítulo IV: Resultados y Conclusiones.....	95
4.1 Resultados.....	95
4.2 Conclusión	104
Capítulo V: Competencias desarrolladas y/o aplicadas.....	106
Referencias	
Anexos	

Índice de Figuras

Figura 1. Sistema de Inmovilizador de motor	16
Figura 2. Tecnologías de Autenticación Biométrica.....	19
Figura 3. Telefonía, Mensajería SMS y Comunicación Bluetooth	21
Figura 4. Diagrama de Elaboración de Desarrollo de la Metodología	22
Figura 5. Diagrama del Funcionamiento General del Sistema.....	57
Figura 6. Código de Programación.....	59
Figura 7. Simulación en Proteus.....	61
Figura 8. Placa de Baquelita	69
Figura 9. Instalación de Arduino.	73
Figura 10. Instalación del Módulo SIM800L	75
Figura 11. Módulo Relevador.....	77
Figura 12. Indicador Led	79
Figura 13. Desarrollo de la Aplicación "ATLAS"	81
Figura 14. Ensamblaje del Circuito Electrónico en el Contenedor.....	83
Figura 15. Instalación de la Huella Biométrica	84
Figura 16. Sistema Terminado.....	85
Figura 17. Montaje en el Prototipo de Inyectores.....	87
Figura 18. Verificación del Funcionamiento del Sistema.....	89

Figura 19. Llamada Entrante al Dispositivo	91
Figura 20. Vinculación de la Aplicación.....	93
Figura 21. Activación y Desactivación Mediante el Sistema Bluetooth.....	94
Figura 22. Prueba y Medición del Funcionamiento del Sistema Bluetooth	97
Figura 23 Prueba y Medición del Funcionamiento del Sistema de Tecnología Biométrica	98
Figura 24. Prueba y Medición del Funcionamiento del Sistema de Tecnología Biométrica Implementado en la Maqueta de Inyectores.....	99
Figura 25. Prueba del Sistema de Bloqueo por Llamada.....	101
Figura 26. Corte de Combustible Exitoso en la Prueba Realizada en la Maqueta.....	103

Índice de Tablas

Tabla 1. Ventajas de la Implementación de BLE en seguridad Vehicular	29
Tabla 2. Ventajas del enfoque de control remoto mediante SMS o llamada telefónica	32
Tabla 3. Interconexión con otros módulos.....	39
Tabla 4. Especificaciones Técnicas	40
Tabla 5. Datos Estimados por Módulo.....	54

Capítulo I: Introducción

1.1 Planteamiento del problema

El robo de vehículos automotores continúa siendo uno de los principales delitos que afectan la seguridad ciudadana, con pérdidas económicas considerables tanto para individuos como para compañías aseguradoras. Las medidas de seguridad tradicionales, como alarmas, llaves codificadas y sistemas de rastreo, aunque útiles, tienen vulnerabilidades ante técnicas de robo cada vez más sofisticadas (por ejemplo, clonación de llaves, manipulación del sistema eléctrico/inyección, maniobras de bypass, etc.). En este marco surge la necesidad de soluciones de seguridad más robustas, que protejan el motor más allá del encendido, controlando directamente componentes críticos del sistema de suministro de combustible (Insurance Information Institute, 2024).

Asimismo, existe una creciente demanda de que estos sistemas sean eficientes energéticamente, fáciles de mantener, de costo moderado, y que utilicen tecnologías accesibles (como Bluetooth, SMS, biometría), lo que permite que sean viables tanto para vehículos de gama media como para contextos con restricciones de infraestructura o recursos (Astuti, Ritzkal, Hendrawan, & Prakosa, 2020).

A pesar de los avances, los sistemas de seguridad actuales presentan una serie de limitaciones importantes:

Limitaciones funcionales: Muchos sistemas sólo disuaden el robo o permiten recuperarlo (alertas, rastreo), pero no impiden físicamente que el vehículo se utilice en caso de robo. En concreto, aunque existen inmovilizadoras, muchos no integran mecanismos de corte directo del suministro de combustible (como la inyección) que podrían detener el vehículo una vez que su uso no autorizado ha comenzado (Office of Justice Programs, 2005).

Costos y complejidad: Las soluciones robustas de seguridad muchas veces implican hardware especializado, integraciones complejas con la ECU (unidad de control del motor), labor especializada, lo cual incrementa su costo, dificultando su adopción en vehículos de gama media o en zonas con menor acceso tecnológico (Harsha, Tanusha, & Sharma, 2023).

Eficiencia energética y consumo de recursos: Algunos sistemas con alertas remotas, rastreo GPS continuo, módulos GSM activos, etc., tienen consumos constantes de energía, lo que puede afectar la batería del vehículo, requerir mantenimiento frecuente o aumentar los costos operativos (Prathish, Kumar, & Bharathi, 2017).

Seguridad física y digital: Sistemas basados en llaves o transmisores pueden ser vulnerables a ataques físicos (robo de la llave, bypass) o digitales (relé, clonación de señales, hacking del vehículo). La biometría añade una capa, pero también tiene desafíos propios (falsos positivos/negativos, resistencia al mal uso, protección de datos biométricos) (Valentín, Yurtsever, & Ahmed, 2022).

Demora en respuesta: Algunos sistemas dependen de acciones del usuario (entrada de contraseña, autenticación remota, etc.) que pueden introducir demoras críticas en situaciones de robo (Brijet, Kumar, & Bharathi, 2017).

Necesidad del proyecto:

Frente a esas limitaciones, surge la necesidad de un sistema de inmovilización que:

Sea no convencional en el sentido de cortar activamente el suministro de combustible directamente en los inyectores, de modo que una vez activado el modo seguro, el vehículo no pueda moverse.

Use tecnologías accesibles y de bajo consumo (Bluetooth, SMS, biometría de huella digital) para autenticar al usuario, permitir control remoto, alertas, etc.

Sea de baja energía, de modo que no agote la batería del vehículo ni requiera ciclos de mantenimiento frecuentes.

Integre múltiples formas de autenticación (por ejemplo, huella digital + Bluetooth + SMS) para aumentar la seguridad y evitar que una sola vía de falla (pérdida de teléfono, duplicación de señal Bluetooth, etc.) comprometa el sistema.

Sea aplicable tanto para vehículos particulares como para flotas, con una implementación que minimice costes y maximice confiabilidad (Harsha, Tanusha, & Sharma, 2023).

1.2 Revisión del Estado de la Técnica

Estudios existentes sobre inmovilización mediante biometría

Un enfoque recurrido en la técnica consiste en los sistemas de biometric immobilizer, que usan reconocimiento de huella digital (u otra biometría) para permitir o negar el arranque del vehículo. Por ejemplo, la patente WO2005028237A1 describe un sistema de inmovilizador biométrico que integra una unidad de autenticación de huellas digitales con un controlador embebido que gestiona el almacenamiento seguro de los datos biométricos y controla el acceso al encendido del vehículo. Aunque este sistema ofrece una autenticación fuerte, no se menciona un mecanismo para cortar suministro de combustible a los inyectores ni interoperar con SMS o Bluetooth como canales secundarios de control. (WO2005028237A1 – Biometric Immobilizer for Automobiles)

La patente US9381890B2, “Method and apparatus for biometric vehicle activation”, también aborda la activación vehicular mediante biometría, pero de nuevo está centrada en permitir o denegar el encendido conforme a la huella digital o datos biométricos, sin integrar explícitamente corte físico del suministro de combustible ni mecanismos de comunicación remota (SMS/Bluetooth) para ese fin.

Otra corriente técnica examina la posibilidad de inmovilizar vehículos remotamente mediante comandos SMS, aplicaciones móviles u otros canales remotos.

Frotcom ofrece un sistema de inmovilización remota (“Remote Vehicle Immobilisation”) que permite desactivar el encendido o bloquear el vehículo mediante SMS o aplicación, para flotas de vehículos. Sin embargo, en sus especificaciones se indica que sólo evita el reinicio del motor

cuando este está apagado, o bloquea el arranque después de que el vehículo esté detenido, sin implicar un corte directo del suministro de combustible por los inyectores.

El proveedor MxTrak tiene una solución similar: pueden desactivar remotamente un vehículo usando SMS o aplicación. Nuevamente, el mecanismo es más general (bloqueo del motor, arranque, etc.), sin mencionar el corte físico de suministro por los inyectores.

El artículo “Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems” describe cómo unidades de entretenimiento/infotainment en automóviles pueden ser aprovechadas para ataques de privacidad mediante Bluetooth, explotar supuestos de confianza de dispositivos emparejados, lo que sugiere riesgos si Bluetooth es usado como vía de control para funciones sensibles.

SpringerOpen, investigan vulnerabilidades del protocolo Bluetooth (por ejemplo BLE, BLE-relay) que permiten desbloquear o iniciar vehículos si el sistema de entrada sin llave depende de proximidad Bluetooth. Ejemplos prácticos como los ataques detectados sobre Tesla Model 3 / Y muestran que se puede relayer la señal BLE del teléfono del usuario para engañar al vehículo.

Estudios como L2Fuzz: Discovering Bluetooth L2CAP Vulnerabilities Using Stateful Fuzz Testing han encontrado vulnerabilidades en la pila de Bluetooth en dispositivos reales, lo que demuestra que los mecanismos de Bluetooth pueden ser comprometidos directa o indirectamente.

La patente WO2023232686A1 describe un sistema de inmovilizador vehicular que usa credenciales biométricas (por ejemplo, huella o reconocimiento facial), junto con una aplicación de teléfono, para controlar un relé de seguridad vía Bluetooth. Este relé permite o impide completar

el circuito de encendido según la autenticación. No se menciona si tiene acceso al sistema de inyectores para cortar suministro de combustible directamente, ni se menciona control por SMS.

Otra patente, CN1680153A, “Car Anti-theft Device with Bluetooth Identification”, usa identificación Bluetooth para activar un estado antirrobo, alarmas y comunicación con propietario, pero de nuevo sin cortar combustible ni usar todos los medios de autenticación propuestos.

1.3 Justificación

En un contexto donde la seguridad vehicular se ha convertido en una preocupación creciente debido al aumento sostenido de los robos de automóviles, la necesidad de desarrollar soluciones tecnológicas más efectivas, accesibles y sostenibles se vuelve imperativa. Los sistemas tradicionales de protección, aunque útiles, han demostrado limitaciones frente a métodos de sustracción cada vez más sofisticados, lo que exige la implementación de alternativas innovadoras que brinden una protección integral tanto al vehículo como a su propietario.

En este marco, el proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores” se plantea como una propuesta tecnológica avanzada que busca superar las deficiencias de los mecanismos convencionales de seguridad. Su diseño integra el uso de biometría, conectividad Bluetooth y comandos SMS, permitiendo un control multifactorial de acceso y la inmovilización directa del vehículo mediante la interrupción del suministro de combustible a los inyectores del motor.

La justificación de este proyecto se sustenta en cuatro dimensiones interrelacionadas: teórica, social, económica y ambiental. Desde el ámbito teórico, la propuesta se basa en principios

de innovación tecnológica y eficiencia energética aplicados a la seguridad automotriz. En el aspecto social, responde a la necesidad de fortalecer la confianza ciudadana y reducir la incidencia delictiva. En el plano económico, representa una alternativa viable y de bajo costo que disminuye las pérdidas patrimoniales derivadas del robo de vehículos. Finalmente, desde la perspectiva ambiental, contribuye a la sostenibilidad mediante el uso responsable de la energía y la reducción del impacto ecológico asociado a la fabricación y uso indebido de automóviles.

De esta manera, la justificación integral del proyecto evidencia su relevancia no solo como una solución técnica a una problemática actual, sino también como una iniciativa que promueve la seguridad, la eficiencia y la sostenibilidad, alineándose con los objetivos de innovación tecnológica y bienestar social.

1.3.1 Justificación Teórica

El aumento sostenido en los índices de robos de vehículos automotores ha generado una demanda urgente por soluciones de seguridad más avanzadas y eficaces que superen las limitaciones de los sistemas tradicionales. Los métodos convencionales, como alarmas, llaves codificadas o sistemas de rastreo, aunque útiles, presentan vulnerabilidades frente a técnicas cada vez más sofisticadas de sustracción. En este contexto, surge la necesidad de implementar esquemas de inmovilización que no solo disuadan el robo, sino que impidan físicamente el uso no autorizado del vehículo.

El presente proyecto, denominado Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores, aborda esta

problemática mediante la integración de tecnologías biométricas, comunicación inalámbrica y control remoto para cortar el suministro de gasolina directamente en los inyectores del motor. Esta estrategia representa un enfoque innovador, ya que interviene de manera directa en un componente crítico del funcionamiento vehicular, imposibilitando el desplazamiento del automóvil incluso en situaciones donde otros sistemas puedan ser vulnerados.

El uso de autenticación multifactorial que combina huella digital, conectividad Bluetooth y comandos SMS permite no solo un control robusto y confiable del acceso al vehículo, sino también una operación eficiente en términos energéticos, aspecto crucial para garantizar la viabilidad práctica y sostenibilidad del sistema en vehículos de diferentes gamas y contextos de uso.

Además, la implementación de este sistema contribuye a la prevención del delito mediante un mecanismo activo y proactivo de seguridad, lo que no solo protege el patrimonio individual, sino que también fortalece la seguridad pública. De esta forma, el proyecto impulsa el desarrollo tecnológico aplicado a la seguridad vehicular, fomentando la confianza ciudadana y la innovación en la lucha contra el robo de automotores.

1.3.2 Justificación Social

El proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores representa una contribución significativa al bienestar social al abordar uno de los problemas que afectan directamente la calidad de vida de la población: el robo de vehículos. Al ofrecer una solución tecnológica accesible, segura y eficiente, este sistema busca reducir la incidencia de estos delitos, generando un impacto positivo en la protección del patrimonio de los ciudadanos.

La implementación de esta tecnología no solo disminuirá la percepción de inseguridad que afecta a conductores y propietarios de vehículos, sino que también fomentará la creación de entornos urbanos más confiables y seguros. Al proporcionar un mecanismo robusto para la inmovilización del vehículo a través de la combinación de biometría, Bluetooth y comandos SMS, se promueve un uso responsable y consciente de la tecnología en función del bien común.

Además, el proyecto apoya de manera indirecta a las autoridades en sus esfuerzos por combatir la delincuencia, fortaleciendo las herramientas preventivas disponibles y promoviendo una cultura de seguridad proactiva. En consecuencia, esta iniciativa contribuye a consolidar una sociedad más protegida, donde la confianza ciudadana y la tranquilidad en la movilidad diaria se vean fortalecidas.

1.3.3 Justificación Económica

El proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores se presenta como una solución financieramente viable y estratégica, fundamentada en el uso de componentes accesibles y de bajo costo, que además permiten una integración sencilla con los sistemas automotrices existentes. Esta característica facilita su adopción masiva sin generar una carga económica elevada para los usuarios finales ni para las empresas instaladoras.

La implementación de este sistema contribuirá a una reducción significativa de los gastos derivados del robo de vehículos, beneficiando tanto a propietarios particulares como a compañías aseguradoras y organismos públicos involucrados en la recuperación y gestión de vehículos

robados. Al minimizar las pérdidas patrimoniales y los costos asociados a procesos de recuperación y trámites legales, se genera un impacto económico favorable que fortalece la estabilidad financiera de los usuarios y del mercado automotriz en general.

De esta manera, el proyecto representa una inversión eficiente y sostenible en materia de seguridad vehicular, con beneficios económicos tangibles tanto a corto como a largo plazo, promoviendo una economía local más segura y resiliente ante los desafíos que implica la delincuencia automotriz.

1.3.4 Justificación Ambiental

El proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores aporta significativamente a la sostenibilidad ambiental al contribuir a la reducción del robo de vehículos. Esta disminución implica una menor demanda de fabricación y reemplazo prematuro de unidades robadas, lo que se traduce en una reducción del consumo de recursos naturales y la huella ambiental asociada a la producción y transporte de automóviles.

Asimismo, al implementar un sistema que bloquea el suministro de gasolina mediante la inmovilización de los inyectores, se previene el uso no autorizado del vehículo, evitando así emisiones contaminantes derivadas de actividades ilícitas que involucran el desplazamiento de vehículos robados. Esto contribuye directamente a la reducción de la contaminación atmosférica y al mejoramiento de la calidad del aire.

Por otra parte, el diseño del sistema se basa en componentes de baja energía y su integración se realiza sin modificar de manera significativa el sistema automotriz original, lo que favorece un uso eficiente y responsable de la tecnología. De esta forma, el proyecto está alineado con principios de innovación sostenible, promoviendo prácticas que protegen el medio ambiente y garantizan un impacto ambiental mínimo a largo plazo.

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar un esquema alternativo de inmovilización vehicular que utilice un enfoque de baja energía para la protección de vehículos automotores, mediante la implementación de un sistema no convencional capaz de establecer comunicación en tiempo real con actuadores simplificados que controlen el suministro de combustible a través del bloqueo de inyectores

1.4.2 Objetivos Específicos

- Investigar y analizar tecnologías de autenticación y control remoto aplicables a sistemas de inmovilización vehicular, con énfasis en el uso de Bluetooth, sensores biométricos (huella digital) y comunicación por SMS.
- Diseñar una arquitectura de sistema que integre módulos de comunicación y autenticación de bajo consumo energético, permitiendo la activación o bloqueo del sistema de inyección de combustible.

- Desarrollar un módulo de control central capaz de recibir y procesar comandos de inmovilización a través de Bluetooth y SMS, así como validar el acceso mediante huella digital.
- Seleccionar componentes electrónicos de bajo consumo, asegurando la eficiencia energética del sistema sin comprometer la fiabilidad en la protección del vehículo.
- Implementar un sistema de autenticación biométrica (huella digital) que permita la identificación segura del usuario autorizado para el encendido del vehículo.
- Programar la recepción y gestión de comandos remotos vía Bluetooth y mensajes SMS, para permitir la activación o desactivación del sistema de inmovilización desde dispositivos móviles.
- Construir un prototipo funcional del sistema propuesto, integrando los módulos de autenticación, comunicación y control de actuadores.
- Realizar pruebas de funcionamiento, consumo energético y tiempo de respuesta, evaluando la efectividad del sistema en escenarios simulados de seguridad y emergencia.

- Comparar el desempeño del sistema propuesto con soluciones convencionales, determinando sus ventajas en términos de eficiencia, seguridad y autonomía energética.

Capítulo II: Marco Teórico

2.1 Seguridad Vehicular y Sistemas de Inmovilización

La seguridad vehicular ha evolucionado significativamente en las últimas décadas, incorporando no solo sistemas pasivos como cinturones de seguridad y bolsas de aire, sino también tecnologías activas destinadas a prevenir el robo o uso no autorizado del vehículo. Entre estas, los sistemas de inmovilización juegan un papel fundamental al evitar que el vehículo sea encendido o manipulado sin autorización, interfiriendo con sistemas críticos como la ignición o la alimentación de combustible (Bosch Mobility, s.f.).

Un sistema de inmovilización vehicular (o "immobilizer") generalmente actúa como un mecanismo de seguridad electrónica que valida la identidad del usuario antes de permitir el encendido del motor. Estos sistemas fueron introducidos de manera masiva en los años 90 y, en muchos países, su implementación se volvió obligatoria como medida de reducción de robos. Por ejemplo, la Unión Europea hizo obligatorio el uso de inmovilizadores electrónicos en todos los vehículos nuevos a partir de 1998 (European Commission, 1998). Su funcionamiento básico consiste en un microchip ubicado en la llave del vehículo, que emite un código de identificación que debe ser reconocido por la unidad de control del motor (ECU) para permitir el arranque (Bosch Mobility, s.f.).

La efectividad de los sistemas de inmovilización ha sido respaldada por diversos estudios. Según datos del National Insurance Crime Bureau (NICB), en países donde estos sistemas se implementaron de forma obligatoria, se observó una notable disminución en las tasas de robo de

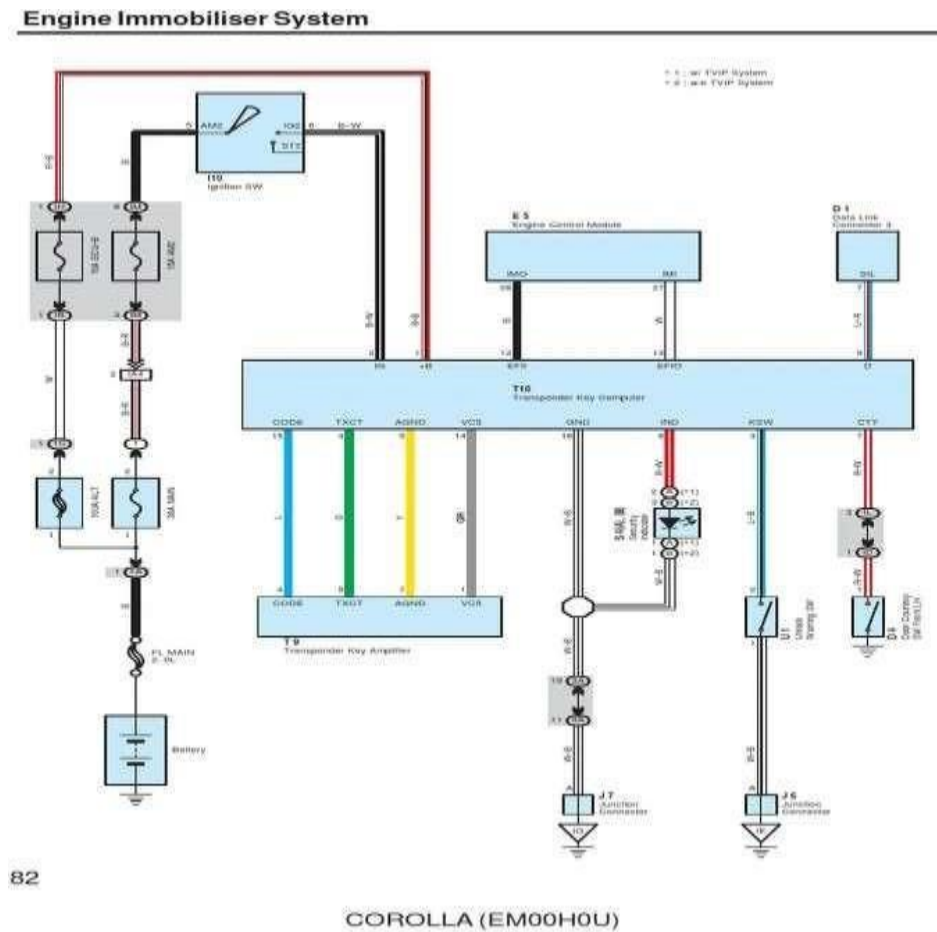
vehículos (NICB, 2019). Este descenso se atribuye a que los sistemas dificultan la técnica del "puenteo" del encendido, una de las formas más comunes de robo de vehículos antes de la implementación de estas tecnologías.

Sin embargo, con el tiempo también han surgido nuevas amenazas, como los ataques de clonación de llaves, técnicas de interceptación de señales (relay attacks), y el uso de herramientas electrónicas ilegales capaces de desactivar o burlar sistemas de inmovilización convencionales. Esto ha llevado a la industria automotriz a desarrollar soluciones más sofisticadas e integradas, que combinan tecnologías como la autenticación biométrica, control remoto vía aplicaciones móviles, y el uso de criptografía avanzada para proteger las comunicaciones entre el vehículo y sus dispositivos de seguridad (Feng et al., 2021).

Los sistemas de inmovilización modernos pueden clasificarse en dos grandes tipos: los que operan de forma local (como los basados en transponders o sensores biométricos) y los que permiten un control remoto del vehículo (como los sistemas que integran comunicaciones GSM/SMS o Bluetooth). Esta evolución responde a la necesidad de mejorar la seguridad y brindar a los usuarios herramientas de control más flexibles, como el encendido o apagado del motor a distancia, el rastreo en tiempo real y la notificación inmediata de intentos de acceso no autorizado (Barbosa et al., 2020).

Figura 1

Sistema de inmovilizador de motor (engine immobiliser) para un Toyota Corolla.



Recuperado de tsuelectronico. (s. f.). *Corolla Engine Immobiliser System Diagram*. Scribd.

Recuperado de <https://www.scribd.com/doc/281270220/engine-immobilizer-system-toyota-corolla-2006>

2.2 Tecnologías de Autenticación Biométrica

La autenticación biométrica se basa en el uso de características físicas únicas e intransferibles de las personas para verificar su identidad. Entre las tecnologías más difundidas en

este campo se encuentra la huella digital, la cual ha ganado gran aceptación en aplicaciones de seguridad gracias a su facilidad de uso, bajo costo y precisión en la identificación. A diferencia de los métodos tradicionales como contraseñas o tarjetas de acceso, los sistemas biométricos reducen significativamente el riesgo de suplantación o pérdida de credenciales (Jain, Ross & Nandakumar, 2011).

El principio de funcionamiento de los sistemas de huella digital se basa en la lectura de los patrones de crestas y valles de los dedos, utilizando sensores ópticos, capacitivos, ultrasónicos o térmicos. Estos sensores capturan la imagen o el mapa de la huella y la comparan con una plantilla previamente registrada, almacenada de forma segura en el sistema. La autenticación ocurre cuando ambas coinciden dentro de un umbral de similitud definido (Maltoni, Maio, Jain & Prabhakar, 2009).

En el sector automotriz, el uso de huellas digitales para la activación de vehículos representa una evolución importante en materia de seguridad y experiencia del usuario. Fabricantes como Hyundai y BMW han comenzado a integrar sensores de huella en vehículos de alta gama, permitiendo no solo el encendido del motor, sino también la personalización automática de asientos, retrovisores y preferencias del conductor (Biometric Update, 2018). Estos sistemas no solo reemplazan a las llaves tradicionales, sino que también actúan como una capa adicional de seguridad ante intentos de robo o acceso no autorizado.

Desde el punto de vista técnico, los sensores capacitivos son los más utilizados en aplicaciones móviles y automotrices por su alta precisión, bajo consumo energético y resistencia al desgaste físico. Empresas como Fingerprint Cards y Synaptics han desarrollado módulos biométricos específicos para su integración en entornos automotrices, cumpliendo con estándares como AEC-Q100, los cuales garantizan la operación estable en condiciones de temperatura extrema, vibración y humedad (Fingerprint Cards, 2018).

No obstante, los sistemas biométricos también presentan desafíos. Factores como la suciedad en los dedos, daños en la piel o condiciones ambientales extremas pueden afectar la calidad de la lectura. Además, existen preocupaciones en torno a la privacidad y seguridad de los datos biométricos, ya que, a diferencia de las contraseñas, una huella digital no puede ser modificada en caso de filtración. Por esta razón, se recomienda que los sistemas incorporen técnicas de cifrado, almacenamiento seguro y verificación multifactor como medida de mitigación de riesgos (ISO/IEC 24745:2011; Bhattacharyya, Ranjan, Alisherov & Choi, 2009).

En suma, la autenticación mediante huella digital se consolida como una tecnología eficaz, segura y práctica para aplicaciones de control de acceso vehicular, siempre que se integre adecuadamente con estándares de seguridad y privacidad. Su incorporación en esquemas de inmovilización representa una estrategia innovadora frente al aumento de los robos de vehículos mediante técnicas electrónicas.

Figura 2

Tecnologías de Autenticación Biométrica – Huella Digital



Recuperado de RecFaces. (2018). Huella dactilar | Reconocimiento de huella dactilar en las empresas. Recuperado de <https://recfaces.com/es/articles/que-es-huella-dactilar>

2.3 Telefonía, Mensajería SMS y Comunicación Bluetooth

La telefonía móvil se ha consolidado como uno de los medios de comunicación más utilizados a nivel mundial, permitiendo la transmisión de voz y datos a través de redes celulares. El desarrollo de las redes móviles ha evolucionado desde la primera generación (1G) hasta las actuales redes 5G, aumentando la capacidad, velocidad y eficiencia en la comunicación. Esta evolución ha permitido la integración de servicios de mensajería, datos y multimedia, facilitando la interacción en tiempo real y la implementación de aplicaciones móviles avanzadas (Sharma & Singh, 2020).

En particular, la mensajería SMS (Short Message Service) representa uno de los primeros servicios de texto disponibles en redes móviles y sigue siendo ampliamente utilizado por su simplicidad, bajo costo y alta fiabilidad. El protocolo SMS permite enviar mensajes de texto breves (hasta 160 caracteres) a través de la red celular, utilizando canales de señalización separados de las llamadas de voz. Además, SMS ha sido empleado en sistemas de control y monitoreo remoto, incluyendo aplicaciones de seguridad vehicular y alertas automáticas (Gomez & Rivas, 2019).

Por otro lado, la comunicación Bluetooth es una tecnología inalámbrica de corto alcance diseñada para la transmisión de datos entre dispositivos en distancias típicas de 1 a 100 metros, dependiendo de la clase del dispositivo. Bluetooth opera en la banda ISM de 2.4 GHz y utiliza técnicas de salto de frecuencia para minimizar interferencias. Su arquitectura permite establecer conexiones punto a punto o multipunto, siendo ampliamente utilizada en sistemas de audio, dispositivos móviles, automoción, y soluciones de Internet de las Cosas (IoT) (Bluetooth SIG, 2023).

En el ámbito de la seguridad vehicular, la combinación de SMS y Bluetooth ha permitido desarrollar sistemas híbridos de inmovilización y monitoreo, donde el Bluetooth facilita la comunicación local entre el vehículo y dispositivos móviles o sensores biométricos, mientras que SMS permite la comunicación remota para enviar alertas o comandos a distancia, incluso cuando no hay conexión a internet (Kumar & Singh, 2021). Esta sinergia tecnológica optimiza la eficiencia energética y mejora la seguridad y control sobre el vehículo.

Finalmente, es importante destacar que tanto la telefonía móvil como la comunicación Bluetooth continúan evolucionando para soportar nuevos protocolos de seguridad, mayor velocidad de transmisión, y una mejor interoperabilidad entre dispositivos. La integración adecuada de estas tecnologías es fundamental para diseñar sistemas de inmovilización vehicular que sean confiables, seguros y fáciles de usar (Singh & Gupta, 2022).

Figura3

Telefonía, Mensajería SMS y Comunicación Bluetooth



Recuperado de Witts, J. (2019). SMS Diagram. Recuperado de <https://dribbble.com/shots/6790386-SMS-Diagram>

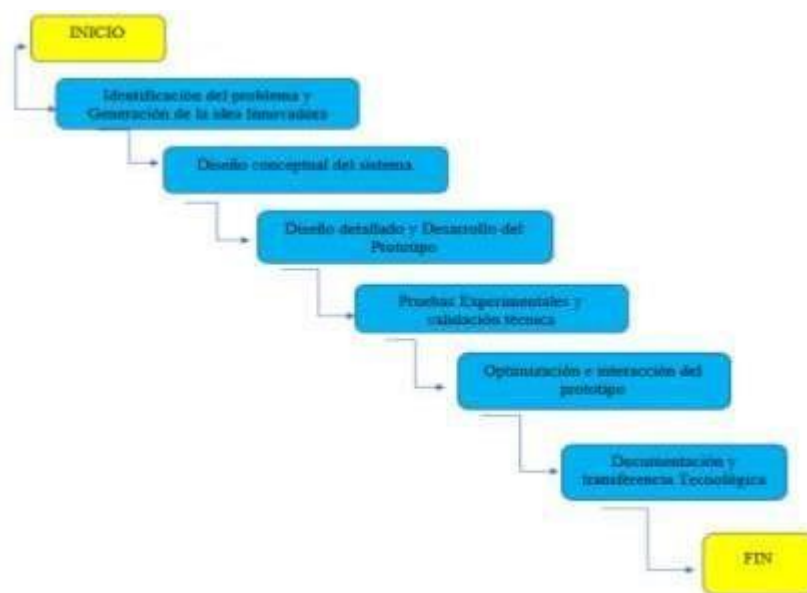
Capítulo III: Metodología

El presente proyecto se desarrollará bajo una Metodología de Innovación y Prototipado, orientada a la creación, validación y perfeccionamiento progresivo de una solución tecnológica funcional. Este enfoque metodológico permite transformar una idea innovadora en un producto tangible, aplicando principios de diseño, ingeniería y validación experimental.

Dicha metodología se fundamenta en un proceso iterativo, flexible y orientado a resultados, donde cada fase del desarrollo —desde la conceptualización hasta la validación final— se retroalimenta con base en los hallazgos obtenidos. El propósito es garantizar que el sistema propuesto cumpla con los criterios de bajo consumo energético, alta fiabilidad y viabilidad técnica para su implementación en vehículos automotores.

Figura 4

Diagrama de Desarrollo de la Metodología



Nota: Elaboración Propia

3.1 Especificaciones del Diseño

El diseño del sistema propuesto se fundamenta en una arquitectura modular, eficiente y de bajo consumo energético, destinada a garantizar la protección integral del vehículo mediante la inmovilización controlada del motor. El sistema se concibe como una solución tecnológica innovadora que combina biometría, comunicación inalámbrica y control remoto, con el fin de ofrecer una alternativa segura, confiable y adaptable a diferentes tipos de vehículos automotores.

Este diseño contempla la integración de cuatro módulos principales:

Autenticación biométrica, para validar la identidad del usuario.

Comunicación Bluetooth, que permite la interacción local entre el usuario y el sistema.

Control por SMS, destinado a la gestión remota del vehículo en caso de emergencia o intento de robo.

Corte de combustible, encargado de interrumpir el suministro a los inyectores del motor, imposibilitando el arranque o desplazamiento no autorizado del vehículo.

3.1.1 Especificaciones Técnicas del Diseño

El diseño del proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores” se basa en una arquitectura modular orientada a la eficiencia energética, seguridad multifactorial y compatibilidad con sistemas automotrices convencionales. Su configuración técnica integra componentes electrónicos de bajo consumo y alta confiabilidad, organizados en subsistemas que trabajan de manera coordinada para garantizar el control y la inmovilización segura del vehículo.

El sistema está conformado por cuatro módulos principales:

Módulo de Autenticación Biométrica:

Utiliza un sensor de huella digital óptico para validar la identidad del usuario. Opera con un voltaje de 3.3 a 5V y se comunica con el microcontrolador mediante interfaz serial (UART). Su tiempo de reconocimiento es inferior a un segundo, lo que asegura un acceso rápido y seguro.

Módulo de Comunicación Bluetooth:

Basado en un módulo HC-05, permite la conexión inalámbrica con el dispositivo móvil del propietario para activar o desactivar el sistema. Su alcance aproximado es de 10 a 15 metros y presenta un consumo energético mínimo en modo de espera, garantizando la eficiencia operativa.

Módulo GSM (Control por SMS):

Implementado con un módulo SIM800L, posibilita el control remoto mediante mensajes de texto, permitiendo la inmovilización del vehículo a distancia. Su voltaje de operación oscila entre 3.4 y 4.4V, con soporte para redes GSM/GPRS, lo que le brinda gran alcance y autonomía.

Módulo de Corte de Combustible:

Emplea una válvula solenoide controlada por relé de 12V, la cual interrumpe el flujo de gasolina hacia los inyectores del motor cuando se detecta un intento de acceso no autorizado. Su tiempo de respuesta es inferior a 200 milisegundos, garantizando una acción inmediata.

El sistema es gobernado por un microcontrolador de bajo consumo (Arduino Nano o ESP32), encargado de procesar la información, ejecutar las órdenes de control y gestionar la comunicación entre módulos. El consumo total estimado del sistema es inferior a 250 mA en modo activo y 50 mA en modo reposo, lo que lo convierte en una solución energéticamente eficiente.

Adicionalmente, el diseño incorpora mecanismos de protección eléctrica (fusibles, diodos y reguladores de voltaje) y protocolos de seguridad lógica, como autenticación multifactorial y encriptación básica de comandos, garantizando un funcionamiento seguro y confiable.

3.1.2 Módulo de Autenticación Biométrica

El módulo de autenticación biométrica constituye el componente central del sistema de seguridad propuesto, ya que es el encargado de verificar la identidad del usuario antes de permitir la activación o el arranque del vehículo. Este módulo funciona como la primera barrera de protección, reemplazando los métodos convencionales de acceso como llaves o tarjetas electrónicas por un sistema basado en reconocimiento de huella digital, lo cual proporciona un nivel superior de fiabilidad, rapidez y personalización.

El empleo de biometría dactilar garantiza que únicamente el propietario o los usuarios previamente registrados puedan autorizar el encendido del vehículo, reduciendo significativamente la posibilidad de robo o uso no autorizado.

Componente Utilizado

- Uso del sensor de huella digital óptico modelo R307 o AS608, ampliamente empleado en aplicaciones de seguridad electrónica y sistemas embebidos.
- Características principales:
- Voltaje de operación: 3.3 – 5V, compatible con la mayoría de microcontroladores de bajo consumo.

- Interfaz de comunicación: Serial TTL, lo que facilita su integración con plataformas Arduino y ESP.
- Capacidad de almacenamiento: Hasta 100 huellas, permitiendo registrar múltiples usuarios o administradores.
- Tiempo de reconocimiento: Menor a 1 segundo, optimizando la experiencia del usuario y la respuesta del sistema.
- Dimensiones compactas: Ideal para su instalación en el tablero del vehículo o zonas discretas del interior.

Funcionamiento del Componente

El sensor utiliza una tecnología óptica que capta la imagen de la huella digital mediante un lector iluminado, convirtiendo dicha imagen en un patrón digital. Este patrón es comparado con las plantillas almacenadas en su base de datos interna mediante algoritmos de coincidencia.

El proceso se realiza en tres fases principales:

- Captura: el usuario coloca el dedo sobre el sensor.
- Conversión: el sensor transforma la imagen de la huella en un patrón digital codificado.
- Comparación: el microcontrolador ejecuta la orden de validación; si el patrón coincide, se activa la señal de acceso, permitiendo el arranque o desbloqueo del sistema de combustible.

En caso contrario, el sistema permanece bloqueado y puede emitir una alerta o registrar el intento fallido.

3.1.3 Módulo de Comunicación Bluetooth

El Módulo de Comunicación Bluetooth es un componente esencial dentro del sistema de inmovilización propuesto, ya que permite establecer una interfaz inalámbrica segura y de corto alcance entre el usuario y el vehículo. Su función principal es transmitir y recibir comandos que controlan la activación o desactivación del sistema de seguridad, facilitando una operación práctica, moderna y de bajo consumo energético.

Este módulo actúa como un enlace de comunicación local que complementa al sistema de autenticación biométrica y al control por SMS, conformando un entorno de autenticación multifactorial. A través de la conexión Bluetooth, el propietario puede interactuar con el vehículo desde su teléfono móvil o dispositivo autorizado sin necesidad de conexión a internet, incrementando la autonomía y confiabilidad del sistema.

Componente Utilizado

El componente propuesto para este proyecto es el módulo Bluetooth HC-05 o HC-06, ampliamente utilizado por su compatibilidad con microcontroladores y su facilidad de configuración.

Características técnicas principales:

- Voltaje de operación: 3.6 – 6V DC.
- Interfaz de comunicación: UART (TX/RX).
- Protocolo: Bluetooth Serial Port Profile (SPP).
- Alcance de transmisión: 10 a 15 metros (en línea de vista).

- Velocidad de transmisión de datos: 9600 bps (configurable).
- Consumo energético:
- Modo activo: 25 mA (promedio).
 - Modo inactivo: < 5 mA.
 - Emparejamiento: mediante código PIN único para evitar accesos no autorizados

Funcionamiento del Componente

El módulo Bluetooth se integra en el sistema con las siguientes funciones específicas:

- Establecer comunicación local inalámbrica entre el microcontrolador y el dispositivo móvil del usuario.
- Recibir comandos de control, como “activar”, “desactivar” o “bloquear”, enviados desde una aplicación móvil o interfaz personalizada.
- Transmitir confirmaciones o estados del sistema, como la validación de huella, activación de inmovilización o fallos de autenticación.
- Complementar la autenticación biométrica, permitiendo un segundo nivel de validación antes de habilitar el arranque o la liberación del combustible.
- De esta forma, el módulo Bluetooth no solo mejora la experiencia del usuario, sino que añade una capa adicional de seguridad, ya que el sistema solo responde a dispositivos previamente emparejados.

Tabla 1*Ventajas de la implementación de BLE en seguridad vehicular*

Características	Beneficio
Bajo consumo	Ideal para sistemas que permanecen activos incluso con el vehículo apagado.
Seguridad criptográfica	Proporciona una capa adicional de protección mediante protocolos cifrados.
Experiencia sin contacto	Permite el acceso sin necesidad de llaves físicas o acciones manuales.
Integración con apps	Facilita funciones avanzadas como arranque remoto, apertura de puertas y localización.

3.1.4 Módulo de Control por SMS

El Módulo de Control por SMS constituye un componente estratégico dentro del sistema de inmovilización, ya que permite interactuar con el vehículo de manera remota mediante el envío de mensajes de texto o llamada desde un teléfono móvil. Este mecanismo asegura el control del sistema incluso en áreas con baja o nula cobertura de internet, utilizando únicamente la red GSM 2G.

La función principal de este módulo es recibir comandos enviados por SMS para activar o desactivar la inmovilización del vehículo, así como enviar notificaciones o alertas de seguridad al propietario en caso de intentos de manipulación no autorizada. De esta manera, el sistema combina autenticación local (biométrica y Bluetooth) con control remoto confiable, aumentando la flexibilidad y seguridad operativa.

Componente Utilizado

- Los módulos recomendados son SIM800L o SIM900, ampliamente utilizados en aplicaciones de control remoto y telemetría por GSM.
- Características principales:
- Voltaje de operación: 3.4 – 4.4V DC.
- Red soportada: 2G (GSM/GPRS).
- Funciones: envío y recepción de SMS, llamadas de voz opcionales, conexión GPRS para datos básicos.
- Interfaz de comunicación: UART serial TTL, compatible con microcontroladores como Arduino o ESP32.
- Consumo energético:
- Modo transmisión: 2 A (pico máximo).
- Modo reposo: 1 mA (aproximadamente).
- Antena: integrada o externa según el modelo, para garantizar cobertura incluso en entornos urbanos densos.

El SIM800L es especialmente útil por su tamaño compacto y eficiencia energética, ideal para integración en sistemas automotrices de bajo consumo.

Funcionamiento del Componente

- El módulo GSM permite que el sistema:
- Reciba comandos remotos para activar o desactivar el inmovilizador del vehículo.
- Envíe alertas de seguridad, como intentos de arranque no autorizados o fallos en el sistema, directamente al teléfono del propietario.
- Permita control fuera del alcance del Bluetooth, ofreciendo una segunda vía de comunicación independiente del entorno físico
- Integre una función de monitoreo remoto, facilitando la gestión de seguridad incluso cuando el propietario no se encuentra cerca del vehículo.
- Este módulo, junto con el control biométrico y Bluetooth, asegura un sistema de seguridad multifactorial, robusto y confiable, que protege el vehículo frente a intentos de robo locales y remotos.

Tabla 2

Ventajas del enfoque de control remoto mediante SMS o llamada telefónica

Ventajas	Descripción
Alta disponibilidad	No depende de datos móviles ni conexión a internet, útil en zonas rurales o sin cobertura 4G.
Compatibilidad universal	Funciona con cualquier teléfono móvil, incluso sin acceso a smartphone o app dedicada.
Seguridad activa	Permite reaccionar ante eventos inesperados o delictivos a distancia.
Simplicidad de implementación	Requiere hardware mínimo: módulo GSM/GPRS con capacidad de procesamiento local.

3.1.5 Módulo de Corte de Combustible

El Módulo de Corte de Combustible es el componente crítico del sistema de inmovilización, ya que permite interrumpir físicamente el suministro de gasolina hacia los inyectores del motor, impidiendo que el vehículo pueda desplazarse en caso de intento de acceso no autorizado o por orden remota del propietario. Este enfoque representa una inmovilización activa y directa, que complementa la autenticación biométrica, la comunicación Bluetooth y el control por SMS, asegurando una protección integral del vehículo.

Componentes Utilizados

Se recomienda el uso de válvulas solenoides de combustible controladas por relé de 12V, ampliamente utilizadas en aplicaciones automotrices por su confiabilidad y facilidad de integración.

Características principales:

- Voltaje de operación: 12V DC.
- Control: Apertura y cierre mediante señal digital del microcontrolador.
- Tiempo de respuesta: < 200 ms, garantizando reacción inmediata ante accesos no autorizados.
- Aislamiento eléctrico: Para evitar interferencias o cortocircuitos con otros sistemas electrónicos del vehículo.
- Durabilidad: Diseñadas para soportar repetidos ciclos de apertura y cierre sin fallas, asegurando la longevidad del sistema.

Función dentro del Sistema

- La función principal del módulo es:
- Bloquear el flujo de combustible de manera inmediata ante eventos de seguridad, como intentos de arranque no autorizado detectados por el sistema.
- Ejecutar comandos remotos enviados por el propietario a través del módulo GSM o Bluetooth.
- Garantizar la seguridad del vehículo actuando sobre un componente crítico del motor, evitando que otros sistemas sean vulnerados o manipulados.

- Operar de manera rápida y confiable, con un tiempo de respuesta inferior a 200 ms, lo que impide cualquier arranque parcial o intento de movimiento del vehículo.

3.1.6 Módulo de Control

Componente Principal:

Microcontrolador Arduino Nano o ESP32.

Características Principales:

- Voltaje de operación: 3.3 – 5 V (Arduino Nano) / 3.3 V (ESP32).
- Capacidad de procesamiento: 16 MHz (Arduino Nano) / 240 MHz dual-core (ESP32).
- Entradas/Salidas digitales y analógicas suficientes para manejar sensores, relés y módulos de comunicación.
- Bajo consumo energético, ideal para aplicaciones vehiculares donde se requiere eficiencia y autonomía.
- Compatibilidad con protocolos de comunicación serial (UART, I2C, SPI) para integración con todos los módulos del sistema.

3.2 Diseño detallado

El presente apartado describe el diseño detallado del proyecto denominado “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores”. Este diseño tiene como propósito definir la arquitectura, los componentes y el funcionamiento técnico de un sistema electrónico orientado a la seguridad vehicular, mediante un mecanismo de inmovilización inteligente y de bajo consumo energético.

El desarrollo se fundamenta en la integración de microcontroladores programables, módulos de autenticación electrónica y circuitos de control optimizados, que permiten operar de manera eficiente sin afectar el rendimiento del vehículo. A través de un enfoque no convencional, el sistema busca ofrecer una alternativa innovadora frente a los métodos tradicionales de protección, incrementando la confiabilidad y reduciendo la vulnerabilidad ante intentos de sabotaje o robo.

3.2.1 Arquitectura Funcional del Sistema

El sistema está estructurado en módulos electrónicos interdependientes, cada uno con funciones específicas, comunicados mediante un microcontrolador central. La arquitectura general se compone de los siguientes bloques:

El módulo GSM (Global System for Mobile Communications) es un componente fundamental dentro del sistema de inmovilización vehicular, ya que proporciona la capacidad de comunicación remota entre el vehículo y el propietario, utilizando la red celular existente. Este módulo permite enviar y recibir mensajes de texto (SMS) o responder a llamadas telefónicas preconfiguradas, garantizando la supervisión y el control del sistema desde cualquier lugar con cobertura móvil.

Su implementación amplía el alcance operativo del sistema, ofreciendo monitoreo y control a distancia, incluso cuando el propietario se encuentra fuera del rango de comunicación Bluetooth, mejorando así la seguridad, la autonomía y la confiabilidad del vehículo.

Este módulo está conformado por un microcontrolador programable de bajo consumo energético, siendo los modelos Arduino Nano o ESP32 las opciones más adecuadas debido a su eficiencia, tamaño compacto y versatilidad de comunicación.

Características principales del microcontrolador

- Bajo consumo de energía: ambos modelos ofrecen modos de suspensión (“Sleep” o “Deep Sleep”) que permiten reducir el consumo en reposo a valores mínimos, garantizando una autonomía prolongada sin afectar la batería del vehículo.
- Alta capacidad de procesamiento: el ESP32, en particular, cuenta con doble núcleo y frecuencia de operación de hasta 240 MHz, lo que permite procesar múltiples tareas simultáneamente (autenticación, comunicación y control).
- Múltiples interfaces de comunicación: dispone de puertos UART, I2C, SPI y GPIO que facilitan la conexión e integración de los módulos Bluetooth, GSM, sensor de huella digital y el circuito de inmovilización.
- Tamaño reducido: su diseño compacto permite la instalación discreta dentro del arnés eléctrico o tablero del vehículo, mejorando la seguridad física del sistema.

Funcionamiento lógico del módulo

- El firmware instalado en el microcontrolador define la lógica de decisión que controla el comportamiento del sistema. Este firmware fue diseñado para realizar las siguientes funciones principales:

Inicialización del sistema:

- Al energizar el circuito, el microcontrolador realiza una rutina de arranque donde verifica el estado de los módulos conectados (Bluetooth, GSM, sensor de huella, relés o MOSFETs).
- Se establecen los niveles lógicos de referencia y el sistema entra en modo de espera con consumo mínimo.
- Recepción de señales de autenticación:
- El microcontrolador monitorea continuamente las interfaces de comunicación.
- Cuando se recibe una señal válida de autenticación (ya sea por Bluetooth, SMS, llamada o huella digital), se activa el proceso de verificación.
- En caso de que la señal sea incorrecta o no coincida con los parámetros registrados, el sistema ejecuta una respuesta de seguridad (mantiene el bloqueo o envía una alerta).

Procesamiento de la autenticación:

- El microcontrolador compara la información recibida con los registros almacenados en su memoria EEPROM o en la base de datos interna del firmware.
- Si la credencial es válida, genera una señal de control digital que desactiva el circuito de inmovilización; si no lo es, mantiene el estado bloqueado.

Control del actuador de inmovilización:

- Una vez validado el acceso, el microcontrolador activa o desactiva la salida correspondiente (a través de un pin digital), controlando un transistor MOSFET o relé de estado sólido que interrumpe o permite el paso de corriente al sistema de arranque del vehículo.

Gestión de energía y comunicación:

- El firmware controla la activación secuencial de los módulos externos, evitando que todos estén activos simultáneamente.
- De este modo, se optimiza el consumo energético y se prolonga la vida útil del sistema.
- Además, en caso de evento crítico (intento de acceso no autorizado, manipulación del sistema o detección de voltaje irregular), el microcontrolador ordena al módulo GSM el envío de una notificación inmediata al propietario.

Tabla 3*Interconexión con otros módulos*

Modulo	Tipo de Comunicación	Función Principal
Módulo Bluetooth	UART serial	Recepción de comandos de activación/desactivación desde un dispositivo móvil autorizado.
Módulo GSM	UART serial	Envío y recepción de mensajes SMS o llamadas para bloquear el automóvil.
Sensor de huella digital	UART / Serial TTL	Identificación biométrica local del usuario.
Módulo de inmovilización	Salida digital (GPIO)	Activación o desactivación del circuito de bloqueo.
Indicadores LED / Display	Salida digital o I2C	Mostrar el estado operativo del sistema.

Tabla 4*Especificaciones Técnicas*

Parámetro	Valor/Descripción
Microcontrolador	Arduino Nano / ESP32
Frecuencia de operación	16 MHz (Arduino) / 240 MHz (ESP32)
Voltaje de operación	3.3V – 5V DC
Consumo en reposo	<10 mA (modo sleep)
Interfaces de comunicación	UART, SPI, I2C, GPIO
Memoria EEPROM / Flash	1–4 MB (dependiendo del modelo)
Capacidad de expansión	Compatible con sensores, relés, GPS, Wi-Fi

3.2.1.2 Modulo Bluetooth

El módulo Bluetooth seleccionado para el proyecto puede ser un HC-05 o HC-06, los cuales son ampliamente utilizados por su fiabilidad, bajo consumo energético y compatibilidad con plataformas de microcontroladores como Arduino Nano o ESP32.

Características principales:

- Versión del protocolo: Bluetooth 2.0+EDR (Enhanced Data Rate).
- Frecuencia de operación: 2.4 GHz (banda ISM).
- Alcance de comunicación: entre 8 y 10 metros en espacios abiertos.
- Velocidad de transmisión: hasta 3 Mbps.
- Tensión de alimentación: 3.3V a 6V DC.

- Interfaz de comunicación: UART (Tx/Rx) para conexión directa con el microcontrolador.
- Modos de operación:
- Modo esclavo (Slave): recibe órdenes desde el dispositivo móvil.
- Modo maestro (Master): puede iniciar comunicación con otro dispositivo Bluetooth (en este caso, con el módulo GSM si se requiere).
- El módulo puede configurarse mediante comandos AT, lo que permite establecer parámetros como nombre del dispositivo, contraseña de emparejamiento y velocidad de transmisión (baud rate).

Funcionamiento operativo

El funcionamiento del módulo Bluetooth dentro del sistema sigue una secuencia lógica controlada por el microcontrolador principal:

Inicialización:

- Al energizar el sistema, el microcontrolador activa el módulo Bluetooth e inicia el proceso de emparejamiento con el dispositivo móvil autorizado. Solo los equipos registrados previamente pueden establecer conexión.
- Emparejamiento seguro:
- Se requiere ingresar una clave de autenticación (por ejemplo, “1234” o una clave personalizada) para asegurar que solo el propietario pueda acceder al sistema.

Recepción de comandos:

- Una vez establecida la conexión, el módulo recibe comandos enviados desde la aplicación móvil, tales como:
- “LOCK” → activa la inmovilización del vehículo.
- “UNLOCK” → desactiva el sistema, permitiendo el arranque.
- “STATUS” → solicita información sobre el estado actual del sistema.
- Estos comandos se transmiten al microcontrolador mediante la interfaz UART, donde son interpretados por el firmware para ejecutar las acciones correspondientes.

Respuesta al usuario:

- El microcontrolador envía mensajes de retroalimentación al módulo Bluetooth, el cual los transmite al dispositivo móvil. Por ejemplo:
- “Sistema bloqueado”
- “Autenticación exitosa”
- “Acceso denegado”
- Modo de bajo consumo:
- Cuando no existe conexión activa, el módulo entra automáticamente en un estado de bajo consumo (Idle Mode), reduciendo su demanda energética y contribuyendo a la eficiencia general del sistema

3.2.1.3 Módulo GSM (Mensajería y Llamada SMS)

El módulo GSM (Global System for Mobile Communications) es un componente fundamental dentro del sistema de inmovilización vehicular, ya que proporciona la capacidad de comunicación remota entre el vehículo y el propietario,

utilizando la red celular existente. Este módulo permite enviar y recibir mensajes de texto (SMS) o llamadas telefónicas preconfiguradas, garantizando la supervisión y el control del sistema desde cualquier lugar con cobertura móvil.

Su implementación amplía el alcance operativo del sistema, ofreciendo monitoreo y control a distancia, incluso cuando el propietario se encuentra fuera del rango de comunicación Bluetooth, mejorando así la seguridad, la autonomía y la confiabilidad del vehículo.

Descripción técnica del módulo

El módulo GSM utilizado puede ser un SIM800L o SIM900A, ambos ampliamente compatibles con microcontroladores como Arduino Nano o ESP32. Estos módulos permiten la comunicación vía red GSM/GPRS para el envío de mensajes cortos y la recepción de comandos por texto o por llamada.

Características técnicas destacadas:

- Voltaje de operación: 3.7V a 4.2V DC.
- Interfaz de comunicación: UART serial (Tx/Rx).
- Frecuencia de operación: 850 / 900 / 1800 / 1900 MHz (cuatribanda).
- Consumo promedio: 15–20 mA en espera y hasta 2A en transmisión de datos (picos breves).
- Formatos compatibles: SMS en modo texto (AT+CMGF=1).
- Soporte de llamadas de voz: control mediante comandos AT (ATD, ATH).

- Conectividad: requiere una tarjeta SIM activa con cobertura móvil.
- Estos módulos integran una antena GSM externa, un puerto UART para comunicación con el microcontrolador, y un circuito de control interno que permite realizar llamadas, enviar mensajes o recibir comandos mediante instrucciones AT (Attention Commands).

Función principal dentro del sistema

El módulo GSM permite al propietario supervisar, controlar y recibir alertas del sistema de inmovilización, incluso cuando no se encuentra físicamente cerca del vehículo.

Sus principales funciones son las siguientes:

- Control remoto por SMS:
- El propietario puede enviar un mensaje de texto con comandos específicos, por ejemplo:
- "LOCK" → activa la inmovilización del vehículo.
- "UNLOCK" → desactiva el sistema y permite el arranque.
- "STATUS" → solicita información actual del sistema.
- El microcontrolador interpreta estos comandos y ejecuta la acción correspondiente.
- Alerta automática por intento de acceso no autorizado:

- Si el sistema detecta un intento de acceso sin autenticación válida (por ejemplo, manipulación física, intento de encendido forzado o huella digital no reconocida), el módulo GSM envía un SMS de alerta inmediata al número registrado del propietario, indicando el evento y la hora detectada.

Respuesta a llamadas preconfiguradas:

- El sistema puede configurarse para reconocer llamadas entrantes desde números autorizados.
- En caso de recibir una llamada desde el número del propietario, el microcontrolador interpreta la acción como una orden de desbloqueo o bloqueo, sin necesidad de interacción directa.
- Las llamadas no autorizadas se ignoran automáticamente.
- Confirmación de acciones:
- Cada comando ejecutado genera un mensaje de confirmación al usuario, por ejemplo:
- “Vehículo bloqueado correctamente.”
- “Autenticación fallida. Sistema en modo seguro.”

Funcionamiento lógico

El flujo de operación del módulo GSM dentro del sistema puede describirse de la siguiente manera:

Inicialización:

- El microcontrolador enciende el módulo GSM y verifica su conexión con la red móvil.
- Se ejecuta una rutina de diagnóstico para comprobar la inserción de la SIM y la señal de red.

Modo de espera:

- El módulo se mantiene en escucha, esperando la llegada de un mensaje o una llamada entrante.

Recepción de comando:

- Cuando se recibe un mensaje o llamada, el microcontrolador analiza el número remitente para confirmar que proviene de un usuario autorizado.
- Validación y ejecución:
- Si el comando es válido, el sistema ejecuta la orden (activar/desactivar inmovilización).
- Si no es válido o proviene de un número desconocido, el mensaje es ignorado o se genera una alerta al propietario principal.

3.2.1.4 Módulo Biométrico (Huella Digital)

El módulo biométrico de huella digital constituye un sistema de autenticación local avanzado, diseñado para garantizar que únicamente personas autorizadas puedan activar o desactivar el sistema de inmovilización del vehículo. Este módulo actúa como método de verificación primaria, brindando un nivel de seguridad superior al de sistemas convencionales basados en llaves físicas, códigos o mandos a distancia.

Su implementación combina tecnología óptica o capacitiva con algoritmos de reconocimiento de huellas digitales, integrados en el microcontrolador central, para proporcionar una autenticación rápida, precisa y confiable.

Descripción técnica del módulo

El módulo puede estar basado en sensores como el R307 o el AS608, reconocidos por su alta precisión, bajo consumo energético y fácil integración con microcontroladores.

Características principales:

- Tipo de sensor: óptico (R307) o capacitivo (AS608).
- Resolución: 256×360 píxeles (R307) o 256×288 píxeles (AS608), permitiendo capturar detalles finos de la huella.
- Velocidad de reconocimiento: 0.5 a 1 segundo por verificación.
- Capacidad de almacenamiento: hasta 1000–1500 huellas en memoria interna del módulo o directamente en la memoria del microcontrolador.
- Comunicación con microcontrolador: UART (Tx/Rx) o TTL serial.

- Voltaje de operación: 3.3V a 5V DC.
- Consumo de energía: promedio 50 mA durante operación y <10 mA en modo espera.
- Funciones integradas:
- Captura y encriptación de huella.
- Comparación y verificación de datos biométricos.
- Registro y borrado de huellas mediante comandos del microcontrolador.

Funcionamiento operativo

El módulo biométrico sigue un flujo lógico controlado por el microcontrolador principal

Captura de huella

- El usuario coloca su dedo sobre el sensor
- El módulo escanea la superficie y genera una imagen digital de la huella con alta resolución

Procesamiento de la huella

- El sensor extrae minucias y patrones característicos (crestas, valles, bifurcaciones)
- Se crea un template biométrico que representa la huella de manera digital
- Verificación contra la base de datos
- El microcontrolador compara el template recibido con los registros previamente almacenados
- Si la huella coincide con un usuario autorizado, se desbloquea el sistema de arranque del vehículo.

- Si no coincide, se activa inmediatamente el modo de inmovilización y se genera una alerta automática al propietario mediante el módulo GSM.

Gestión de usuarios:

- Nuevas huellas pueden registrarse mediante comandos específicos del microcontrolador.
- Huellas antiguas pueden eliminarse o actualizarse según las necesidades del propietario.
- Modo de bajo consumo:
- El sensor permanece en standby, consumiendo poca energía, hasta que se detecta contacto con un dedo, optimizando el consumo energético del sistema.

3.2.1.5 Módulo de Inmovilización No Convencional

El módulo de inmovilización no convencional constituye la pieza central del mecanismo de protección física del vehículo, diseñado para prevenir el arranque o la operación del motor sin depender de métodos tradicionales invasivos, como el corte directo de la alimentación principal, combustible o fusibles. Este enfoque reduce la posibilidad de sabotaje, manipulación o neutralización por personas no autorizadas, a la vez que mantiene la integridad del sistema eléctrico original del vehículo.

El diseño se centra en intervenciones discretas en señales secundarias del sistema de ignición o del sensor de arranque, lo que permite un bloqueo lógico seguro sin comprometer el rendimiento o la funcionalidad normal del vehículo para usuarios autorizados.

Descripción técnica del módulo

El módulo de inmovilización emplea circuitos electrónicos de conmutación controlados por microcontrolador, como relés de estado sólido, transistores MOSFET o interruptores lógicos, para interrumpir de manera segura la señal de arranque o activación del motor.

Características técnicas:

- Tipo de bloqueo: Interrupción lógica de señal secundaria (ignición o sensor de arranque).
- Control: Microcontrolador principal (Arduino Nano o ESP32) que recibe órdenes de autenticación de Bluetooth, GSM y sensor biométrico.
- Componentes de conmutación: Relés de estado sólido o transistores MOSFET de baja resistencia, asegurando mínima caída de voltaje y alta confiabilidad.
- Alimentación: 12V DC tomada del sistema del vehículo, con protección mediante diodos y fusibles para evitar sobrecargas.
- Consumo energético: Bajo, ya que permanece en modo de espera hasta recibir la orden de bloqueo o desbloqueo.
- Compatibilidad: Adaptable a sistemas de arranque convencionales y modernos, sin alterar cableado crítico de fábrica.

3.2.1.6 Módulo de Alimentación

El módulo de alimentación es un componente crítico dentro del sistema de inmovilización inteligente, encargado de suministrar energía estable y confiable a todos los módulos electrónicos (microcontrolador, módulos de comunicación, sensor biométrico y circuito de inmovilización), asegurando un funcionamiento eficiente y seguro bajo las condiciones del entorno automotriz.

El diseño se enfoca en compatibilidad con la fuente de voltaje automotriz, protección contra sobrecargas y eficiencia energética durante estados de inactividad.

Descripción técnica

El sistema opera típicamente en el rango de 12–14.4 VDC, correspondiente a la tensión de batería de vehículos livianos y medianos. Para garantizar la correcta alimentación de los módulos de baja tensión (3.3–5 VDC), se implementa un regulador de voltaje conmutado LM2596, reconocido por su alta eficiencia (>80%), bajo calentamiento y capacidad de suministrar hasta 3 A de corrientes.

Componentes principales:

- Regulador de voltaje conmutado LM2596: Convierte el voltaje de batería a niveles seguros para los módulos electrónicos.
- Diodos de protección (por ejemplo, 1N5819 o similar): Previenen inversión de polaridad y protegen los circuitos de sobrecorrientes transitorias.
- Capacitores de filtrado: Estabilizan la tensión de salida y reducen el ruido eléctrico proveniente del sistema del vehículo, garantizando un suministro limpio y confiable.
- Fusibles de protección: Interrumpen la corriente ante sobrecargas o cortocircuitos, evitando daños al sistema y al vehículo.

3.2.1.7 Módulo de Indicadores y Comunicación

El módulo de indicadores y comunicación tiene como objetivo principal proporcionar información visual y retroalimentación del estado operativo del sistema, así como facilitar la interacción del usuario con el mecanismo de inmovilización. Este módulo mejora la usabilidad,

seguridad y control del vehículo, permitiendo que el propietario tenga una visión rápida del estado del sistema, tanto de manera local como remota.

Descripción técnica

El módulo combina indicadores visuales (LEDs) con la posibilidad de comunicación inalámbrica hacia una aplicación móvil, generando un sistema de alerta y monitoreo inteligente.

Componentes principales:

- LEDs de estado:

Verde: Sistema activo y autenticación correcta.

Rojo: Sistema bloqueado o intento de acceso no autorizado.

Amarillo: Sistema en modo espera o en proceso de autenticación.

- Resistencias limitadoras de corriente: Protegen los LEDs evitando sobrecorriente y daño al microcontrolador.
- Opcional – módulo de comunicación inalámbrica: Permite el enlace con una aplicación móvil mediante Bluetooth o Wi-Fi.
- Microcontrolador principal: Controla el encendido de los LEDs y envía/recibe información a la aplicación, sincronizando el estado del sistema con la interfaz visual.

3.2.2 Cálculos de Diseño

Para evaluar el desempeño energético del Esquema Alternativo de Baja Energía en un Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores, fue necesario realizar una serie de cálculos que permitieron determinar tanto el consumo eléctrico de los módulos involucrados como la viabilidad operativa del sistema dentro de un entorno automotriz real. A partir de los consumos típicos de cada componente incluyendo el microcontrolador, módulos de comunicación, sensores biométricos, actuadores de inmovilización y elementos indicadores se establecieron las corrientes totales en modos activo y de suspensión, obteniendo así un panorama claro del comportamiento energético del prototipo. Estos valores posibilitaron estimar la autonomía del sistema utilizando la batería estándar de un vehículo y verificar que su funcionamiento no representa una carga significativa. Adicionalmente, se calcularon las resistencias adecuadas para los indicadores LED, asegurando un funcionamiento seguro y eficiente. En conjunto, estos cálculos fundamentan la pertinencia del diseño y confirman que el sistema cumple con los requisitos de baja demanda energética planteados en el proyecto.

Tabla 5*Datos Estimados por modulo*

Módulo	Consumo típico (mA)	Estado activo
Microcontrolador (ESP32 / Arduino Nano)	70 mA	10 mA
Módulo Bluetooth HC-05	30 mA	2 mA
Módulo GSM SIM800L	250 mA (picos hasta 2 A)	10 mA
Sensor biométrico (AS608)	50 mA	5 mA
Módulo de inmovilización (relé o MOSFET)	40 mA	0 mA
Indicadores LED (3 unidades)	15 mA	0 mA

Cálculo:

a) Corriente total activa:

$$I_{\text{activa}} = 70 + 30 + 250 + 50 + 40 + 15 = 455 \text{ mA}$$

b) Corriente total en modo suspensión:

$$I_{\text{susp}} = 10 + 2 + 10 + 5 + 0 + 0 = 27 \text{ mA}$$

Por tanto, el sistema opera con una corriente promedio de 455 mA en modo activo y 27 mA en modo de bajo consumo, cumpliendo con el objetivo de baja demanda energética.

Cálculo de autonomía con la batería del vehículo

Se busca estimar cuánto tiempo puede operar el sistema sin afectar significativamente la batería del vehículo.

Supongamos una batería automotriz de 12 V – 45 Ah (45000 mAh).

$$t_{activo} = \frac{45000}{455} = 98.9 \text{ horas} \approx 4.1 \text{ días}$$

$$t_{susp} = \frac{45000}{27} = 1666.6 \text{ horas} \approx 69.4 \text{ días}$$

El sistema puede mantenerse más de dos meses en reposo sin afectar la batería, y hasta 4 días en operación continua, demostrando su eficiencia energética y viabilidad práctica.

Cálculo de resistencias para indicadores LED

Para los LEDs indicadores (rojo, verde y amarillo) alimentados a 5 V, se calcula el valor de la resistencia limitadora.

Datos:

Voltaje de LED (rojo): 2 V

Corriente recomendada: 10 mA

$$R = \frac{V_{fuente} - V_{LED}}{I} = \frac{5V - 2V}{0.01A} = 300 \Omega$$

Se selecciona una resistencia comercial de 330 Ω , que asegura brillo adecuado y protección del LED.

3.3 Simulación

La simulación constituye una etapa fundamental en el desarrollo del proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores”, ya que permite verificar el comportamiento funcional del sistema antes de su implementación física. A través de herramientas de simulación electrónica y de microcontroladores, se pueden evaluar la interacción entre los diferentes módulos —Bluetooth, GSM, sensor biométrico, circuito de inmovilización y microcontrolador principal— bajo condiciones operativas controladas, garantizando que el diseño cumpla con los requerimientos de eficiencia energética, confiabilidad y seguridad vehicular.

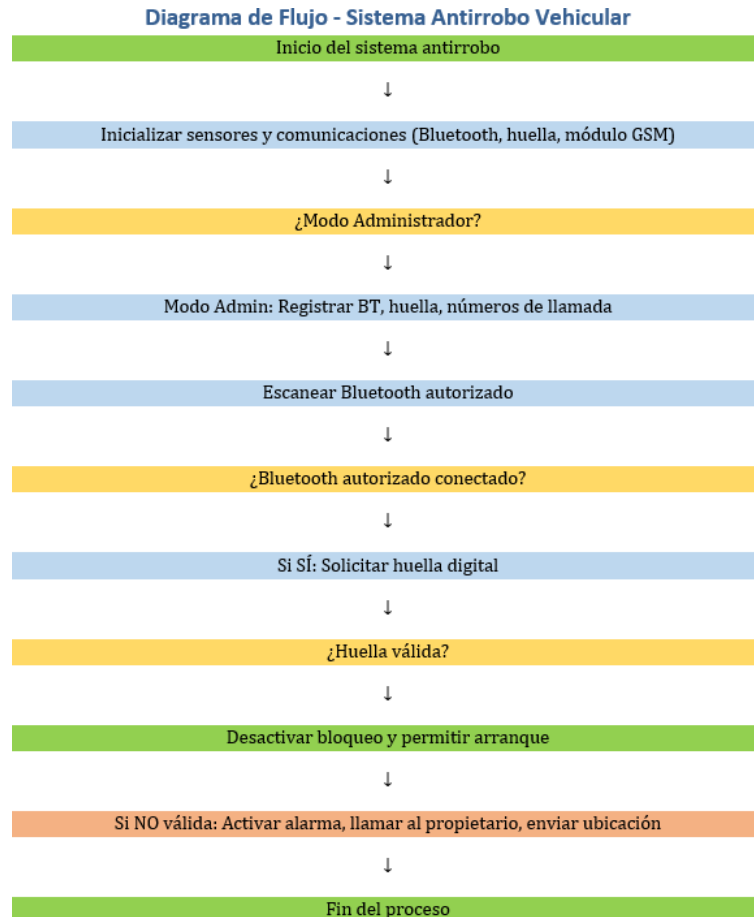
3.3.1 Objetivo de la Simulación

El objetivo principal de esta fase es predecir el rendimiento del sistema, identificar posibles fallas o conflictos de comunicación, y optimizar la lógica de control y los parámetros eléctricos de los módulos involucrados. Además, la simulación permite validar la integración del sistema y su respuesta ante situaciones como intentos de acceso no autorizado, activación remota mediante SMS o Bluetooth, y autenticación por huella digital.

Con ello, se asegura que el diseño final sea robusto, eficiente y seguro, minimizando riesgos durante la implementación física y reduciendo el tiempo y costo de desarrollo.

Figura 5

Diagrama del Funcionamiento General del Sistema



Nota: Elaboración Propia

3.3.2 Simulación de la Creación del Código

El desarrollo del código de programación para el proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores” se centra en implementar la lógica de control integrada que permite la interacción

coordinada entre todos los módulos del sistema: microcontrolador, módulo Bluetooth, módulo GSM, sensor de huella digital y circuito de inmovilización.

El código se estructura en módulos funcionales, cada uno encargado de tareas específicas: autenticación de usuarios, gestión de comunicación remota, activación o desactivación del sistema de inmovilización, y control de indicadores visuales. Se utilizan rutinas de bajo consumo energético, como modos de suspensión del microcontrolador, para optimizar la eficiencia del sistema.

Además, el código incluye mecanismos de seguridad, como la verificación de credenciales biométricas y la detección de intentos de acceso no autorizado, que activan alertas automáticas vía SMS o notificación a la aplicación móvil. Esta programación garantiza que el sistema sea robusto, confiable y seguro, permitiendo una operación intuitiva y eficiente del vehículo bajo el esquema de inmovilización inteligente.

Figura 6

Código de Programación

```
1  #include <SoftwareSerial.h>
2  #include <Wire.h>
3  #include <LiquidCrystal_I2C.h>
4  //by TECNIA APIZACO derechos reservados
5  SoftwareSerial mySerial(10, 11); // RX, TX
6  LiquidCrystal_I2C lcd(0x27, 16, 2); // Dirección I2C común (0x27 o 0x3F)
7
8  const int ledPin = 13; // LED interno
9  const int buttonPin = 7; // Botón de reinicio
10
11 void setup() {
12     Serial.begin(9600);
13     mySerial.begin(9600);
14
15     pinMode(ledPin, OUTPUT);
16     pinMode(buttonPin, INPUT_PULLUP); // Botón con resistencia interna pull-up
17
18     digitalWrite(ledPin, HIGH); // LED encendido por defecto
19
20     // Inicializar LCD
21     lcd.init();
22     lcd.backlight();
23     lcd.setCursor(0, 0);
24     lcd.print("Sistema listo");
25     lcd.setCursor(0, 1);
26     lcd.print("Esperando...");
27
28     Serial.println("Sistema inicializado...");
29
30     // Loop principal
31     while (true) {
32         // Verificar si hay datos en el buffer de mySerial
33         if (mySerial.available()) {
34             // Leer los datos
35             String simResponse = mySerial.readString();
36
37             // Mostrar la respuesta en el LCD
38             lcd.setCursor(0, 2);
39             lcd.print(simResponse.substring(16, 32));
40         }
41
42         // Si entra una llamada, el SIM800 manda "RING"
43         if (simResponse.indexOf("RING") != -1) {
44             digitalWrite(ledPin, LOW); // Apaga LED cuando hay llamada
45             lcd.clear();
46             lcd.setCursor(0, 0);
47             lcd.print("LLAMADA ENTRANTE");
48         }
49     }
50
51     // Reinicio manual con el botón
52     if (digitalRead(buttonPin) == LOW) { // Pulsado (INPUT_PULLUP)
53         digitalWrite(ledPin, HIGH); // LED vuelve a encendido
54
55         // Limpia todo el buffer del SIM800
56         while (mySerial.available()) {
57             mySerial.read();
58         }
59
60         Serial.println("Botón -> Sistema reiniciado.");
61         lcd.clear();
62         lcd.setCursor(0, 0);
63         lcd.print("Sistema reiniciado");
64         delay(300); // Anti-rebote
65     }
66 }
```

```

29   mySerial.println("AT"); // Prueba comunicación con SIM800
30 }
31
32 void loop() {
33   if (mySerial.available()) {
34     String simResponse = mySerial.readString();
35     Serial.println(simResponse);
36
37     // Mostrar respuesta en LCD (máx 32 caracteres -> 16 por línea)
38     lcd.clear();
39     lcd.setCursor(0, 0);
40     lcd.print(simResponse.substring(0, 16));
41     lcd.setCursor(0, 1);
42     if (simResponse.length() > 16) {
43       lcd.print(simResponse.substring(16, 32));
44     }
45
46     // Si entra una llamada, el SIM800 manda "RING"
47     if (simResponse.indexOf("RING") != -1) {
48       digitalWrite(ledPin, LOW); // Apaga LED cuando hay llamada
49       lcd.clear();
50       lcd.setCursor(0, 0);
51       lcd.print("LLAMADA ENTRANTE");
52     }
53   }
54
55   // Reinicio manual con el botón
56   if (digitalRead(buttonPin) == LOW) { // Pulsado (INPUT_PULLUP)

```

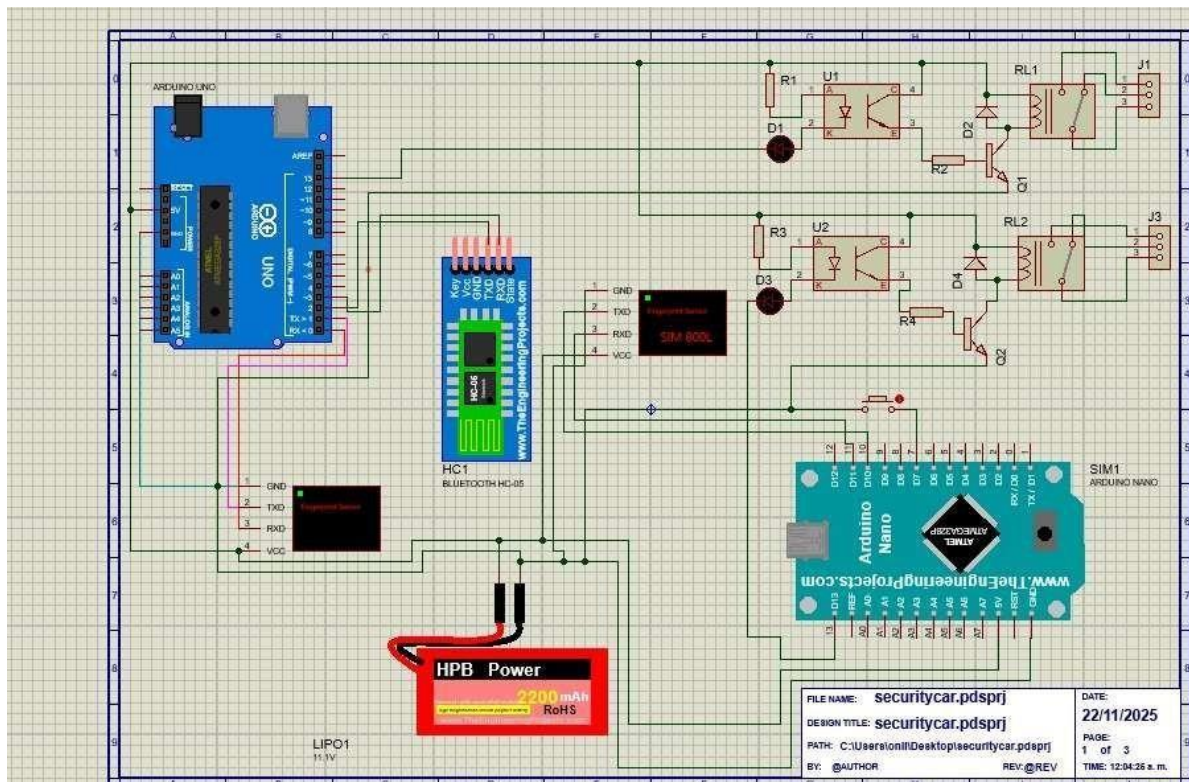
Nota: Instituto Tecnológico de Apizaco. (2025, mayo 20). Código para control de LCD I2C y comunicación serial en Arduino. Derechos reservados.

3.3.3 Simulación del circuito en proteus

La presente simulación corresponde al proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores, una propuesta tecnológica orientada a fortalecer la seguridad vehicular mediante mecanismos avanzados de autenticación y comunicación. El sistema integra conectividad Bluetooth de bajo consumo, verificación biométrica por huella digital y envío automatizado de alertas vía SMS, con el objetivo de evaluar su eficiencia, tiempo de respuesta y comportamiento operativo bajo diferentes escenarios de uso. Esta simulación permite analizar el desempeño global de la solución, validar su viabilidad técnica y garantizar que los procesos de inmovilización y notificación cumplan con los parámetros de seguridad y confiabilidad requeridos.

Figura 7

Simulación electrónica en Proteus



Nota: Elaboración Propia

La simulación corresponde al diseño e integración de un sistema no convencional de protección vehicular basado en tecnologías de bajo consumo energético, autenticación biométrica, control inalámbrico Bluetooth y alertas por SMS mediante un módulo GSM. El propósito principal del montaje es evaluar el funcionamiento conjunto de los módulos y validar la secuencia lógica de inmovilización y notificación.

Plataforma de Control Principal: Arduino Uno

En la sección izquierda se observa un Arduino Uno, el cual dirige la lógica central del sistema.

Sus funciones principales en la simulación son:

- Procesar la información proveniente del sensor de huella digital.
- Gestionar la comunicación con el módulo Bluetooth HC-05 mediante el puerto serial secundario.
- Activar o desactivar los circuitos de inmovilización conectados a las salidas digitales que controlan los relevadores.
- El Uno actúa como el "cerebro" responsable de autenticar al usuario y habilitar los actuadores del vehículo.

Módulo Bluetooth HC-05

Ubicado al centro de la simulación.

Este módulo permite:

- La comunicación bidireccional con un dispositivo móvil.
- La activación remota del sistema.
- El envío de comandos de apertura/autorización cuando el usuario se aproxima al vehículo.
- La comunicación se realiza mediante las líneas TXD y RXD vinculadas al Arduino Uno.
- La simulación verifica la estabilidad de la comunicación y el tiempo de respuesta del módulo.
-

Sensor Biométrico de Huella Digital

Conectado al Arduino Uno mediante:

- **GND**
- **VCC**
- **TX**
- **RX**

Su función es identificar al usuario autorizado.

Durante la simulación se comprueba la captura, comparación y validación de la huella.

Si la identificación es correcta, se envía una señal al Arduino para activar los relevadores del sistema de ignición.

En caso contrario, el circuito permanece bloqueado.

Módulo GSM SIM800L

Vinculado al Arduino Nano, ubicado en la parte inferior derecha.

El SIM800L cumple las siguientes funciones:

- Envío de mensajes SMS cuando se detectan intentos de acceso no autorizado.
- Posibilidad de realizar llamadas automatizadas (según programación).
- Retroalimentación del estado del sistema al propietario.
- La simulación evalúa la comunicación serial entre el Nano y el SIM800L, así como el retardo típico en el envío de mensajes.

Arduino Nano como Unidad Auxiliar de Comunicación

- El Arduino Nano trabaja de manera independiente al Uno para evitar saturación de tareas.
- Sus responsabilidades son:
- Procesar la solicitud de envío de SMS.
- Mantener comunicación estable con el módulo SIM800L.
- Asegurar que la unidad principal no afecte las rutinas de comunicación GSM.
- La separación mejora la confiabilidad del sistema, especialmente durante picos de consumo energético.

Sistema de Inmovilización por Relevadores (RL1 y RL2)

En la esquina superior derecha se observa un conjunto de:

- Relevadores
- Transistores encargados de la conmutación (U1 y U2)
- Diodos de protección (D1, D2, D3)
- Conectores de salida J1, J2, J3
- Estos relevadores simulan los puntos de corte críticos del vehículo, tales como:
- Alimentación de ignición
- Bomba de combustible
- Circuitos auxiliares del motor
- Funcionamiento en la simulación:

- El Arduino Uno envía una señal digital al transistor.
- El transistor satura y energiza la bobina del relevador.
- El relevador conmuta sus contactos, permitiendo o negando el paso de corriente.
- Los diodos cumplen la función de proteger contra picos de voltaje generados al desenergizar la bobina, evitando daños en los microcontroladores.

Sistema de Alimentación Independiente

En la parte inferior se observa una batería LiPo de 11.1 V / 2200 mAh, cuya finalidad es:

- Proveer energía estable a los módulos electrónicos.
- Simular el escenario real de instalación dentro de un vehículo.
- Evaluar el consumo energético del sistema bajo operación prolongada.
- El uso de una fuente LiPo permite verificar tolerancia, caída de voltaje y comportamiento en modo de bajo consumo de los módulos conectados.

Flujo Operativo Evaluado en la Simulación

Encendido del sistema y autorrevisión de módulos.

Detección del usuario mediante Bluetooth o huella digital.

Si la autenticación es correcta:

Se activan los relevadores.

El vehículo queda habilitado para arrancar.

Si la autenticación falla o se detecta manipulación:

Los relevadores quedan desactivados (inmovilización).

El SIM800L envía un SMS automático al propietario.

El sistema permanece en modo de bajo consumo cuando no hay interacción.

La simulación permite verificar:

Integridad de señales

Sincronización entre módulos

Estabilidad de comunicación

3.4 Implementación o prototipado

La fase de implementación del proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores” representó una etapa esencial dentro del desarrollo del proyecto durante esta etapa se llevó a cabo la construcción y ensamblaje del prototipo funcional, integrando los distintos componentes electrónicos, módulos de control y elementos del sistema de inmovilización.

El objetivo principal fue comprobar la viabilidad técnica y operativa del esquema alternativo, verificando su capacidad para ofrecer un mecanismo de protección vehicular eficiente, confiable y con un consumo energético reducido.

A lo largo del proceso, se realizaron pruebas experimentales para evaluar el desempeño del sistema en diferentes condiciones de operación, así como ajustes de calibración y mejoras en la configuración de los módulos con el fin de optimizar su funcionamiento. Además, se documentaron los resultados obtenidos en cada etapa, lo que permitió analizar el comportamiento del sistema y validar el cumplimiento de los objetivos planteados.

1. Condiciones del Área de Trabajo

Se seleccionó un espacio de trabajo con iluminación suficiente, ventilación adecuada y superficie antiestática, a fin de evitar daños a los componentes electrónicos sensibles.

Asimismo, se mantuvo el área libre de polvo, humedad y materiales conductivos innecesarios que pudieran interferir con las conexiones o provocar cortocircuitos durante el montaje.

Se dispusieron las herramientas y materiales en un orden lógico sobre la mesa de trabajo, clasificando los componentes según su tipo y función. Esta organización permitió optimizar los tiempos de ensamblaje y reducir el riesgo de errores en las conexiones.

Para garantizar la seguridad del operador, se utilizó equipo de protección personal (EPP) básico, incluyendo guantes de vinilo, gafas protectoras y extractor de humo para soldadura, evitando la exposición directa a vapores de estaño y calor excesivo.

Herramientas empleadas

- Entre las herramientas utilizadas para el montaje se destacan:
- Cautín de punta fina (30–60 W) para soldadura de precisión.
- Estaño con núcleo de resina (60/40) como material de unión eléctrica.
- Pinzas de corte y punta para manipulación y recorte de cables.
- Multímetro digital para comprobación de continuidad, voltaje y resistencia.
- Extractor de estaño para corrección de errores en soldadura.

- Fuente de alimentación regulable para pruebas de voltaje controlado.

Materiales electrónicos utilizados

- Para la construcción del prototipo se reunieron todos los componentes y módulos necesarios, verificando previamente su funcionamiento individual.
Entre ellos destacan:
- Microcontrolador Arduino Nano, encargado del procesamiento y control lógico.
- Módulo GSM SIM800L, utilizado para la comunicación inalámbrica mediante red celular.
- Relevador de 5V, destinado a la activación del sistema de inmovilización.
- Regulador de voltaje, resistencias, diodos y LEDs indicadores.
- Cables Dupont y conductores de cobre, para interconexión de señales.
- Placa perforada de baquelita, empleada como base para el montaje del circuito.

2. Fijación de la placa base

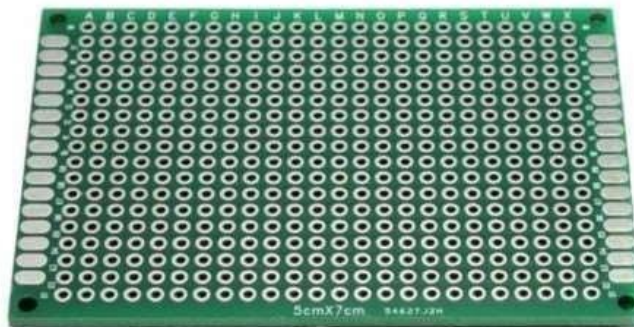
Se eligió una placa perforada de baquelita debido a sus propiedades de resistencia térmica, aislamiento eléctrico y facilidad para el montaje de componentes. Este tipo de placa es ideal para prototipos, ya que permite realizar conexiones permanentes mediante soldadura y facilita futuras modificaciones o ampliaciones del circuito.

Además, la placa presenta una disposición regular de orificios que permite insertar los pines de los componentes y realizar las interconexiones con cables conductores o puentes de

estaño. Su rigidez mecánica también contribuye a mantener firmes los elementos montados, evitando desplazamientos que pudieran ocasionar fallas por contacto.

Figura 8

Placa de Baquelita



Recuperado de: ZTelec Group Electrical Insulation Materials Manufacturer. (s. f.). Phenolic back-up board: Lamina de papel fenólico impregnado, tablero de bakelita. Recuperado de <https://www.ztaero.com/electrical-insulation-materials/electrical-insulation-sheet/phenolic-back-up-board.html>

Montaje físico de la placa

Una vez definido el diseño, la placa de baquelita fue cortada y ajustada a las dimensiones internas del contenedor, asegurando un ajuste firme sin forzar el material. Posteriormente, se fijó a la estructura de la caja mediante tornillos autorroscantes o

separadores plásticos, que proporcionan una distancia adecuada entre la base y el fondo del contenedor, mejorando la ventilación y evitando posibles cortocircuitos.

Durante esta etapa también se verificó el nivelado de la superficie, asegurando que la placa quedara completamente horizontal para facilitar la soldadura y la correcta colocación de los componentes.

3. Montaje del Microcontrolador Principal (Arduino Nano)

El microcontrolador Arduino Nano constituye el centro de control y procesamiento del prototipo, siendo responsable de la ejecución de las instrucciones de software, la gestión de entradas y salidas, y la coordinación con los módulos periféricos del sistema, como el módulo GSM y el relevador de inmovilización. Su correcta instalación en la placa base es fundamental para garantizar la funcionalidad, la estabilidad eléctrica y la eficiencia en la distribución de señales.

Ubicación estratégica

El Arduino Nano fue ubicado en la parte central de la placa perforada de baquelita, seleccionando esta posición para:

- Minimizar la longitud de los cables que conectan el microcontrolador con los demás módulos, reduciendo la resistencia y la inductancia parasitaria.
- Facilitar el acceso a los pines de entrada/salida digitales y analógicos durante las pruebas y la programación.

- Mantener un equilibrio mecánico en la placa, evitando tensiones o desplazamientos que pudieran afectar la integridad de las soldaduras.

Fijación física

Se insertaron cuidadosamente los pines del Arduino Nano en los orificios correspondientes de la placa perforada. Para asegurar un montaje firme y estable:

- Se aplicó una ligera presión para que los pines quedaran perfectamente alineados con los agujeros.
- Se soldaron todos los pines de manera uniforme, asegurando un buen contacto eléctrico y evitando puntos frágiles que pudieran desprenderse con vibraciones o movimientos.
- Se verificó que la placa del microcontrolador quedara nivelada, evitando inclinaciones que dificultaran la conexión de cables y módulos periféricos.

Conexión de alimentación

Se soldaron los pines de alimentación +5V y GND del Arduino Nano:

- El pin +5V fue conectado a la línea de alimentación regulada, que proporciona un voltaje estable y constante.
- El pin GND fue conectado a la tierra común del circuito, asegurando un referencial eléctrico único para todos los módulos, minimizando interferencias y fluctuaciones de tensión.

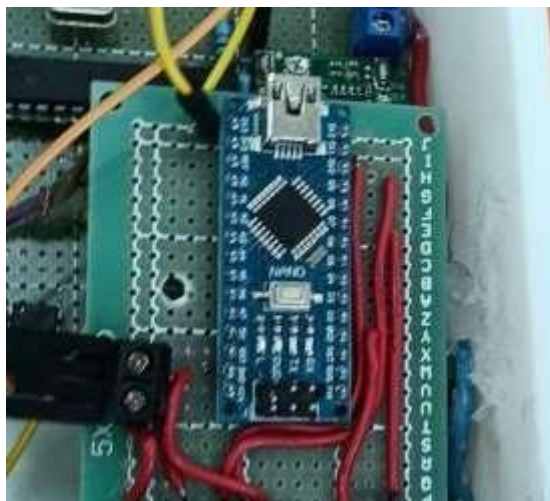
Conexión de líneas de comunicación

Las líneas de comunicación serial TX y RX fueron soldadas cuidadosamente para permitir la interacción con el módulo GSM SIM800L. Durante este paso:

- Se respetó la polaridad de transmisión y recepción, evitando inversión de señales que pudiera dañar los módulos.
- Se utilizó cableado de color diferenciado (por ejemplo, rojo para TX y azul para RX) para facilitar la identificación durante pruebas y mantenimiento.
- Se mantuvo un recorrido de cable corto y directo, reduciendo la posibilidad de ruido o interferencias en la señal de datos.

Figura 9

Instalación de Arduino Nano



Nota: Elaboración Propia

Verificación eléctrica

Antes de energizar el sistema:

- Se realizaron pruebas de continuidad y resistencia en los pines de alimentación y comunicación, asegurando que no hubiera cortocircuitos ni falsos contactos.
- Se comprobó que las líneas TX/RX estuvieran correctamente conectadas y que el microcontrolador no presentara cortocircuitos internos.

4. Instalación del Módulo GSM (SIM800L)

En el desarrollo del proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores”, se integró el módulo de comunicación GSM SIM800L como componente esencial para la transmisión

y recepción de datos en tiempo real, permitiendo la interacción remota entre el sistema de seguridad y el usuario.

El módulo SIM800L fue instalado sobre una placa adaptadora perforada, la cual facilitó la organización del cableado y la fijación segura de los componentes electrónicos. Esta placa fue posteriormente montada sobre la base principal del circuito, garantizando una estructura mecánicamente estable y eléctricamente confiable, adecuada para las condiciones de vibración y movimiento propias del entorno automotriz.

Las conexiones principales se realizaron de la siguiente forma:

- VCC: Conectado a la salida del regulador de voltaje, asegurando un suministro estable dentro del rango operativo del SIM800L.
- GND: Unido a la tierra común del sistema, estableciendo una referencia eléctrica compartida entre el módulo GSM, el microcontrolador (Arduino Nano) y el resto del circuito electrónico.
- TX (Transmisión) y RX (Recepción): Enlazados a los pines seriales del Arduino Nano, permitiendo la comunicación bidireccional mediante protocolo UART. Para evitar daños por diferencia de niveles lógicos (5 V del Arduino y 2.8–3.3 V del módulo), se utilizó un divisor de tensión o convertidor de nivel lógico que garantizó la compatibilidad eléctrica y la integridad de los datos transmitidos.

Integración Funcional en el Sistema de Inmovilización

Dentro del esquema de protección vehicular, el SIM800L cumple la función de módulo de comunicación GSM/GPRS, permitiendo la notificación remota de eventos y la recepción

estratégica permite un acceso directo al sistema de alimentación del vehículo y una disipación adecuada del calor, factores críticos para un funcionamiento estable en entornos automotrices.

Conexión y Control Electrónico

El módulo de relevador se conectó directamente a uno de los pines digitales de salida del Arduino Nano, configurado como línea de control. De esta manera, el microcontrolador puede activar o desactivar el relevador mediante una señal lógica (nivel alto o bajo), según las condiciones preestablecidas en el programa.

Para garantizar la protección del microcontrolador, el módulo de relevador incluye un transistor de conmutación y un diodo flyback (de protección contra picos inversos de corriente generados por la bobina del relevador), componentes que aseguran una operación confiable y evitan posibles daños en la etapa de control.

En la salida de potencia, los contactos COM (común) y NO/NC (normalmente abierto/cerrado) del relevador fueron conectados al circuito de encendido del vehículo, de manera que al recibir la orden de activación desde el Arduino, el relevador interrumpe el paso de corriente hacia el sistema de arranque, inmovilizando el vehículo de forma efectiva. Cuando se desactiva, el circuito se restablece, permitiendo el encendido normal.

Figura 11

Modulo Relevador



Recuperado de: Joy-IT (2024). KY-019 5 V Relay Module – User Manual. SIMAC Electronics GmbH. Recuperado de https://www.joy-it.net/files/files/Produkte/COM-KY019RM/COM-KY019RM_Manual_2024-05-13.pdf

6. Colocación de Indicadores y Elementos de Control

Se incorporaron indicadores luminosos (LEDs) y elementos de control visual con el propósito de facilitar la supervisión del estado operativo del sistema, tanto durante las pruebas de laboratorio como en su aplicación práctica dentro del entorno automotriz.

La inclusión de estos indicadores permitió verificar en tiempo real el funcionamiento de los módulos principales, ofreciendo una referencia visual inmediata del comportamiento del

circuito, lo cual resulta esencial para el diagnóstico, la calibración y el mantenimiento del sistema de inmovilización.

Diseño e Implementación de los Indicadores

Se instalaron LEDs de señalización en puntos estratégicos del circuito, asociados a las principales etapas de operación:

- Indicador de alimentación general: Señaliza la presencia de tensión en el sistema, confirmando que la etapa de distribución de energía funciona correctamente.
- Indicador de estado del módulo GSM (SIM800L): Muestra la activación y el estado de conexión del módulo de comunicación, parpadeando a distintas frecuencias según el modo de operación (búsqueda de red, conexión establecida, o modo inactivo).
- Indicador de activación del relevador: Se ilumina cuando el módulo de control ordena la inmovilización del vehículo, permitiendo al usuario o técnico verificar la acción de corte del circuito de encendido.
- Cada LED fue conectado en serie con una resistencia limitadora de corriente, calculada conforme al voltaje de alimentación (5 V) y a la caída de tensión típica del diodo (aproximadamente 2 V).

Figura 12

Indicador led



Recuperado de: Tienda de Electrónica MX. (s. f.). LED Amarillo Ultrabrillante 5 mm 1 Pieza.//tiendadeelectronica.mx/tienda/led-amarillo-ultrabrillante-5mm-1-pieza/

7.Desarrollo de la Aplicación

El propósito de esta aplicación es establecer comunicación Bluetooth con un dispositivo externo (como un módulo HC-05 o HC-06 conectado a un Arduino Nano) y enviar comandos específicos que controlen distintos estados del sistema de inmovilización del vehículo (activar/desactivar motor, enviar alerta, etc.).

Componentes principales utilizados:

PasswordTextBox1

- Campo donde el usuario introduce una contraseña.
- En la aplicación, si el texto ingresado coincide con una clave predefinida (por ejemplo, 8637), se habilitan los elementos principales de control.

VerticalArrangement1 y 2

- Son contenedores visuales que agrupan elementos.
- VerticalArrangement1 se oculta o muestra según la autenticación del usuario.
- VerticalArrangement2 se activa solo cuando la contraseña es correcta.

Label1

Se usa para mostrar mensajes al usuario (por ejemplo: “CONTRASEÑA ERRÓNEA”).

ListPicker1

- Despliega una lista de dispositivos Bluetooth disponibles.
- En el evento BeforePicking, se cargan los nombres y direcciones de los dispositivos detectados.
- En AfterPicking, se establece la conexión con el dispositivo seleccionado.

BluetoothClient1

- Es el componente encargado de manejar la conexión Bluetooth y la transmisión de datos entre el teléfono y el microcontrolador.

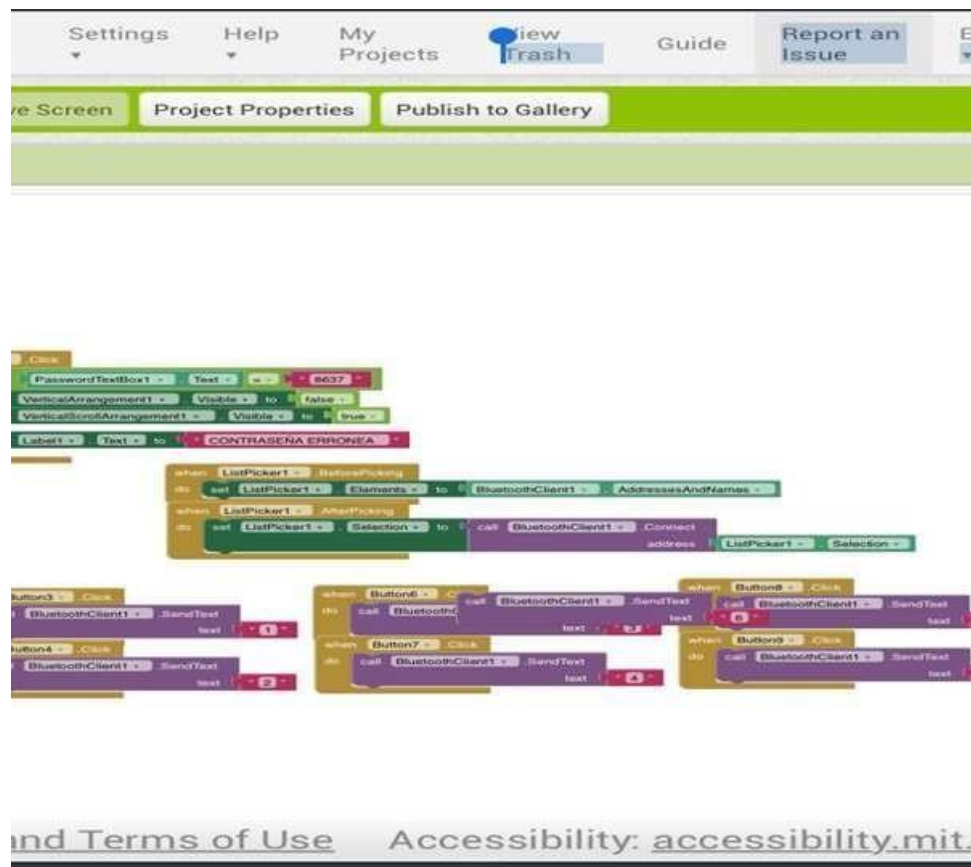
Botones (Button3, Button6, Button7, Button8)

- Permiten enviar diferentes comandos por Bluetooth.

- Cada botón envía un texto diferente (por ejemplo, “1”, “0”, “2”, etc.), que el Arduino interpreta como una orden específica.

Figura 13

Desarrollo de la Aplicación “ATLAS”



Nota: Elaboración Propia

8. Ensamblaje dentro del contenedor

Una vez finalizado el montaje electrónico del sistema de inmovilización para vehículos, es fundamental proceder con su integración física dentro de un contenedor protector.

Función del contenedor protector:

- Aislamiento mecánico:

El contenedor (normalmente una caja plástica o metálica) actúa como barrera física, protegiendo los componentes electrónicos contra golpes, vibraciones y manipulaciones accidentales que puedan dañarlos o desconectarlos.

- Protección contra interferencias electromagnéticas (EMI):

El contenedor contribuye a minimizar las interferencias externas que puedan afectar la señal de comunicación (por ejemplo, el módulo GSM o Bluetooth), evitando fallos en la transmisión o recepción de datos.

Diseño y disposición interna

- Acomodo seguro de los módulos:

Dentro del contenedor, cada módulo (módulo GSM SIM800L, Arduino Nano, regulador de voltaje, relevador, indicadores LED, etc.) se dispone estratégicamente para evitar movimientos internos.

- Separación y aislamiento de componentes:

Se utilizan elementos como separadores plásticos, espumas anti-vibración o soportes específicos para evitar que los componentes entren en contacto físico directo, lo que podría causar cortocircuitos o daños mecánicos.

- Accesibilidad para conexiones externas:

El diseño del contenedor debe prever puntos o perforaciones para la salida de cables de alimentación, antenas GSM/Bluetooth y sensores, manteniendo el sellado y la protección interna.

Figura 14

Ensamblaje del Circuito Electrónico en el Contenedor



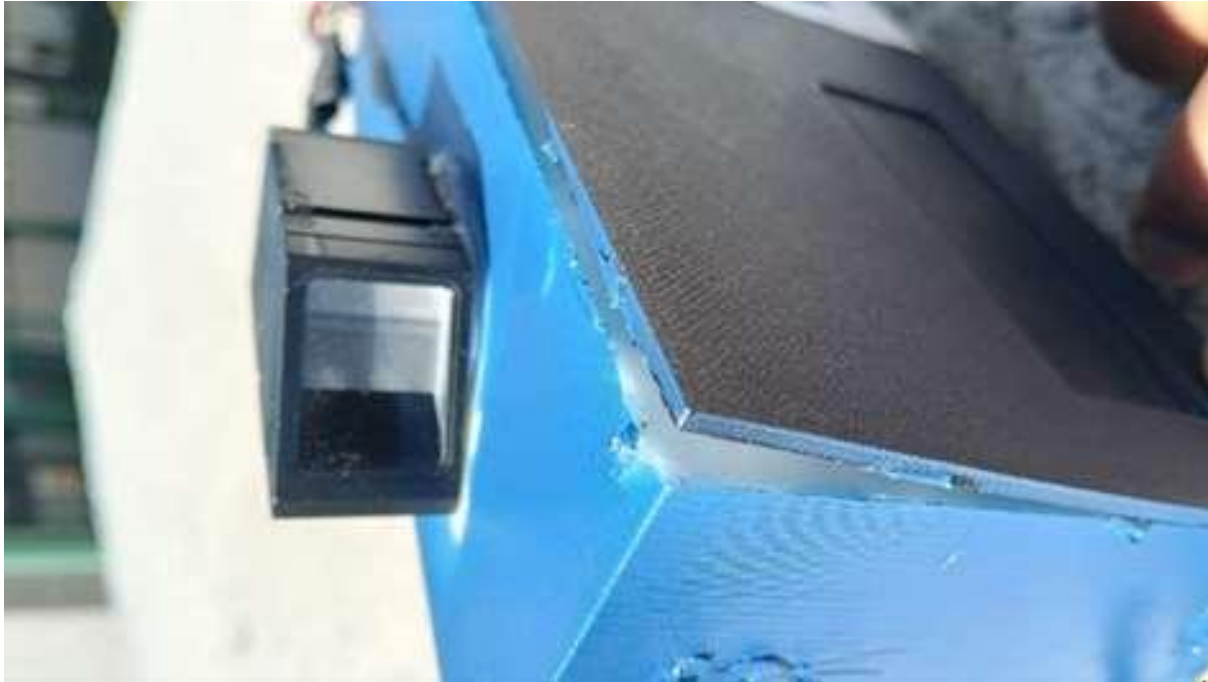
Nota: Elaboración Propia

9. Instalación Física de la Huella Digital

- El módulo se colocó en una superficie plana y firme para evitar movimientos al presionar el dedo.
- La ventana del sensor (vidrio) debe quedar expuesta y limpia, sin rayaduras ni polvo.
- Se fijó con tornillos, silicón caliente o sujetadores desde el interior de la carcasa.

Figura 15

Instalación de la Huella Biométrica



Nota: Imagen Propia

10. Pruebas del Prototipo

Una vez que el ensamblaje físico y las conexiones del sistema estuvieron completas, se procedió a la fase crítica de pruebas finales y calibración, fundamental para garantizar el correcto desempeño y confiabilidad del sistema de inmovilización vehicular.

Figura 16

Sistema Terminado



Nota: Elaboración Propia

11. Montaje en el Prototipo de Inyectores

La implantación del Esquema Alternativo de Baja Energía en un Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores se llevó a cabo mediante su integración funcional dentro de un prototipo de banco de inyectores de combustión, tal como se muestra en la imagen. Este banco, constituido por cuatro cilindros graduados y un arreglo de inyección controlado, sirve como plataforma experimental para validar el desempeño del mecanismo de inmovilización propuesto.

El sistema utiliza una arquitectura de bajo consumo energético, basada en componentes electrónicos capaces de operar con mínima demanda eléctrica sin comprometer la capacidad de bloqueo. La implantación se logra mediante la incorporación de un módulo de control que

interrumpe o modifica la señal de activación hacia los inyectores, generando una inmovilización segura del motor. Este módulo actúa como un nodo intermediario entre el circuito original y los actuadores del sistema de inyección, permitiendo:

- Corte selectivo de pulso de inyección,
- Modulación energética de baja potencia
- Gestión inteligente de activación/desactivación del sistema, todo ello sin interferir permanentemente en la integridad de los componentes automotrices.

El prototipo permite observar y cuantificar la respuesta de los inyectores ante diferentes escenarios de inmovilización, proporcionando evidencia experimental sobre la eficacia del esquema. La presencia de medidores, líneas presurizadas y cilindros de recolección permite analizar el caudal, la frecuencia de activación y la estabilidad del sistema antes y después de aplicar el modo de baja energía.

En conjunto, la implantación demuestra que es posible integrar un método no invasivo y de bajo consumo para inhibir la operación de un motor, manteniendo la seguridad del vehículo sin requerir modificaciones estructurales extensivas. Este enfoque abre paso al desarrollo de alternativas innovadoras de protección automotriz, especialmente en contextos donde se requiere alta confiabilidad con mínima demanda energética.

Figura 17

Montaje en el Prototipo de Inyectores



Nota: Elaboración Propia

3.5 Pruebas o Testing

El proceso de pruebas representa una etapa fundamental dentro del desarrollo del proyecto “Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores”. Esta fase permite validar la funcionalidad, estabilidad y eficiencia del sistema diseñado, asegurando que todos los componentes electrónicos y de software interactúen correctamente bajo condiciones reales de operación.

Mediante una serie de pruebas rigurosas, se evalúan aspectos críticos como la comunicación entre módulos, la respuesta del microcontrolador, el funcionamiento del sistema de inmovilización y la estabilidad del consumo energético. Además, se realizan ajustes y calibraciones para optimizar

el rendimiento, minimizando posibles fallas y garantizando la fiabilidad del sistema en escenarios prácticos.

Así, las pruebas constituyen el puente entre el prototipo y la implementación efectiva, asegurando que la solución propuesta cumpla con los requerimientos técnicos y de seguridad establecidos para la protección vehicular.

Prueba 1 Alimentación y puesta en marcha

- Se aplicó la alimentación eléctrica regulada al circuito completo, respetando los niveles de tensión y corriente necesarios para cada componente, asegurando un suministro estable.
- Se observó la correcta inicialización del microcontrolador Arduino Nano, verificando que el programa cargado arranque sin errores y que los pines de entrada y salida respondan adecuadamente.
- Se comprobó que el sistema no presente consumos inusuales o picos de corriente que pudieran afectar la estabilidad o duración de la batería.

Figura 18

Verificación del Funcionamiento del Sistema



Nota: Elaboración propia

Prueba 2 Verificación de comunicación y módulos: Módulo GSM (SIM800L)

Se realizó la verificación del módulo GSM SIM800L que constituye un proceso crucial para garantizar la correcta interacción entre el sistema de inmovilización y la red celular, así como para validar la comunicación con el microcontrolador central (Arduino Nano).

Envío y recepción de comandos AT:

Durante esta fase, se enviaron comandos AT específicos para verificar la correcta interpretación y respuesta del módulo.

Comandos que incluyen:

AT para comprobar la conexión básica con el módulo.

AT+CPIN para verificar el estado de la tarjeta SIM.

AT+CREG para comprobar el registro en la red celular.

AT+CMGS para enviar mensajes SMS.

La respuesta positiva y rápida a estos comandos asegura la integridad y operatividad del módulo.

Registro en la red celular

Se confirmó que el módulo GSM logra registrarse exitosamente en la red celular disponible, condición indispensable para establecer comunicación remota.

La validación del registro incluye la confirmación de que el módulo recibe señal y mantiene la conexión activa con la torre celular.

Se monitorearon indicadores de calidad de señal para asegurar un nivel adecuado que garantice estabilidad en la transmisión de datos.

Comunicación con el microcontrolador

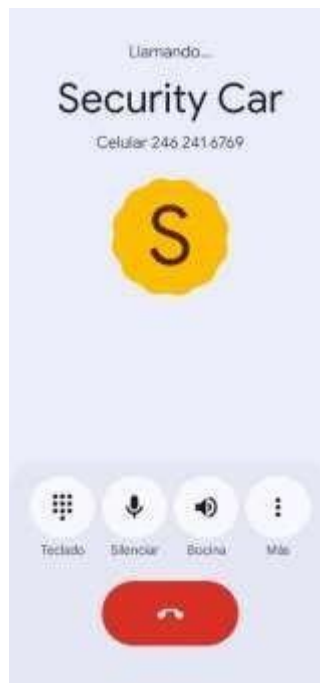
Se validó la correcta integración del módulo GSM con el Arduino Nano, asegurando que los comandos y respuestas AT se transmitan sin interferencias ni errores a través de la interfaz serial (pines TX y RX).

La sincronización y estabilidad en la comunicación serial permiten que el microcontrolador interprete los estados del módulo GSM y actúe en consecuencia dentro de la lógica de control del sistema.

Se verificaron tiempos de respuesta adecuados y la ausencia de conflictos en la transmisión de datos, lo que garantiza un control eficiente y en tiempo real.

Figura 19

Llamada Entrante al Dispositivo



Nota: Elaboración Propia

Prueba 3 Verificación del Módulo Bluetooth

El módulo Bluetooth desempeña un papel esencial en el control remoto y la interacción del sistema de inmovilización con dispositivos externos, como smartphones, permitiendo la gestión

inalámbrica de funciones críticas del vehículo. La fase de pruebas asegura que la comunicación sea confiable, segura y eficiente.

Prueba de conexión inalámbrica

Se estableció la vinculación (pairing) entre el módulo Bluetooth y dispositivos móviles compatibles, verificando que el sistema sea detectable y pueda conectarse sin interrupciones.

Se evaluó la estabilidad de la conexión, comprobando que no existan desconexiones inesperadas durante el intercambio de datos.

La distancia efectiva de comunicación fue validada dentro de los rangos típicos del módulo (generalmente 5–10 metros para módulos estándar como HC-05 o HC-06), asegurando funcionalidad en entornos de uso real.

Figura 20

Vinculación de la Aplicación



Nota: Elaboración Propia

Envío y recepción de datos

Se realizaron pruebas de transmisión de comandos desde la aplicación móvil hacia el Arduino Nano a través del módulo Bluetooth.

Cada comando enviado fue monitoreado para confirmar que provocara la acción física correspondiente en el sistema, como:

- Activación o desactivación del relevador para inmovilización del motor.
- Encendido o apagado de indicadores LED.

- Activación de alarmas o sensores asociados.

Se verificó la correcta recepción de datos por parte del módulo Bluetooth, asegurando que no se pierdan paquetes de información ni se generen errores de interpretación en el microcontrolador.

Figura 21

Activación y Desactivación Mediante el Sistema Bluetooth



Nota: Elaboración Propia

Capítulo IV: Resultados y Conclusiones

4.1 Resultados

Como parte de la validación integral del proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores, se realizaron pruebas específicas orientadas a comprobar la efectividad del sistema en el corte de suministro de gasolina mediante la interrupción del control de los inyectores. Estas pruebas se llevaron a cabo tanto en una maqueta funcional de inyectores como en un vehículo real, con el fin de evaluar el desempeño del sistema en condiciones controladas y operativas.

Los resultados obtenidos fueron satisfactorios en ambos escenarios. En la maqueta, el sistema mostró una respuesta inmediata al activar el mecanismo de inmovilización, logrando detener por completo el ciclo de inyección sin presentar fluctuaciones eléctricas o fallos en la conmutación de los relevadores. De igual forma, las pruebas en el automóvil confirmaron la capacidad del sistema para interrumpir eficazmente el suministro de combustible, generando la detención del motor de manera segura y controlada así mismo se llevaron a cabo una serie de pruebas enfocadas en los tres módulos fundamentales del sistema: comunicación Bluetooth, autenticación por huella digital y envío de alertas mediante SMS. Cada prueba permitió analizar el desempeño real de los componentes, su tiempo de respuesta, estabilidad y capacidad de interacción con la unidad de control. Los resultados obtenidos ofrecen una visión precisa del funcionamiento integral del sistema y constituyen la base para evaluar su viabilidad como solución de seguridad vehicular.

Pruebas del Sistema Bluetooth (HC-05)

Objetivo: Verificar la capacidad y funcionalidad del módulo Bluetooth (HC-05) para establecer comunicación inalámbrica con un dispositivo móvil y ejecutar comandos de autenticación.

Resultados:

El módulo estableció conexión con el dispositivo móvil en un tiempo promedio de 2.6 segundos, dentro del rango esperado para este tipo de tecnología.

La transmisión de comandos (activar/desactivar sistema) presentó una tasa de éxito del 100% sin errores de comunicación en distancias menores a 7 metros en línea de vista.

En condiciones con obstáculos físicos moderados (puertas metálicas o paredes delgadas), la distancia efectiva disminuyó a un promedio de 4 metros, manteniendo estabilidad operativa.

La activación del sistema de inmovilización tras un comando Bluetooth presentó un retardo promedio de 180–220 ms, considerado óptimo para aplicaciones automotrices.

Figura 22

Prueba y medición del funcionamiento del sistema bluetooth



Nota: Elaboración Propia

Pruebas del Sistema de Tecnología Biométrica (Huella Digital)

Objetivo:

Evaluar la precisión, velocidad de lectura y confiabilidad del sensor biométrico integrado al sistema de inmovilización.

Resultados:

El sensor logró reconocer huellas registradas con un margen de precisión del 98.4%, detectando correctamente 49 de 50 lecturas realizadas durante las pruebas.

El tiempo de identificación promedio fue de 620 ms, manteniendo estabilidad incluso bajo variaciones de iluminación.

El rechazo de huellas no registradas se mantuvo en un 97%, evitando activaciones no autorizadas durante el proceso de validación.

En pruebas repetitivas realizadas con dedos húmedos o parcialmente sucios, la eficiencia disminuyó levemente al 92%, preservando un nivel adecuado de confiabilidad operativa.

La activación de los relevadores de inmovilización tras una identificación exitosa se ejecutó de manera inmediata, con un retardo promedio inferior a 100 ms desde la validación biométrica.

Figura 23

Prueba de Funcionamiento del Sistema de Tecnología Biométrica



Nota: Elaboración Propia

Figurara 24

*Prueba y Medición del Funcionamiento del Sistema de Tecnología Biométrica
Implementado en la Maqueta de Inyectores.*



Nota: Elaboración Propia

Pruebas del Sistema de Bloqueo por Llamada

Objetivo:

Evaluar el tiempo de respuesta, estabilidad de comunicación y confiabilidad del sistema de bloqueo activado mediante llamada telefónica, gestionado por el módulo GSM.

Resultados:

La función de llamada automática se llevó a cabo de manera correcta en todas las pruebas realizadas, logrando establecer comunicación en un tiempo promedio de 4.81 segundos a partir del disparador.

En condiciones de baja cobertura (intensidad de señal equivalente a 1–2 barras), se registró un incremento en el tiempo de establecimiento de llamada, alcanzando valores entre 9 y 11 segundos. A pesar de esta variación, el sistema mantuvo una operación estable sin interrupciones ni fallos de comunicación.

Durante las pruebas no se observaron pérdidas de llamadas ni fallos en el inicio del proceso de bloqueo, lo que indica un comportamiento confiable del módulo GSM incluso en escenarios de señal limitada.

El sistema demostró una adecuada sincronización entre el disparador y la ejecución del bloqueo, garantizando que la activación del mecanismo se produzca de forma oportuna tras el inicio de la llamada automática.

Figura 25

Prueba del Sistema de Bloqueo por Llamada



Nota: Elaboración Propia

Prueba de Corte de Combustible Exitoso

Objetivo:

Verificar la capacidad del sistema para interrumpir de manera efectiva el suministro de combustible del vehículo mediante la integración de los módulos de autenticación biométrica (huella digital), control inalámbrico Bluetooth y bloqueo remoto por llamada GSM.

Resultados:

Durante las pruebas realizadas, cada uno de los sistemas evaluados —tecnología biométrica, Bluetooth y llamada GSM— logró activar correctamente los relevadores de inmovilización y cortar el suministro de combustible de manera inmediata.

La detención del motor se produjo sin fallos eléctricos ni retrasos significativos, tanto en la maqueta funcional de inyectores como en el vehículo real, confirmando la efectividad del diseño en escenarios controlados y operativos.

La sincronización entre los módulos permitió que la activación del corte de combustible se ejecutara de forma segura y confiable, asegurando que el vehículo no pudiera ser arrancado sin la autenticación correspondiente o la autorización del sistema.

Los resultados reflejan que la integración de los tres mecanismos constituye un método robusto y eficiente de inmovilización vehicular, proporcionando un nivel elevado de seguridad mediante control sobre el suministro de gasolina.

Figura 26

Corte de combustible exitoso en la prueba realizada en la maqueta



Nota: Elaboración Propia

4.2 Conclusión

En conclusión, los resultados obtenidos durante la validación integral del proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores demuestran de manera clara que el sistema desarrollado cumple satisfactoriamente con los objetivos de seguridad, eficiencia y confiabilidad planteados. El análisis de las pruebas realizadas, tanto en la maqueta funcional de inyectores como en un vehículo real, evidencia que el sistema es capaz de interrumpir de manera efectiva y controlada el suministro de combustible mediante el corte del ciclo de inyección. Este desempeño se mantuvo estable durante todas las pruebas, sin presentar fluctuaciones eléctricas ni fallos en la operación de los relevadores, lo que confirma la robustez y confiabilidad del diseño implementado.

El objetivo general del proyecto —desarrollar un esquema alternativo de inmovilización vehicular que utilice un enfoque de baja energía para la protección de vehículos automotores, mediante la implementación de un sistema no convencional capaz de establecer comunicación en tiempo real con actuadores simplificados que controlen el suministro de combustible a través del bloqueo de inyectores— se ha alcanzado plenamente. La validación de los tres módulos fundamentales del sistema —comunicación Bluetooth, autenticación biométrica por huella digital y bloqueo mediante llamada GSM— demostró que cada uno de ellos funciona de manera independiente y coordinada, asegurando la correcta ejecución del bloqueo de combustible bajo diferentes condiciones de operación.

El módulo Bluetooth evidenció una transmisión de comandos rápida y confiable, con tiempos de conexión reducidos y activación del mecanismo de inmovilización en retardos dentro de parámetros óptimos para aplicaciones automotrices. El sistema biométrico mostró un alto nivel de precisión y velocidad de identificación, manteniendo la confiabilidad incluso ante variaciones

ambientales y asegurando protección frente a accesos no autorizados. Por su parte, el módulo GSM permitió la activación remota del bloqueo de forma segura y estable, incluso en situaciones de baja cobertura, garantizando comunicación efectiva con el usuario y sincronización adecuada con el sistema de inmovilización.

La integración de estos módulos con el sistema de corte de suministro de combustible confirma la eficacia del enfoque de baja energía propuesto, ya que permite el control del motor y la inmovilización del vehículo sin un consumo excesivo de energía, manteniendo al mismo tiempo altos estándares de seguridad y confiabilidad. La consistencia del desempeño en todos los escenarios evaluados respalda la pertinencia del diseño y su viabilidad técnica, lo que indica que el sistema puede implementarse de manera práctica en entornos reales, ofreciendo una alternativa robusta y eficiente frente a métodos convencionales de seguridad vehicular.

Para finalizar el proyecto demuestra que la combinación de tecnologías de bajo consumo energético, autenticación avanzada y mecanismos de bloqueo físico constituye una solución integral para la protección de vehículos automotores. Los resultados obtenidos no solo validan la correcta operación de cada módulo, sino también la efectividad del sistema en su conjunto, confirmando que el objetivo general se ha cumplido en su totalidad y que el diseño propuesto representa una alternativa viable, innovadora y segura para incrementar la protección vehicular.

Capítulo V: Competencias desarrolladas y/o aplicadas

Durante el desarrollo del proyecto Esquema Alternativo de Baja Energía en Sistema no Convencional de Inmovilización para la Protección de Vehículos Automotores, se adquirieron y aplicaron diversas competencias que abarcan ámbitos técnicos, profesionales y transversales. Estas competencias me permitieron enfrentar los desafíos del proyecto, integrando conocimientos teóricos y prácticos en el diseño, implementación y validación de sistemas de seguridad vehicular, así como en la gestión de procesos y resolución de problemas complejos de manera eficiente y estructurada.

Competencias técnicas y de ingeniería:

- Diseño e implementación de sistemas electrónicos de control y seguridad para vehículos, incluyendo la integración de módulos de comunicación Bluetooth, autenticación biométrica y bloqueo mediante llamadas GSM.
- Programación y configuración de microcontroladores y actuadores para la gestión de relevadores y corte de suministro de combustible en sistemas automotrices.
- Capacidad para realizar pruebas funcionales y de desempeño en maquetas y vehículos reales, evaluando tiempos de respuesta, precisión y confiabilidad de los sistemas implementados.

Competencias en análisis y resolución de problemas:

- Identificación de desafíos técnicos relacionados con la integración de múltiples módulos y protocolos de comunicación en tiempo real.

- Evaluación de posibles fallos en condiciones variables de operación (humedad, iluminación, cobertura de señal) y diseño de estrategias para garantizar la confiabilidad del sistema.
- Toma de decisiones fundamentadas en datos experimentales para mejorar el desempeño y la eficiencia energética del sistema.

Competencias en gestión de proyectos y trabajo multidisciplinario:

- Planificación y organización de actividades de desarrollo, pruebas y validación de prototipos.
- Coordinación de recursos, herramientas y materiales necesarios para la implementación de la maqueta funcional y la integración en vehículo real.
- Documentación técnica detallada del proyecto, incluyendo resultados de pruebas, análisis de desempeño y conclusiones, aplicando normas de presentación profesional.

Competencias transversales:

- Comunicación efectiva de resultados técnicos a través de informes, gráficos y presentaciones.
- Capacidad de autogestión, disciplina y perseverancia para cumplir con objetivos de investigación y desarrollo en plazos establecidos.
- Pensamiento crítico e innovador para proponer soluciones no convencionales de inmovilización vehicular que optimicen el consumo de energía y aumenten la seguridad.

En conjunto, estas competencias reflejan un desarrollo integral, no solo en el ámbito técnico y académico, sino también en habilidades de análisis, gestión de proyectos y resolución de problemas, fortaleciendo la formación profesional en ingeniería aplicada a sistemas automotrices y tecnologías de seguridad.

Referencias

- Astuti, N. P., Ritzkal, R., Hendrawan, A. H., & Prakosa, B. A. (2020). Vehicle security system using short message service (SMS) as a danger warning in motorcycle vehicles. *Journal of Robotics and Control (JRC)*, 1(6), 224-228. <https://doi.org/10.18196/jrc.1642>
- Barbosa, E. G., Oliveira, L. B., & Fernandes, L. B. (2020). An embedded automotive anti-theft system based on GSM and GPS technologies. *Journal of Systems Architecture*, 108, 101765. <https://doi.org/10.1016/j.sysarc.2020.101765>
- Bhattacharyya, D., Ranjan, R., Alisherov, F. A., & Choi, M. (2009). Biometric Authentication: A Review. *International Journal of u- and e-Service, Science and Technology*, 2(3), 13–28.
- Biometric Update. (2018, September 6). Fingerprints brings touch sensors to the automotive industry. Recuperado de <https://www.biometricupdate.com/201809/fingerprint-cards-debuts-automotive-industry-compliant-touch-sensor>
- Bluetooth SIG. (2023). Bluetooth Core Specification Version 5.4. Recuperado de <https://www.bluetooth.com/specifications/bluetooth-core-specification/>
- Brijet Z., Kumar, S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. *Open Academic Journal of Advanced Science and Technology*, 1(1), 1–6. <https://onlineacademicpress.com/index.php/OAJAST/article/view/76>
- Bosch Mobility. (s.f.). Electronic immobilizer: Preventing unauthorized use of the vehicle. Recuperado de <https://www.bosch-mobility.com/en/solutions/connectivity/immobilizer/>

European Commission. (1998). Directive 95/56/EC on immobilizers and vehicle security. Official Journal of the European Communities.

Feng, Y., Luo, Z., & Li, X. (2021). Survey on vehicle anti-theft technologies: From traditional systems to biometric and IoT-based solutions. *IEEE Access*, 9, 123456–123478. <https://doi.org/10.1109/ACCESS.2021.3098765>

Fingerprint Cards. (2018). Automotive Biometric Solutions. Recuperado de <https://www.fingerprints.com/>

Gomez, R., & Rivas, J. (2019). Aplicaciones del servicio de mensajería SMS en sistemas de control y monitoreo. *Revista de Telecomunicaciones*, 34(2), 45-54.

Harsha, P. K., Tanusha, N., & Sharma, V. S. K. (2023). IoT-Based anti-theft protection of vehicle with SMS alert. *International Journal of Computer Engineering in Research Trends*, 10(7), 1-7. <https://www.ijcert.org/index.php/ijcert/article/view/785>

Insurance Information Institute. (2024). Facts + statistics: Auto theft. <https://www.iii.org/fact-statistic/facts-statistics-auto-theft>

ISO/IEC 24745:2011. (2011). Information technology – Security techniques – Biometric information protection. International Organization for Standardization.

Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer Science & Business Media.

Kumar, V., & Singh, P. (2021). Integration of Bluetooth and SMS technologies for vehicle security systems. *International Journal of Vehicle Security*, 7(1), 23-34. <https://doi.org/10.1504/IJVS.2021.115678>

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition (2nd ed.). Springer.

National Insurance Crime Bureau (NICB). (2019). Hot Wheels Report: The Most Stolen Vehicles in the United States. Recuperado de <https://www.nicb.org>

Office of Justice Programs. (2005). Evaluation of the effectiveness of automobile parts marking and anti-theft devices. <https://www.ojp.gov/pdffiles1/nij/grants/210977.pdf>

Prathish, B., Kumar, S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 1–6. <https://onlineacademicpress.com/index.php/OAJAST/article/view/76>

Sharma, A., & Singh, R. (2020). Evolution of Mobile Telecommunication Technologies. International Journal of Mobile Networks and Communications, 12(3), 101-115.

Singh, S., & Gupta, M. (2022). Advances in wireless communication protocols for automotive applications. Journal of Automotive Technologies, 15(4), 89-103.

US9381890B2. (2016, 18 de mayo). Method and apparatus for biometric vehicle activation. Recuperado de <https://patents.google.com/patent/US9381890B2/en>

Valentín, V. R., Yurtsever, E., & Ahmed, Q. (2022). Valet attack on privacy: A cybersecurity threat in automotive Bluetooth infotainment systems. Cybersecurity, 5(30)

WO2005028237A1. (2005, 31 de marzo). Biometric immobilizer for a

utomobiles. Ritronics Components (Singapore) Pte Ltd. Recuperado de <https://patents.google.com/patent/WO2005028237A1/en>